ixia

Master Test Plan

Essential Testing for WLAN Networks Master Test Plan

Version History

Date	Version	Comments
03/21/2007	1.1	Initial Release
08/08/2007	1.3	Modified and extended a/b/g Test Cases from Version 1.1 Added 3 new QoS Functional Test Cases Added Test Case Profiles applicable to a specific SUT configuration or a specific test area
10/18/2007	1.4	Added Power Save Transition test cases Completed System and Stress test case sections Completes 802.11a/b/g test plan
08/20/2008	1.5	Added 802.11n Test Cases Modified Power Save and QoS Test cases to use WaveDynamix Removed Test Cases involving non-productized scripts

Table of Contents

Introduction

WLAN networks are rapidly evolving as well as expanding into many deployments and usage models. It has quickly replaced wired LAN as the main access technology in SoHo, Enterprise and is rapidly gaining acceptance in city-wide mesh networks. Since the deployment of wireless networks is becoming mission-critical to small businesses and revenue models, it is imperative that these networks be tested for compliance, performance, reliability and security to ensure a high-quality end-user experience.

When the dominant use of WLAN was for in-home convenience, it was sufficient to perform only basic authentication/association tests with a few security types, with simple traffic simulation devices based on end-user equipment. With WLAN making the transition into the enterprise, the expectation of the end customer is for the same level of quality that the wired LAN industry has delivered. Because wireless networks provide access for a wide variety of clients with many levels of performance requirements, wireless network equipment must be qualified with regards to all traffic behaviors, power management techniques, and security methods, and in the presence of all types of clients simultaneously. This test plan provides the enterprise-class coverage necessary to ensure compliance and performance of WLAN systems.

Also, the soon to be finalized 802.11n standard brings a new level of functionality and performance to the world of Wireless LAN. Components are becoming available, and are being designed into Access Points in both consumer and enterprise network equipment. To deliver a competitive 802.11n Access Point, the Development and QA Engineers have two major challenges ahead of them:

- Ensuring their 802.11n Access Points work flawlessly in 802.11a/b/g legacy modes, and
- Delivering on the performance enhancements in speed and range that 802.11n offers.

These two initiatives are of prime importance to the end customer. To make the leap to the new technology, they must be confident that current network performance will not be compromised, and that there is a definite performance gain available from the new features that is worth the cost and risk of changeover.

Any chipset and system design introducing a new standard is prone to issues related to support of both legacy standards for backwards compatibility and implementation of the new standard. Both performance and functionality is not assured just by design. To meet the demanding requirements of 802.11n, the components and drivers have been substantially changed from earlier chipset designs. This means that the verification of all features, modes and functions set forth by the both 802.11a/b/g and 802.11n sections of the standard must be performed on the Access Point and associated WLAN controller.

Essential WLAN testing requirements can be categorized into four major areas - **functional verification**, **performance measurement and network capacity assessment**, **system testing**, and **stress testing**.

Goals

This test plan addresses the testing requirements of WLAN infrastructure equipment by focusing on the four major categories mentioned above. The test plan uses the VeriWave WaveTest™ TGA platform to test features supported by components that make up the WLAN such as APs, Controllers and LAN switches (hereby collectively called the **SUT**). These tests should be conducted during hardware and software qualification, software/firmware release testing, vendor selection or as a part of pre-deployment testing.

The emphasis of this test plan is on many aspects of security policies, power management, bandwidth capacity and performance of the APs, WLAN Controllers and the wired infrastructure such as Ethernet switches, DHCP and RADIUS servers etc.

SUT Overview

The important building blocks that constitute the SUT and some of the key functionalities that may be supported include the following:

- WLAN Access Point
  - Establishes the wireless channel(s) for communication with WLAN clients
  - Authenticates and allows clients to connect to the WLAN
  - Acts as a conduit for WLAN client traffic sent to and received from the wired network and also between clients in the same BSS
  - Encrypts and decrypts 802.11 frames destined to and originating from WLAN clients if encryption is turned on
- WLAN Controller
  - Supports various client management functions such as allowing client associations, authentications and maintaining or rejecting connections
  - Performs security handshakes required by security protocols as well as port-based authentication
  - Manages prioritization of traffic flowing into and out of the SUT as well as bandwidth management
  - Balances client load to limit the number of client connections accepted to ensure that the traffic handling performance is not disrupted
  - Acts as a Stateful firewall that controls access and inspects traffic flow in order to enforce user/group policies and prevent denial-of-service attacks
  - Implements IDS/IPS modules to detect and prevent intrusions from disrupting the availability of the WLAN

- Executes, controls and manages mobility aspects including Layer 3 roaming and fast roaming
- Provides SSID/BSSID and VLAN management to support all the virtual networks supported by the WLAN and wired-LAN
- Switches traffic from/to multiple Downlink ports on the controller to the up-link port(s) as well as switching traffic between different Downlink ports

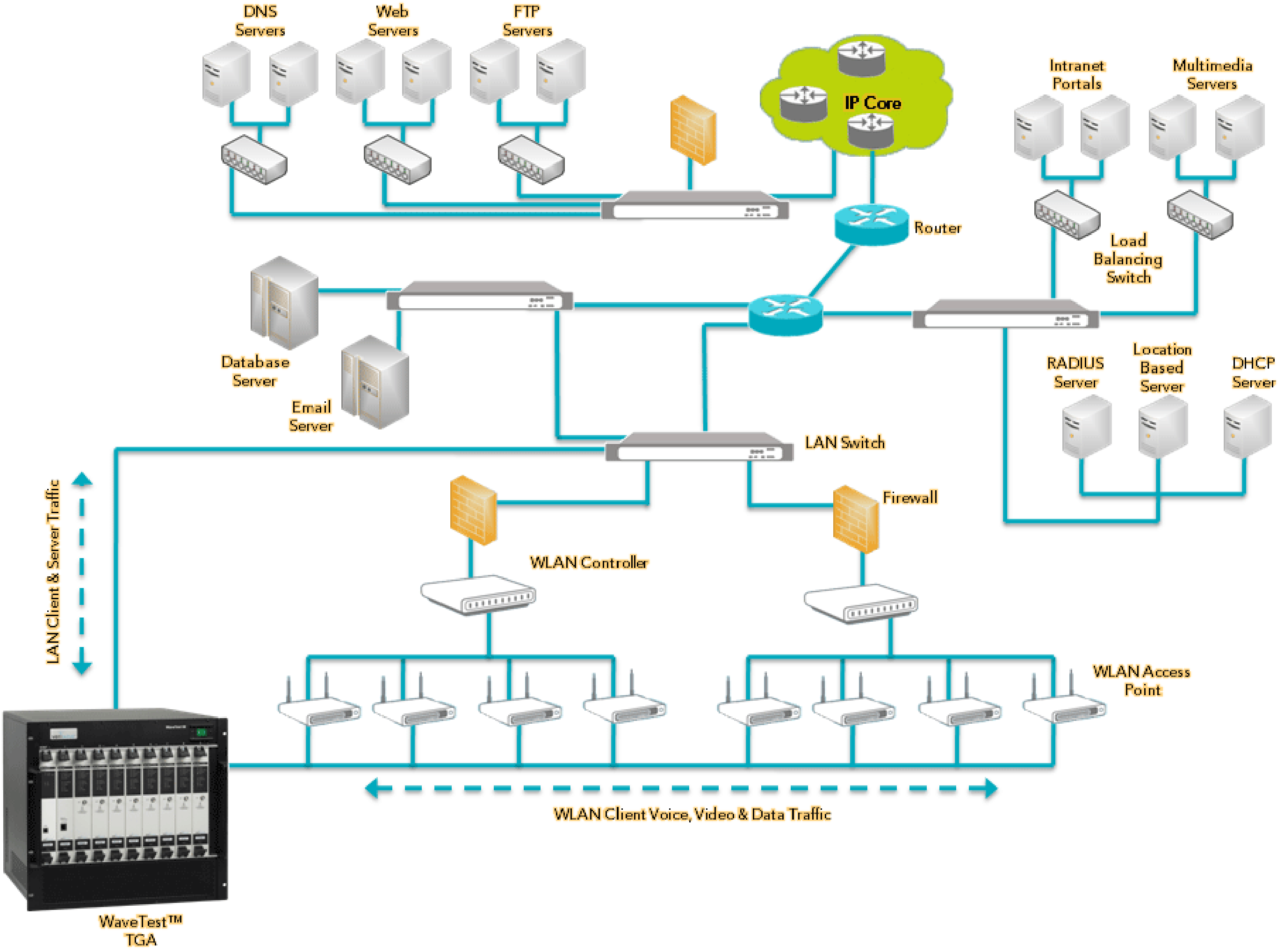

Fig 1: A typical network topology with WaveTest™ Client access

VeriWave Applications

A variety of test applications are available for the WaveTest platform. New applications are being added continuously, and the VeriWave website contains a current listing, as well as an updated version of this document. All of these applications provide a Command-Line-Interface (CLI) that can be integrated into an automation framework which will configure and manage both the SUT and the WaveTest system for fully automated execution and reporting.

Shown below is a list of applications available at the time this document was released. Some of the applications listed also have GUI interfaces available for driving the scripts, which allows for more manual operation and functional testing as desired. The results from these tests can be compared to other versions of the same SUT (as in previous SW and FW versions), as well as to competing products from other vendors.

The applications are arbitrarily classified for easier comprehension into five categories: Data Plane, Control Plane / Security, QoS, Mesh and Miscellaneous.

Data Plane

The following tests measure performance metrics and also expose issues relating to bandwidth, delay times and data integrity thereby allowing the tester to quantify, qualify and benchmark the data plane of the SUT.

Unicast Throughput

The Throughput test identifies the maximum rate at which the SUT can forward packets without loss.

This test determines the throughput rate by using a binary search algorithm. The test starts by offering the maximum theoretical or user-specified load to the SUT. Packet loss is then measured. If packet loss is detected the offered load (OLOAD) is cut in half. If there is no packet loss the OLOAD is doubled. This process continues until the difference between OLOAD values is less than the search resolution setting. The process is repeated for each frame size specified in the test.

The results show the throughput rates in frames per second for each frame size and the average throughput rate for all trials.

Running this test provides a baseline of the SUT's overall capability to handle traffic. It is a standard measure of performance as defined by draft-IEEE-802.11.2 (similar to RFC 2544 for wired networks). The throughput number can be easily compared to theoretical limits, at any given frame size, to other versions of the same SUT (as in previous SW and FW versions), as well as to competing products from other vendors. The throughput number provides the absolute maximum capacity of the SUT to pass traffic with no loss, and sets the bar for the most stringent applications. Successfully passing this test verifies that the SUT can consistently handle traffic loads without losing a single packet, a critical measure for delivery of high services requiring high QoS such as voice and video

Unicast Forwarding Rate

The Maximum Forwarding Rate test determines the maximum rate at which the system under test (SUT) receives and forwards frames regardless of frame loss. A binary search algorithm obtains a rate at which the SUT maximizes the number of forwarded frames.

The results show the maximum forwarding rates in frames per second for each frame size.

Running this test provides a baseline of the SUT's maximum capacity to pass traffic, regardless of frames lost in the process. It is a standard measure of performance as defined by draft-IEEE-802.11.2 (similar to RFC 2544 for wired networks). The unicast maximum forwarding rate can be easily compared to theoretical limits, at any given frame size, to other versions of the same SUT (as in previous SW and FW versions), as well as to competing products from other vendors. The unicast maximum forwarding rate offers a measure of the SUT switching data plane to handle extremely high loads. It is critical to run this test to verify the SUT's ability not only to handle high loads, but also to do so consistently across the entire spectrum of frame sizes.

Unicast Packet Loss

The Packet Loss test determines how many frames the system under test (SUT) can successfully forward at a variety of offered loads. Forwarding rate is measured by counting the number of packets that have been successfully received at the destination port(s) over the course of the test. Packet loss is calculated by taking the difference between the offered packets and the received packets. WaveApps™ presents to the SUT an intended load (ILOAD) and measures the response in terms of forwarding rate and loss packets. If you have multiple clients, the ILOAD is divided evenly between the clients sourcing traffic into the SUT. You can specify a variety of ILOAD conditions and the test produces the measured results for each ILOAD.

Running this test offers a convenient means to debug a SUT's behavior when abnormal packet loss is observed for a particular frame size or frame size range. An additional benefit is the ability to characterize the behavior of the system as the number of served clients increases, thus verifying that the SUT performs equally well as the number of users in increased. Unicast packet loss is a standard measure of performance as defined by draft-IEEE-802.11.2 (similar to RFC 2544 for wired networks). The unicast maximum forwarding rate can be compared to other versions of the same SUT (as in previous SW and FW versions), as well as to competing products from other vendors.

Unicast Latency

The Unicast latency test determines the latency of the system under test (SUT). The results show the latencies for each frame size as distributed into 16 latency buckets. It also shows the minimum, maximum, and average latencies for all the trials. The test presents the SUT with an intended load (ILOAD) and measures the time that it takes for frames to be forwarded through the SUT. The test compares the transmit timestamp for each frame with the receive timestamp for the corresponding frame. Frames are transmitted for a fixed period of time. The difference between the transmit time and the receive time is the latency. If you have multiple clients, the ILOAD is divided evenly between the clients sourcing traffic into the SUT. For accurate latency measurement, the ILOAD must be at a level that produces no frame loss. Use the Throughput test to determine the maximum ILOAD that can be achieved without frame loss.

Running this test provides a baseline of delay introduced by the SUT. This is a critical performance measure for any application, as high latency will cause unacceptable end-user experience especially in delay sensitive applications such as voice and video. An additional benefit is the ability to characterize the behavior of the system as the number of served clients increases, thus verifying that the SUT performs equally well as the number of users in increased. It is a standard measure of performance as defined by draft-IEEE-802.11.2 (similar to RFC 2544 for wired networks). The unicast latency be compared to other versions of the same SUT (as in previous SW and FW versions), as well as to competing products from other vendors.

TCP Goodput

The TCP Goodput test measures the number of TCP payload bytes per second that the system under test (SUT) can transfer between its ports and a variable maximum segment size (MSS). The TCP payload is the sum of the TCP segment bytes minus the TCP headers and options. The test associates clients with the SUT and generates unidirectional TCP traffic. The test iterates through each element in the TCP maximum segment size list.

Running this test provides a necessary measure to verify the SUT’s ability to efficiently handle stateful layer 4 traffic in conjunction with proper 802.11 MAC behavior. The TCP goodput can be compared to new and older software and hardware versions of the SUT, as well as for competitive product comparisons.

Control Plane

The following tests measure performance metrics and expose issues relating to roaming, client capacity, client-connection stress and intrusion detection/protection thereby allowing the tester to quantify, qualify and benchmark the control plane of the SUT.

Benchmark Roaming

The Roaming Benchmark tests the WLAN controller to determine the number of roams per unit of time the controller can support. The test determines the roam delay and packet loss at a particular roam rate with a given configuration using a predefined roaming pattern.

The test sends UDP packets from the Ethernet client to the roaming wireless clients. The roam rate and pattern are constant. After each roam operation, the test measures the time taken to roam and the number of data packets (from Ethernet to Wireless) lost during the roam. The test creates a report with the minimum, maximum and average roam delays for each test client, the number of roams performed, and the average number of packets lost per roam for each client.

Running this test provides a clear benchmark of the SUT's ability to handle a very large scale of roaming clients, each behaving independently of the other clients. The results offered by this test are invaluable in characterizing the SUT's behavior in a highly mobile environment, and thus a critical measure of its readiness for deployment in such an environment

Stress Association Database Capacity (Client Capacity)

The Maximum Client Capacity test measures the number of clients that are successfully created and pass traffic within a permissible loss tolerance. This test can exercise multiple APs. Each AP is sequentially tested. The maximum client capacity is calculated on a particular frame size and an intended load.

The test first attempts to associate a large number of clients, stopping when it fails to associate any more clients or reaches the value specified for Search Maximum. Once the upper limit is determined and the learning traffic is complete, traffic runs from the Ethernet client through the SUT to the wireless clients. At the end of the transmit duration, the frame loss rate for each client is calculated. If the frame loss rate falls below the acceptable loss tolerance, the maximum number of clients has been identified and the test terminates. If the frame loss rate is above the acceptable loss tolerance, then one client is disassociated and the test runs again. This is repeated until the maximum number of clients is identified.

This test offers a very important metric of any installed network – its ability to handle multiple clients. Unlike other connection tests that may validate on the SUT's ability to connect clients, this test actually sends traffic through these connections, thus verifiying that the SUT is not only able to connect the clients, but also let traffic pass through the network.

QoS

The following tests measure performance metrics and expose issues relating to VoIP call capacity, mobile VoIP call quality and QoS-based prioritization thereby allowing the tester to quantify, qualify and benchmark the QoS performance of the SUT.

VoIP QoS Service Capacity

The Service Capacity test measures the maximum number of voice calls of different types (G.711, G.729, and G.723) that can be sustained by the WLAN system at a specified minimum call quality (R-value). A background best-effort data traffic load can be specified along with the voice calls. This quantifies the total voice capacity of the WLAN system.

The Ethernet port sends non-voice, data background traffic to a non-voice wireless client, creating contention for the wireless bandwidth. The test increases the number of voice calls for each iteration as long as the service level criterion is met and computes the maximum number of high priority flows the SUT can support with acceptable performance.

The service level criterion is defined as a MOS (Mean Opinion Score) or R-Value, for each of the independent voice calls created by the test system. The user has broad control over the type of voice calls created (codec type, encryption type, etc.) as well as over the 802.11e/WMM or 802.1Q user priorities assigned to the voice calls.

This test is the only tool available to characterize a SUT's ability to handle mixed voice and data traffic while properly differentiating the various traffic types as per Layer 2 802.11e/ WMM and 802.1Q and/or Layer 3 TOS/DSCP priority settings.

VoIP Service Assurance

Measures the maximum level of best-effort data traffic load that can be presented to the WLAN system without causing the call quality of the applied voice traffic to drop below a minimum service level threshold. This quantifies the ability of the WLAN system to protect voice calls (uses WMM/802.11e, if supported by the WLAN system) from data traffic system.

The service level criterion is defined as a MOS (Mean Opinion Score) or R-Value, for each of the independent voice calls created by the test system. The user has broad control over the type of voice calls created (codec type, encryption type, etc.) as well as over the 802.11e or WMM user priorities assigned to the voice calls.

This test is the only tool available to characterize a SUT's ability to handle mixed voice and data traffic while properly differentiating the various traffic types as per 802.11e or WMM. The test provides a clear metric of how many concurrent voice calls a SUT can carry while providing proper voice / data differentiation.

VoIP Roaming

Measures call quality while roaming multiple handsets (voice calls of different types – G.711, G.729, and G.723) between APs in the WLAN system. Also assesses roaming delays and lost packets. The test supports WMM/802.11e operation. The user can select the voice codec type, number of voice clients and the roaming profile. The test offers the same reports as the Roaming Delay test along with an R-value per client graph.

Running this test is the only means to precisely measure the SUT's capability to handle dozens, or even hundreds, of asynchronous roaming events by voice clients in a repeatable way. The service restoration time, measured by this test, is a true measure of end-user experience, as a client roams from one AP to another. The results, presented as MOS (Mean Opinion Score) or R-Value, per client, offered by this test are invaluable in characterizing the SUT's behavior in a highly mobile environment, and thus a critical measure of its readiness for deployment in such an environment

Mesh

The mesh tests described below provide a complete view of the capability of a mesh network to handle hundreds of clients, the capacity of the mesh network, the expected quality of service and resiliency of the network, in the presence of controlled and repeatable backhaul link impairments producing interference and noise effects.

Mesh client capacity

The Mesh Client Capacity test identifies the maximum number of clients at which the Mesh Network can support a given SLA (Service Level Agreement). The SLA is defined by three parameters: Maximum packet loss, guaranteed throughput, and the maximum acceptable latency. Multiple iterations are used to find the maximum number.

If clients fail to connect, ARPs fail to complete, measured packet loss is greater than SLA Acceptable Loss, the offered load is less than SLA Minimum Throughput, or if any of the frames' latency exceeds the SLA Maximum Latency, then the iteration has failed.

This test uses a binary search algorithm to determine the result and it can be run with no backhaul impairment introduced, or with varying rates of backhaul impairments, defined by the user.

Mesh VoIP call capacity

This test works in a similar manner to the VoIP QoS Capacity test with an additional capability to configure different amount of background traffic load on each mesh node.

The report for this test is similar to the VoIP QoS capacity test with an additional graph that shows the max number of voice calls and amount of achieved background load per node in the mesh.

The test can be run with no backhaul impairment introduced, or with varying rates of backhaul impairments, defined by the user.

Mesh Throughput per hop

The Mesh Throughput per hop test is similar to the Unicast Throughput test, with the addition of reporting the throughput for each hop in the mesh network.

The test can be run with no backhaul impairment introduced, or with varying rates of backhaul impairments, defined by the user.

Mesh Forwarding Rate per hop

The Mesh Forwarding Rate per hop test is similar to the Unicast Forwarding rate test, with the addition of reporting the forwarding rate for each hop in the mesh network.

The test can be run with no backhaul impairment introduced, or with varying rates of backhaul impairments, defined by the user.

Mesh Latency per hop

The Mesh Latency per hop is similar to the Unicast Latency test, with the addition of reporting the latency for each hop in the mesh network.

The test can be run with no backhaul impairment introduced, or with varying rates of backhaul impairments, defined by the user

Mesh Backhaul Failover (Self-healing)

The mesh backhaul failover test utilizes the VeriWave system’s ability to carete precise impairments on the backhaul link (or links), using the 802.11 Backhaul Load and Obstruction Generator (BLOG). The BLOG allows the user to generate deterministic bit error rates (BERs) on 802.11 mesh backhaul link(s). This capability enables the user to control the exact amount of RF interference to be injected into the backhaul link(s) of a mesh network deployment configuration being tested in the test lab.

The mesh backhaul failover test measures the time to reroute packets in a mesh network when the backhaul link(s) is impaired. Additionally, throughput per hop, aggregate throughput, latency per hop, and aggregate latency can be measured. The BER can be varied during the course of a test to emulate to a real world scenario.

Miscellaneous

AAA Authentication Load

The AAA Authentication Load Test measures the capability of a WLAN controller and/or a RADIUS server to sustain a constant but very high authentication rate load of clients using complex security schemes such as EAP/TLS, PEAP etc.

Test-bed Configuration

For optimum performance and flexibility, each Access Point is directly connected to a WiFi WaveBlade with sufficient RF isolation techniques to ensure that the only signal available to load the Access Point is that coming from the WaveBlade. This is achieved through the use of RF enclosures for the Access Points, and high-quality RF cables.

The RF connection of the WBW1000 WiFi WaveBlade is typically connected directly to an RF enclosure through a 30 dB attenuator.   This is because an Access Point set to minimum output power will deliver a signal that is outside the dynamic range of the WiFi WaveBlade for optimum receive performance. Frame errors will result that have negative impact on tests. 802.11 receivers work best in the approximate range of -20 dBm to -50 dBm. Inserting a 20 dB attenuator between the WaveBlade output and the antenna connection of the Access Point ensures that the signal received by both the WaveBlade and the Access Point will be in this range.

The Access Point is connected via RF cable between the SMA bulkhead on the RF enclosure and the antenna connector. If the Access Point is designed such that two diversity antennas are active, a splitter can be used to connect the two antennas to the single SMA bulkhead connector of the RF enclosure. If the Access Point is one that contains radios in both the 802.11a and 802.11b/g bands, a splitter can be used to connect one WaveBlade to the two antenna ports, or separate single connections can be made between two WaveBlades and the two antenna ports.

All RF cables available through VeriWave are double shielded, which is highly recommended. This is to ensure that all RF signals being carried to and from the RF enclosures do not radiate to other Access Points nor pick up signals from nearby Access Points or clients that may be nearby and not a part of the test setup.

Ethernet connections made to each Access Point need to go into each RF enclosure through a filtered bulkhead connector. This is to ensure that the Ethernet cables do not carry RF signals in or out of the enclosure. Without this filtering, it would be possible for RF energy to be carried from on Access Point back to a switch or router, and carried into another Access Point inside another RF enclosure, resulting in the second Access Point deferring to what it interprets as traffic. Since 802.11 employs a carrier-sense medium access scheme, unintentional traffic being present can cause a significant drop in throughput, Console connections made to each Access Point also must be filtered at the bulkhead connector, for the same reason cited above.

Using the configuration described, a large number of Access Points may be placed in close proximity to each other, and any Access Point can be operated on any channel desired. Figure 2 below shows a typical rack installation which manages all connections, power and cooling for 8 access points plus the associated WaveTest chassis and WaveBlades in a single 19” rack. To expand the number of Access Points included in the test bed, the rack configuration in Figure 2 is simply duplicated.

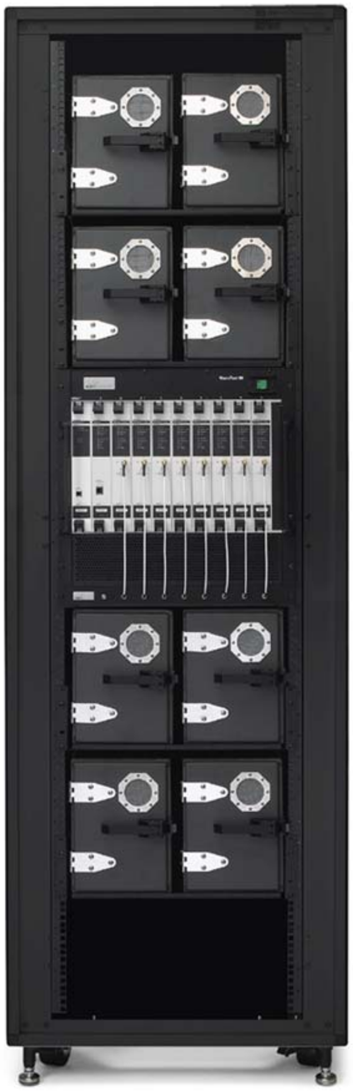

Fig 2 WaveTest™ 90 rack-mounted with APs in Isolation chambers

Test Case Profiles

A large number of test cases are listed and specified in the following section. Not all test cases are applicable to all WLAN SUTs. For example, tests performed on single APs cannot encompass roaming or mesh functions. In addition, specific areas of interest (such as QoS capability) require only a subset of the listed test cases.

To facilitate the rapid selection of the subset of test cases that are pertinent to a specific SUT configuration or a specific test area, this section utilizes *test profiles*. A test profile is a selected subset of test cases that address a narrowly defined area or requirement. Only those tests listed in the profile need to be performed in order to fully cover the functionality and performance aspects of the target area.

Four profiles are described here:

1) Single-AP Test Profile. This profile contains the test cases usable for standalone APs, or for testing the AP functionality within a SUT comprising APs connected to a WLAN controller. They are intended to be performed on a single AP.
2) Mesh Test Profile. This profile lists the test cases that must be applied to functional, performance and stress testing of mesh SUTs. Mesh SUTs must comprise two or more APs.
3) QoS Test Profile. The tests listed in this profile are applicable to determining the QoS capabilities of a device (single AP, SUT consisting of multiple APs and a controller, or mesh system).
4) Roaming Test Profile. The tests listed here are usable for determining the mobility performance and functional capabilities of a multi-AP SUT, typically comprising multiple lightweight APs and a WLAN controller (but also covering the case of multiple standalone APs interconnected by means of an Ethernet switch).

The profiles are provided in the form of tables. Each table contains the list of test case identifiers and the corresponding titles. The test case identifiers correspond to the test case listing in the next section.

Single-AP Test Profile

The following table lists the test cases applicable to single AP testing, whether standalone or controller-based.

AP Test Profile	
Functional Tests	
Basic Association	
ATC 001	Basic_80211a-mode_Association
ATC 002	Basic_80211bg-mode_Association
ATC 003	Basic_80211b-only-mode_Association
ATC 004	Basic_80211g-only-mode_Association
ATC 005	Mixed_80211ag-mode_Association
ATC 006	Mixed_80211ab-mode_Association
ATC 007	Mixed_80211bg-mode_Association
Security and DHCP	

AP Test Profile	
STC 001	Security_Baseline_Test
STC 002	Open_WEP40
STC 003	Open_WEP128
STC 004	Shared-Key_WEP40
STC 005	Shared-Key_WEP128
STC 006	DWEP_EAP-TLS
STC 007	DWEP_EAP-TTLS
STC 008	DWEP_PEAP-MSCHAPv2
STC 009	LEAP
STC 010	WPA_PSK_And_WPA_PSK_AES
STC 011	WPA_EAP-TLS_And_WPA_EAP-TLS_AES
STC 012	WPA_EAP-TTLS
STC 013	WPA_PEAP-MSCHAPv2_And_WPA_PEAP-MSCHAPv2_AES
STC 014	WPA_EAP-FAST
STC 015	WPA_LEAP
STC 016	WPA2_PSK_And_WPA2_PSK_TKIP
STC 017	WPA2_EAP-TLS_And_WPA2_EAP-TLS_TKIP
STC 018	WPA2_EAP-TTLS
STC 019	WPA2_PEAP-MSCHAPv2_And_WPA2_PEAP-MSCHAPv2_TKIP
STC 020	WPA2_EAP-FAST
STC 021	WPA2_LEAP
STC 022	Mixed_WPA_WPA2_PSK
STC 023	Mixed_WPA_PSK_WPA2_EAP-TLS
STC 024	Mixed_80211bg_WEP_WPA2_EAP-TLS
Basic Forwarding	
BTC 001	Upstream_80211g_Packet_Loss_Sweep
BTC 002	Downstream_80211g_Packet_Loss_Sweep
BTC 003	Bidirectional_80211g_Packet_Loss_Sweep
BTC 004	Upstream_80211a_Packet_Loss_Sweep
BTC 005	Downstream_80211a_Packet_Loss_Sweep
BTC 006	Bidirectional_80211a_Packet_Loss_Sweep
Power Save	
PTC 001	Power_Save_Baseline_CAM_Test
PTC 002	Power-Save_Legacy_PS_Poll
PTC 002	Power-Save_Legacy_Null_Frame
PTC 003	Power-Save_APSD
PTC 004	Power-Save_Mixed_1
PTC 005	Power-Save_Mixed_2
PTC 006	Power-Save_Mixed_3
PTC 007	Power-Save_Mixed_4
PTC 008	Power-Save_Mixed_5
QoS	
QTC 001	Basic_WMM_Association
QTC 002	Single_Station_Downstream_Fairness
QTC 003	Single_Station_Downstream_Priority
QTC 004	Multi_Station_Downstream_Fairness
QTC 005	Multi_Station_Downstream_Priority
QTC 006	Multi_Station_Upstream_Fairness
QTC 007	Multi_Station_Upstream_Priority
QTC 008	Legacy_QoS_Coexistence
QTC 009	Basic_Call_Admission_Control

AP Test Profile	
QTC 010	Call_Admission_Control_Denial_PHY_Rate
QTC 011	Call_Admission_Control_Denial_Utilization
QTC 012	Call_Admission_Control_Codec_Type
Performance Tests	
Client/Call Capacity	
CBTC 001	Max_Client_Capacity
CBTC 002	Max_Client_Capacity_DHCP
CBTC 003	Max_VoIP_Call_Capacity
CBTC 004	Max_VoIP_Call_Capacity_DHCP
Rate vs. Range	
CBTC 009	Rate_vs_Range_80211b
CBTC 010	Rate_vs_Range_80211g
CBTC 011	Rate_vs_Range_80211a
Throughput	
PBTC 001	Upstream_UDP_80211g_Throughput
PBTC 002	Downstream_UDP_80211g_Throughput
PBTC 003	Bidirectional_UDP_80211g_Throughput
PBTC 004	Upstream_UDP_80211a_Throughput
PBTC 005	Downstream_UDP_80211a_Throughput
PBTC 006	Bidirectional_UDP_80211a_Throughput
PBTC 007	Upstream_TCP_80211g_Throughput
PBTC 008	Downstream_TCP_80211g_Throughput
PBTC 009	Upstream_TCP_80211a_Throughput
PBTC 010	Downstream_TCP_80211a_Throughput
PBTC 011	Downstream_UDP_Power_Save_80211g_Throughput
PBTC 012	Downstream_UDP_Power_Save_80211a_Throughput
PBTC 013	Downstream_TCP_Power_Save_80211g_Throughput
PBTC 014	Downstream_TCP_Power_Save_80211a_Throughput
Packet Latency	
PBTC 015	Upstream_80211g_Packet_Latency
PBTC 016	Downstream_80211g_Packet_Latency
PBTC 017	Upstream_80211a_Packet_Latency
PBTC 018	Downstream_80211a_Packet_Latency
Packet Loss	
PBTC 019	Upstream_80211g_Packet_Loss
PBTC 020	Downstream_80211g_Packet_Loss
PBTC 021	Upstream_80211a_Packet_Loss
PBTC 022	Downstream_80211a_Packet_Loss
Maximum Forwarding Rate	
PBTC 023	Upstream_80211g_Max_Forwarding Rate
PBTC 024	Downstream_80211g_Max_Forwarding Rate
PBTC 025	Upstream_80211a_Max_Forwarding Rate
PBTC 026	Downstream_80211a_Max_Forwarding Rate
Maximum Stateful TCP Goodput	
PBTC 027	Upstream_80211g_Max_TCP_Goodput
PBTC 028	Downstream_80211g_Max_TCP_Goodput
PBTC 029	Upstream_80211a_Max_TCP_Goodput
PBTC 030	Downstream_80211a_Max_TCP_Goodput
Quality Of Service	
PBTC 059	VoIP_SLA_Assurance
Client Association Rate	

AP Test Profile	
PBTC 066	Max_Client_Association_Rate
PBTC 067	Max_Client_Association_Rate_DHCP
System/Stress Tests	
System Resiliency and Availability	
OFTC 004	AP_Reset_Recovery

Mesh Test Profile

The following table lists the test cases applicable to mesh SUTs.

Mesh Test Profile	
Functional Tests	
Basic Association	
ATC 001	Basic_80211a-mode_Association
ATC 002	Basic_80211bg-mode_Association
ATC 003	Basic_80211b-only-mode_Association
ATC 004	Basic_80211g-only-mode_Association
ATC 005	Mixed_80211ag-mode_Association
ATC 006	Mixed_80211ab-mode_Association
ATC 007	Mixed_80211bg-mode_Association
Security and DHCP	
STC 001	Security_Baseline_Test
STC 002	Open_WEP40
STC 003	Open_WEP128
STC 010	WPA_PSK_And_WPA_PSK_AES
STC 011	WPA_EAP-TLS_And_WPA_EAP-TLS_AES
STC 013	WPA_PEAP-MSCHAPv2_And_WPA_PEAP-MSCHAPv2_AES
STC 016	WPA2_PSK_And_WPA2_PSK_TKIP
STC 017	WPA2_EAP-TLS_And_WPA2_EAP-TLS_TKIP
STC 019	WPA2_PEAP-MSCHAPv2_And_WPA2_PEAP-MSCHAPv2_TKIP
Basic Forwarding	
BTC 001	Upstream_80211g_Packet_Loss_Sweep
BTC 002	Downstream_80211g_Packet_Loss_Sweep
BTC 003	Bidirectional_80211g_Packet_Loss_Sweep
Power Save	
PTC 001	Power_Save_Baseline_CAM_Test
PTC 003	Power-Save_APSD
PTC 004	Power-Save_Mixed_1
PTC 005	Power-Save_Mixed_2
PTC 006	Power-Save_Mixed_3
PTC 007	Power-Save_Mixed_4
PTC 008	Power-Save_Mixed_5
QoS	
QTC 001	Basic_WMM_Association
QTC 002	Single_Station_Downstream_Fairness
QTC 003	Single_Station_Downstream_Priority
QTC 004	Multi_Station_Downstream_Fairness
QTC 005	Multi_Station_Downstream_Priority

Mesh Test Profile	
QTC 006	Multi_Station_Upstream_Fairness
QTC 007	Multi_Station_Upstream_Priority
QTC 008	Legacy_QoS_Coexistence
QTC 009	Basic_Call_Admission_Control
QTC 013	Call_Admission_Control_Mesh
Performance Tests	
Client/Call Capacity	
CBTC 005	Max_Mesh_Client_Capacity
CBTC 006	Max_Mesh_Client_Capacity_DHCP
Rate vs. Range	
CBTC 009	Rate_vs_Range_80211b
CBTC 010	Rate_vs_Range_80211g
CBTC 011	Rate_vs_Range_80211a
Maximum Stateful TCP Goodput	
PBTC 027	Upstream_80211g_Max_TCP_Goodput
PBTC 028	Downstream_80211g_Max_TCP_Goodput
PBTC 029	Upstream_80211a_Max_TCP_Goodput
PBTC 030	Downstream_80211a_Max_TCP_Goodput
Roaming Performance	
PBTC 031	Roaming_Delay_80211g_Baseline
PBTC 032	Roaming_Delay_80211a_Baseline
PBTC 033	Roaming_Delay_80211g_Secure
PBTC 034	Roaming_Delay_80211a_Secure
PBTC 035	Roaming_Delay_80211g_DHCP
PBTC 036	Roaming_Delay_80211a_DHCP
Mesh Per-Hop and Aggregate Throughput	
PBTC 041	Upstream_UDP_Per-Hop_Throughput
PBTC 042	Downstream_UDP_Per-Hop_Throughput
PBTC 043	Bidirectional_UDP_Per-Hop_Throughput
PBTC 044	Upstream_TCP_Per-Hop_Throughput
PBTC 045	Downstream_TCP_Per-Hop_Throughput
PBTC 046	Bidirectional_TCP_Per-Hop_Throughput
PBTC 047	Upstream_UDP_Aggregate_Throughput
PBTC 048	Downstream_UDP_Aggregate_Throughput
PBTC 049	Bidirectional_UDP_Aggregate_Throughput
PBTC 050	Upstream_TCP_Aggregate_Throughput
PBTC 051	Downstream_TCP_Aggregate_Throughput
PBTC 052	Bidirectional_TCP_Aggregate_Throughput
Mesh Per-Hop and Aggregate Packet Latency	
PBTC 053	Upstream_UDP_Per-Hop_Latency
PBTC 054	Downstream_UDP_Per-Hop_Latency
PBTC 055	Upstream_UDP_Aggregate_Latency
PBTC 056	Downstream_UDP_Aggregate_Latency
Quality Of Service	
PBTC 059	VoIP_SLA_Assurance
PBTC 060	VoIP_Roaming_80211g
PBTC 061	VoIP_Roaming_80211a
PBTC 062	VoIP_Roaming_80211g_Accel
PBTC 063	VoIP_Roaming_80211a_Accel
System/Stress Tests	

Mesh Test Profile	
Traffic Variation	
TVTC 001	Data_Load_Isolation
TVTC 002	Roaming_Isolation_Network
TVTC 003	Roaming_Isolation_SSID
WiMix Tests	
WMTC 005	WiMix_Triple_Play_Unicast
WMTC 006	WiMix_Triple_Play_Multicast
Mesh Interference Effects	
IETC 001	Mesh_Interference_Reroute
IETC 002	Mesh_UDP_Throughput_Interference_Impact
IETC 003	Mesh_Latency_Interference_Impact
Traffic Stress	
TSTC 001	Traffic_Stress
Roaming Stress	
RSTC 001	Data_Roaming_Stress
RSTC 002	VoIP_Roaming_Stress
Connection Stress	
CSTC 001	Client_Connection_Stress
CSTC 002	Client_Connection_Data_Overload_Stress

QoS Test Profile

The following table lists the test cases applicable to testing the WMM/802.11e QoS and APSD Power Save capabilities of an AP or a SUT.

QoS Test Profile	
Functional Tests	
QoS Power Save	
PTC 001	Power_Save_Baseline_CAM_Test
PTC 003	Power-Save_APSD
PTC 005	Power-Save_Mixed_2
PTC 006	Power-Save_Mixed_3
PTC 007	Power-Save_Mixed_4
PTC 008	Power-Save_Mixed_5
QoS	
QTC 001	Basic_WMM_Association
QTC 002	Single_Station_Downstream_Fairness
QTC 003	Single_Station_Downstream_Priority
QTC 004	Multi_Station_Downstream_Fairness
QTC 005	Multi_Station_Downstream_Priority
QTC 006	Multi_Station_Upstream_Fairness
QTC 007	Multi_Station_Upstream_Priority
QTC 008	Legacy_QoS_Coexistence
QTC 009	Basic_Call_Admission_Control
QTC 010	Call_Admission_Control_Denial_PHY_Rate
QTC 011	Call_Admission_Control_Denial_Utilization
QTC 012	Call_Admission_Control_Codec_Type
Performance Tests	
Client/Call Capacity	
CBTC 003	Max_VoIP_Call_Capacity

QoS Test Profile	
CBTC 004	Max_VoIP_Call_Capacity_DHCP
Packet Latency	
PBTC 020	Upstream_80211g_Packet_Latency
PBTC 021	Downstream_80211g_Packet_Latency
PBTC 022	Upstream_80211a_Packet_Latency
PBTC 023	Downstream_80211a_Packet_Latency
Quality Of Service	
PBTC 059	VoIP_SLA_Assurance
PBTC 060	VoIP_Roaming_80211g
PBTC 061	VoIP_Roaming_80211a
PBTC 062	VoIP_Roaming_80211g_Accel
PBTC 063	VoIP_Roaming_80211a_Accel
System/Stress Tests	
WiMix Tests	
WMTC 005	WiMix_Triple_Play_Unicast
WMTC 006	WiMix_Triple_Play_Multicast
Roaming Stress	
RSTC 002	VoIP_Roaming_Stress

Roaming Test Profile

The following table lists the test cases applicable to testing the roaming functionality and performance of a multi-AP SUT.

Roaming Test Profile	
Performance Tests	
Roaming Performance	
PBTC 031	Roaming_Delay_80211g_Baseline
PBTC 032	Roaming_Delay_80211a_Baseline
PBTC 033	Roaming_Delay_80211g_Secure
PBTC 034	Roaming_Delay_80211a_Secure
PBTC 035	Roaming_Delay_80211g_DHCP
PBTC 036	Roaming_Delay_80211a_DHCP
PBTC 037	Roaming_Delay_80211g_Accel
PBTC 038	Roaming_Delay_80211a_Accel
PBTC 039	Roaming_Delay_80211g_MultiSSID
PBTC 040	Roaming_Delay_80211a_MultiSSID
Quality Of Service	
PBTC 060	VoIP_Roaming_80211g
PBTC 061	VoIP_Roaming_80211a
PBTC 062	VoIP_Roaming_80211g_Accel
PBTC 063	VoIP_Roaming_80211a_Accel
System/Stress Tests	
Traffic Variation	
TVTC 002	Roaming_Isolation_Network
TVTC 003	Roaming_Isolation_SSID
Roaming Stress	
RSTC 001	Data_Roaming_Stress
RSTC 002	VoIP_Roaming_Stress

Test Plan

Functional Verification

This section covers test cases that are essential to qualify the various functional modules supported by the SUT. Test case results either indicate that the specific functional module is functioning as expected, or indicates a failure condition that must be fixed before conducting more advanced testing.

Testing of Functions and Features

Verification of individual features during hardware and firmware development is important to ensure robust design implementation. Test methodologies applied should configure clients and traffic exactly as desired, run traffic in a controlled manner, record detailed statistics, and capture frame-level logfiles for analysis. Examples of basic features and functions that need to be verified on any WLAN equipment include:

- Operation at each PHY rate
- Maximum frame forwarding rate at multiple frame lengths
- Retransmission frequency, frame error rates
- Operation at various CWmin, CWmax, SIFS, DIFS, slot time and retry settings
- Power save mode
- Security methods and encryption selections
- Static IP and DHCP functionality
- Performance in the presence of media contention
- Performance at various client power levels
- Performance with various traffic types and QoS levels
- Performance with different channel models

Note that while the tests in this section are comprehensive, passing results on all of these individual functional test cases do not necessarily imply that the SUT is capable of operating in deployment conditions. The relevant performance, system and stress tests (as called out by the appropriate equipment profiles) must also be conducted in order to ensure that the SUT can be safely and effectively deployed.

Association

The following tests verify the general association functionality of the SUT. The tests span all valid operating channels as well as mixed-mode functioning (e.g., combinations of 2.4 GHz and 5 GHz channels). Successful completion of these tests indicates that the SUT is capable of being discovered and associated to by clients under various circumstances. Failure of any of these basic tests indicates a potential issue with client connnection capability in deployed networks and should be addressed before conducting any further tests.

The association tests are performed with different frame sizes, numbers of clients, and probe functionality (i.e., passive or active scanning AP discovery methods) to ensure that successful association can be achieved under many different client behaviors.

ATC 001 Basic_80211a-mode_Association

Title	Verify basic association on all channels in IEEE 802.11a mode
Purpose	Tests the SUT for basic support of IEEE 802.11a by performing association with one or more client stations on all valid 802.11a channels. Test traffic is sent from each associated client to the SUT in order to verify successful association.
SUT Feature(s) Tested	IEEE 802.11a client support
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the 802.11a band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Run test using IEEE 802.11a channels (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161) • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 1 and 10 clients • Run test with unicast active scan (probing), broadcast active scan (probing), and passive scan (no probing) client functionality
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the initial channel to channel 36 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address(es) 5. Set client probe behavior to broadcast probing before association 6. Create an Ethernet client group on the correct port(s) with the

	initial number of Ethernet clients set to 1 7. Set the initial number of Wi-Fi clients to 1 8. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 9. Set the ILOAD to 100 frames/second 10. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 4 to 13 with 10 clients 15. Repeat steps 4 to 14 with channels 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161 16. Repeat steps 4 to 15 with unicast probing before association 17. Repeat steps 4 to 15 with no probing before association (passive scanning)
Test Priority	Mandatory
Test Type	General
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss on all 802.11a-band channels and under all test conditions.

ATC 002 Basic_80211bg-mode_Association

Title	Verify basic association on all channels in IEEE 802.11g mode
Purpose	Tests the SUT for basic support of IEEE 802.11g by performing association with one or more client stations on all valid 802.11g channels. Test traffic is sent from each associated client to the SUT in order to verify successful association.
SUT Feature(s) Tested	IEEE 802.11g client support
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the 802.11g band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e.,

	connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Run test using IEEE 802.11g channels (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11) • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 1 and 10 clients • Run test with unicast active scan (probing), broadcast active scan (probing), and passive scan (no probing) client functionality
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the initial channel to channel 1 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address(es) 5. Set client probe behavior to broadcast probing before association 6. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 7. Set the initial number of Wi-Fi clients to 1 8. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 9. Set the ILOAD to 100 frames/second 10. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 4 to 13 with 10 clients 15. Repeat steps 4 to 14 with channels 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 16. Repeat steps 4 to 15 with unicast probing before association 17. Repeat steps 4 to 15 with no probing before association (passive scanning)
Test Priority	Mandatory
Test Type	General
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss on all 802.11g-

	band channels and under all test conditions.

ATC 003 Basic_80211b-only-mode_Association

Title	Verify basic association on all channels for IEEE 802.11b clients
Purpose	Tests the SUT for basic support of IEEE 802.11b by performing association with one or more 802.11b-only client stations on all valid 802.11b channels. Test traffic is sent from each associated client to the SUT in order to verify successful association.
SUT Feature(s) Tested	IEEE 802.11b client support
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 11Mbps and ensure that either b-only or b/g operation is selected, if necessary • Set client flow and connection PHY rates to 11 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Run test using IEEE 802.11b channels (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11) • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 1 and 10 clients • Run test with unicast active scan (probing), broadcast active scan (probing), and passive scan (no probing) client functionality
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the initial channel to channel 1 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address(es), and also configure the clients to 802.11b-only mode with 11 Mb/s flow and connection PHY rates 5. Set client probe behavior to broadcast probing before association

	6. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 7. Set the initial number of Wi-Fi clients to 1 8. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 9. Set the ILOAD to 100 frames/second 10. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 4 to 13 with 10 clients 15. Repeat steps 4 to 14 with channels 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 16. Repeat steps 4 to 15 with unicast probing before association 17. Repeat steps 4 to 15 with no probing before association (passive scanning)
Test Priority	High
Test Type	General
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss on all 802.11b-band channels and under all test conditions.

ATC 004 Basic_80211g-only-mode_Association

Title	Verify basic association on all channels for IEEE 802.11g-only clients, while blocking IEEE 802.11b-only clients
Purpose	Tests the SUT for basic support of IEEE 802.11b by performing association with one or more 802.11g-only client stations on all valid 2.4 GHz channels, but blocking all 802.11b-only client stations. Test traffic is sent from each associated client to the SUT in order to verify successful association of 802.11g-only clients and complete failure of 802.11b-only clients. This test is only usable with SUTs that have the capability to refuse admission of 802.11b-only clients.
SUT Feature(s) Tested	IEEE 802.11g-only client support with a non-mixed BSS
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables

	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps, and ensure that g-only operation is selected, if possible • Set client flow and connection PHY rates to 11 Mb/s and 1 Mb/s respectively for the b-only client, and to 54 Mb/s and 6 Mb/s respectively for the g-only client. • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Run test using IEEE 802.11g channels (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11) • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 1 and 10 clients • Run test with unicast active scan (probing), broadcast active scan (probing), and passive scan (no probing) client functionality
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the initial channel to channel 1 4. Select SSID and configure two client groups for open authentication with no encryption and static IP address(es); set one group of clients to use 802.11g-only mode (set flow and connection PHY rates to 54 Mb/s and 6 Mb/s respectively) and set the other group of clients to use 802.11b-only mode (select 802.11b-only Mode, set the flow PHY rate to 11 Mb/s, and set the connection PHY rate to 6 Mb/s) 5. Set client probe behavior to broadcast probing before association 6. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 7. Set the initial number of Wi-Fi clients to 1 per group 8. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 9. Set the ILOAD to 100 frames/second 10. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 4 to 13 with 10 clients per group 15. Repeat steps 4 to 14 with channels 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

	16. Repeat steps 4 to 15 with unicast probing before association 17. Repeat steps 4 to 15 with no probing before association (passive scanning)
Test Priority	High
Test Type	General
Pass/Fail Criteria	The 802.11g-only Wi-Fi client(s) should successfully associate with the SUT. The 802.11b-only Wi-Fi client(s) should be refused association by the SUT. (NOTE: no traffic will be passed.)

ATC 005 Mixed_80211ag-mode_Association

Title	Verify concurrent association of mixed IEEE 802.11a and IEEE 802.11g clients
Purpose	Tests the SUT for support of a mixed IEEE 802.11a and 802.11g client environment by performing association with one or more 802.11g client stations and one or more 802.11a client stations. Test traffic is sent from each associated client to the SUT in order to verify successful association.
SUT Feature(s) Tested	Mixed IEEE 802.11a & 802.11g client support
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 2xWi-Fi Waveblades and 1xEthernet Waveblade • SUT with AP(s) set up to operate in the IEEE 802.11b/g as well as 802.11a bands (note: if SUT supports it, a single AP can be used simultaneously in both bands) • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlades to the SUT via RF cables; one WaveBlade must be connected to the 802.11b/g port and another to the 802.11a port of the SUT • Configure the SUT to open authentication mode on all APs • Set Basic Rate Set on both the 802.11b/g and 802.11a ports/APs of SUT to 6Mbps, 12Mbps, 24Mbps; if possible disable association by 802.11b-only clients to SUT • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Run test using combinations of three IEEE 802.11b/g channels (1, 6, 11) and three IEEE 802.11a channels (36, 64, 161) • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 1 and 10 clients per port • Run test with unicast active scan (probing), broadcast active scan (probing), and passive scan (no probing) client

	functionality
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the two test ports (i.e., APs/ports in SUT corresponding to the two WaveBlades) to use for the test; set the initial 802.11a channel to channel 36 and the initial 802.11g channel to channel 1 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address(es); ensure that 802.11b-only mode is turned off 5. Set client probe behavior to broadcast probing before association 6. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 7. Set the initial number of Wi-Fi clients to 1 per port 8. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 9. Set the ILOAD to 100 frames/second 10. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 4 to 13 with 10 clients 15. Repeat steps 4 to 14 with 802.11g channels 6, 11 16. Repeat steps 4 to 15 with 802.11a channels 64, 161 17. Repeat steps 4 to 16 with unicast probing before association 18. Repeat steps 4 to 16 with no probing before association (passive scanning)
Test Priority	High
Test Type	General
Pass/Fail Criteria	All the Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions.

ATC 006 Mixed_80211ab-mode_Association

Title	Verify concurrent association of mixed IEEE 802.11a and IEEE 802.11b clients

Purpose	Tests the SUT for support of a mixed IEEE 802.11a and 802.11b client environment by performing association with one or more 802.11b client stations and one or more 802.11a client stations. Test traffic is sent from each associated client to the SUT in order to verify successful association.
SUT Feature(s) Tested	Mixed IEEE 802.11a & 802.11b client support
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 2xWi-Fi Waveblades and 1xEthernet Waveblade • SUT with AP(s) set up to operate in the IEEE 802.11b as well as 802.11a bands (note: if SUT supports it, a single AP can be used simultaneously in both bands) • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlades to the SUT via RF cables; one WaveBlade must be connected to the 802.11b port and another to the 802.11a port of the SUT • Configure the SUT to open authentication mode on all APs • Set Basic Rate Set on the 802.11b port/AP of the SUT to 1Mbps, 2Mbps, 5.5Mbps and 11Mbps, and the 802.11a port/AP to 6Mbps, 12Mbps, 24Mbps • Set 802.11b-client flow PHY rate to 11 Mb/s and management (i.e., connection) PHY rate to 1 Mb/s; set 802.11a-client flow PHY rate to 54 Mb/s and management PHY rate to 1 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Run test using combinations of three IEEE 802.11b channels (1, 6, 11) and three IEEE 802.11a channels (36, 64, 161) • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 1 and 10 clients per port • Run test with unicast active scan (probing), broadcast active scan (probing), and passive scan (no probing) client functionality
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the two test ports (i.e., APs/ports in SUT corresponding to the two WaveBlades) to use for the test; set the initial 802.11a channel to channel 36 and the initial 802.11b channel to channel 1 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address(es); on client(s) assigned to the 802.11b port, enable 802.11b-only mode 5. Set client probe behavior to broadcast probing before association

	6. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 7. Set the initial number of Wi-Fi clients to 1 per port 8. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 9. Set the ILOAD to 100 frames/second 10. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 4 to 13 with 10 clients 15. Repeat steps 4 to 14 with 802.11b channels 6, 11 16. Repeat steps 4 to 15 with 802.11a channels 64, 161 17. Repeat steps 4 to 16 with unicast probing before association 18. Repeat steps 4 to 16 with no probing before association (passive scanning)
Test Priority	High
Test Type	General
Pass/Fail Criteria	All the Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions.

ATC 007 Mixed_80211bg-mode_Association

Title	Verify concurrent association of mixed IEEE 802.11b and IEEE 802.11g clients in the same BSS
Purpose	Tests the SUT for support of a mixed IEEE 802.11a and 802.11b (legacy) client environment by performing association with one or more 802.11g client stations and one or more 802.11b client stations. Test traffic is sent from each associated client to the SUT in order to verify successful association.
SUT Feature(s) Tested	Mixed IEEE 802.11b & 802.11g client support
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblades and 1xEthernet Waveblade • SUT with AP set up to operate in the 2.4 GHz bands (note: more than one AP may be used, but each AP must be presented with a mixture of 802.11b and 802.11g clients) • Static IP addressing configured in the SUT

Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to open authentication mode • Set Basic Rate Set on the port/AP of SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set 802.11b client flow PHY rate to 11 Mb/s and management (i.e., connection) PHY rate to 1 Mb/s; set 802.11g client flow PHY rate to 54 Mb/s and management PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Run test using IEEE 802.11b/g channels (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11) • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 1 and 10 clients per port • Run test with unicast active scan (probing), broadcast active scan (probing), and passive scan (no probing) client functionality
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port to use for the test and set the initial channel to channel 1 4. Select SSID and configure two sets of clients on this SSID with open authentication with no encryption, and static IP addresses; one set is configured to use 802.11g rates (54 Mb/s and 6 Mb/s), and the other set is configured to use 802.11b rates (11 Mb/s and 1 Mb/s) with 802.11b-only mode being set on the latter 5. Set client probe behavior to broadcast probing before association 6. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 7. Set the initial number of Wi-Fi clients to 1 8. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 9. Set the ILOAD to 100 frames/second 10. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 6 to 13 with 10 clients

	15. Repeat steps 6 to 14 with channels 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 16. Repeat steps 6 to 15 with unicast probing before association 17. Repeat steps 6 to 15 with no probing before association (passive scanning)
Test Priority	Mandatory
Test Type	General
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss on all channels and under all test conditions.

ATC 008 Basic_80211n-mode_Association

Title	Verify basic association of HT mode clients under different channel conditions
Purpose	Tests the SUT for basic support of IEEE 802.11n HT mode by performing association with one or more client stations. Test traffic is sent from each associated client to the SUT in order to verify successful association.
SUT Feature(s)	IEEE 802.11n HT mode support
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • Static IP addressing configured in the SUT
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to MCS 7 and management (i.e., connection) PHY rate to 6Mbps • For the HT client set Guard Interval mode to LGI • For the HT client set Channel Width to 20MHz • For the HT client set the HT mode to mixed • Set Client Channel Model to use as "Bypass" • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations

	• Run test using IEEE 802.11g channel1 and/or IEEE 802.11a channels 36 • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 1 and 10 clients • Run test with unicast active scan (probing) client functionality
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the initial channel to channel 1 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address(es) 5. Set client probe behavior to broadcast probing before association 6. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 7. Set the initial number of Wi-Fi clients to 1 8. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 9. Set the ILOAD to 100 frames/second 10. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 4 to 13 with 10 clients 15. Repeat steps 4 to 14 using another Channel Model. Select any one channel model to use from A to F.
Test Priority	Mandatory
Test Type	General
Pass/Fail Criteria	The HT client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss on all 802.11g and/or 802.11a band channels and under all test conditions.

ATC 009 Mixed_80211n-and-Legacy_Association

Title	Verify concurrent association of mixed IEEE 802.11n HT and non-HT mode clients
Purpose	Tests the SUT for support of a mixed IEEE 802.11n HT and non-HT client environment by performing association with one or

	more HT-mode client stations and one or more non-HT-mode client stations. Test traffic is sent from each associated client to the SUT in order to verify successful association.
SUT Feature(s)	Mixed IEEE 802.11n HT mode & non-HT mode client support
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • Static IP addressing configured in the SUT
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use ports A and B on Wi-Fi WaveBlade if SUT supports just 2 antenna ports o Use ports A, B and C on Wi-Fi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set HT client flow PHY rate to MCS 15 and management (i.e., connection) PHY rate to 6Mbps • For the HT client set Guard Interval mode to LGI • For the HT client set Channel Width to 20MHz • For the HT client set the HT mode to mixed • Set Channel Model to use as "Bypass" • Set non-HT client flow PHY rate to 54Mbps and management (i.e., connection) PHY rate to 6Mbps • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations for each client • Run test using IEEE 802.11g channel 1and/or IEEE 802.11a channel 36 • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 2 and 10 clients with equal number of HT and non-HT clients • Run test with broadcast active scan (probing)
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the initial channel to channel 1 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address(es) 5. Set client probe behavior to broadcast probing before

	association 6. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 2 7. Set the initial number of Wi-Fi clients to 2 8. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 9. Set the ILOAD to 100 frames/second 10. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 4 to 13 with 10 clients
Test Priority	Mandatory
Test Type	General
Pass/Fail Criteria	Both HT and non-HT clients should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss on all 802.11g and/or 802.11a band channels and under all test conditions.

Security and DHCP

Network security is a major enterprise WLAN concern and requires comprehensive testing. Most enterprise WLANs use strong authentication and encryption, usually server-based (i.e., RADIUS) to differentiate and centrally control user access and privileges. WPA and WPA2 (IEEE 802.11i) are the key wireless-specific security protocols that mediate between clients and authentication servers. The common authentication protocols used in wireless networks in the enterprise include PSK, EAP-PEAP/MS-CHAPv2, EAP-TTLS-GTC, LEAP, EAP-FAST, and EAP-TLS. DHCP is a closely related function - without security keys being properly negotiated and installed, DHCP will not complete, or will complete incorrectly.

The following tests verify that the SUT is capable of supporting all the standard enterprise-class security modes with different numbers of clients and DHCP modes. Separate iterations verify that both passive-scan and active-scan methods can be used by clients in order to acquire the necessary BSS and security information. The tests are assumed to be performed using the 2.4 GHz band (with an 802.11b/g SUT port) but can be applied to the 5 GHz band if desired, by changing the operating channel(s).

STC 001 Security_Baseline_Test

Title	Record baseline open authentication behavior with no encryption
Purpose	Test the SUT for connectivity to WLAN clients using open authentication support without encryption. This test serves as a baseline for the subsequent secure connectivity tests. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment.
SUT Feature(s) Tested	Baseline insecure connectivity, DHCP with no security
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to open authentication mode with no cipher, and to allow clients to use static IP addresses as well as DHCP • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to open authentication with no encryption 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1

	8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Mandatory
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 002 Open_WEP40

Title	Verify support of WEP security with open authentication using 40-bit keys
Purpose	Test the SUT for connectivity to WLAN clients using open authentication support with WEP encryption and 40-bit key widths. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	WEP-40 with Open authentication, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to open authentication mode with WEP-40 encryption, and to allow clients to use static IP addresses as well as DHCP

	• Configure 40-bit hex encryption key in SUT to ‘3031323334’ • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to WEP-Open with 40-bit hex key of ‘3031323334’ • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead

	of static IP addresses
Test Priority	Low
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 003 Open_WEP128

Title	Verify support of WEP security with open authentication using 128-bit keys
Purpose	Test the SUT for connectivity to WLAN clients using open authentication support with WEP encryption and 128-bit key widths. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters. NOTE: 128-bit keys are sometimes referred to as 104-bit keys
SUT Feature(s) Tested	WEP-128 with Open authentication, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to open authentication mode with WEP-40 encryption, and to allow clients to use static IP addresses as well as DHCP • Configure 128-bit hex encryption key in SUT to '30313233343536373839303132' • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to WEP-Open with 128-bit hex key of '30313233343536373839303132' • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security

	parameters - Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Low
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 004 Shared-Key_WEP40

Title	Verify support of WEP security with shared-key authentication using 40-bit keys

Purpose	Test the SUT for connectivity to WLAN clients using shared-key authentication support with WEP encryption and 40-bit key widths. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	WEP-40 with Shared-key authentication, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to shared-key authentication mode with WEP-40 encryption, and to allow clients to use static IP addresses as well as DHCP • Configure 40-bit hex encryption key in SUT to ‘3031323334’ • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to WEP-Shared with 40-bit hex key of ‘3031323334’ • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the

	initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Low
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 005 Shared-Key_WEP128

Title	Verify support of WEP security with shared-key authentication using 128-bit keys
Purpose	Test the SUT for connectivity to WLAN clients using open authentication support with WEP encryption and 128-bit key widths. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters. NOTE: 128-bit keys are sometimes referred to as 104-bit keys
SUT Feature(s) Tested	WEP-128 with Shared-key authentication, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables

	• Configure the SUT to shared-key authentication mode with WEP-40 encryption, and to allow clients to use static IP addresses as well as DHCP • Configure 128-bit hex encryption key in SUT to '30313233343536373839303132' • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to WEP-Shared with 128-bit hex key of '30313233343536373839303132' • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients

	16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Low
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 006 DWEP_EAP-TLS

Title	Verify support of Dynamic WEP security mode with EAP/TLS network authentication
Purpose	Test the SUT for connectivity to WLAN clients using EAP/TLS authentication with Dynamic WEP encryption (40-bit) and key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	DWEP, EAP/TLS with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for EAP/TLS support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support WEP encryption with EAP/TLS network authentication and DWEP key management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with valid root, client and CA certificates and private key, plus user login name of ‘anonymous’ and password of ‘whatever’ • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to DWEP-EAP-TLS with appropriate certificates, plus login name and password of ‘anonymous’ and ‘whatever’ respectively • Set offered test traffic load to 100 frames/second

	• Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Low
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 007 DWEP_EAP-TTLS

Title	Verify support of Dynamic WEP security mode with EAP/TTLS-GTC network authentication
Purpose	Test the SUT for connectivity to WLAN clients using EAP/TTLS-GTC authentication with Dynamic WEP encryption (40-bit) and key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	DWEP, EAP/TTLS-GTC with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for EAP/TTLS-GTC support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support WEP encryption with EAP/TTLS-GTC network authentication and DWEP key management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with valid root certificate, anonymous ID of ‘anonymous’, and user login name of ‘anonymous’ and password of ‘whatever’ • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to DWEP-EAP-TTLS-GTC with appropriate root certificate, plus anonymous ID, login name and password of ‘anonymous,’ ‘anonymous,’ and ‘whatever’ respectively • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite

	3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Low
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 008 DWEP_PEAP-MSCHAPv2

Title	Verify support of Dynamic WEP security mode with PEAP/MSCHAPv2 network authentication
Purpose	Test the SUT for connectivity to WLAN clients using PEAP/MSCHAPv2 authentication with Dynamic WEP encryption (40-bit) and key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	DWEP, PEAP/MSCHAPv2 with RADIUS, DHCP

Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for PEAP/MSCHAPv2 support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support WEP encryption with PEAP/MSCHAPv2 network authentication and DWEP key management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with valid root certificate, plus user login name of 'anonymous' and password of 'whatever' and anonymous ID of 'anonymous' • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to DWEP-PEAP-MSCHAPv2 with root certificate, plus user login name of 'anonymous' and password of 'whatever' and anonymous ID of 'anonymous' • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1

	8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Low
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 009 LEAP

Title	Verify support of LEAP network authentication (with WEP encryption)
Purpose	Test the SUT for connectivity to WLAN clients using LEAP authentication, encryption (WEP, 40-bit) and key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	LEAP/WEP with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for LEAP support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support LEAP encryption and network authentication, and to allow clients to use static IP addresses

	as well as DHCP • Configure RADIUS server with user login name of 'anonymous' and password of 'whatever' • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to LEAP with login name and password of 'anonymous' and 'whatever' respectively • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning)

	17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Medium
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 010 WPA_PSK_And_WPA_PSK_AES

Title	Verify support of WPA-PSK security mode (WPA key management, TKIP or AES encryption, PSK authentication)
Purpose	Test the SUT for connectivity to WLAN clients using WPA-PSK security mode and TKIP or AES encryption. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	WPA-PSK, TKIP, AES, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to support both TKIP and AES encryption with WPA key management and PSK authentication, with shared secret set to 'whatever', and to allow clients to use static IP addresses as well as DHCP • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with client security method set to WPA-PSK and WPA-PSK-AES, with shared secret set to 'whatever' • Run test with 1 and 10 clients using the same security parameters

	• Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above, starting with WPA-PSK 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses 18. Repeat steps 4 to 17 with WPA-PSK-AES used as the security mode
Test Priority	Mandatory for WPA-PSK; Medium for WPA-PSK-AES
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 011 WPA_EAP-TLS_And_WPA_EAP-TLS_AES

Title	Verify support of WPA security mode with EAP/TLS network

	authentication
Purpose	Test the SUT for connectivity to WLAN clients using EAP/TLS authentication with TKIP or AES encryption and WPA key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	TKIP, AES, WPA, EAP/TLS with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for EAP/TLS support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support both TKIP and AES encryption with EAP/TLS network authentication and WPA key management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with valid root, client and CA certificates and private key, plus user login name of ‘anonymous’ and password of ‘whatever’ • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with client security method set to WPA-EAP-TLS and WPA-EAP-TLS-AES, with shared secret set to ‘whatever’, plus login name and password of ‘anonymous’ and ‘whatever’ respectively • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1

	4. Select SSID and configure the client(s) to use security parameters as indicated above, starting with WPA-EAP-TLS 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses 18. Repeat steps 4 to 17 with WPA-EAP-TLS-AES used as the security mode
Test Priority	Mandatory for WPA-EAP-TLS; Medium for WPA-EAP-TLS-AES
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 012 WPA_EAP-TTLS

Title	Verify support of WPA security mode with EAP/TTLS-GTC network authentication
Purpose	Test the SUT for connectivity to WLAN clients using EAP/TTLS-GTC authentication with TKIP encryption and WPA key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	TKIP, WPA, EAP/TTLS-GTC with RADIUS, DHCP

Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for EAP/TTLS-GTC support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support TKIP encryption with EAP/TTLS-GTC network authentication and WPA key management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with valid root certificate, anonymous ID of 'anonymous', and user login name of 'anonymous' and password of 'whatever' • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to WPA-EAP-TTLS-GTC with appropriate root certificate, plus anonymous ID, login name and password of 'anonymous,' 'anonymous,' and 'whatever' respectively • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1

	8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Mandatory
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 013 WPA_PEAP-MSCHAPv2_And_WPA_PEAP-MSCHAPv2_AES

Title	Verify support of WPA security mode with PEAP/MSCHAPv2 network authentication
Purpose	Test the SUT for connectivity to WLAN clients using PEAP/ MSCHAPv2 authentication with TKIP or AES encryption and WPA key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	TKIP, AES, WPA, PEAP/MSCHAPv2 with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for PEAP/MSCHAPv2 support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support both TKIP and AES encryption with PEAP/ MSCHAPv2 network authentication and WPA key

	management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with valid root certificate, plus user login name of ‘anonymous’ and password of ‘whatever’ and anonymous ID of ‘anonymous’ • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with client security mode set to WPA-PEAP-MSCHAPv2 or WPA-PEAP-MSCHAPv2-AES, with a root certificate, plus user login name of ‘anonymous’ and password of ‘whatever’ and anonymous ID of ‘anonymous’ • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above, starting with WPA-PEAP-MSCHAPv2 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes

	14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses 18. Repeat steps 4 to 17 with WPA-PEAP-MSCHAPv2-AES used as the security mode
Test Priority	Mandatory for WPA-PEAP-MSCHAPv2; Medium for WPA-PEAP-MSCHAPv2-AES
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 014 WPA_EAP-FAST

Title	Verify support of WPA security mode with EAP/FAST network authentication
Purpose	Test the SUT for connectivity to WLAN clients using EAP/FAST authentication with TKIP encryption and WPA key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	TKIP, WPA, EAP/FAST with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for EAP/FAST support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support TKIP encryption with EAP/FAST network authentication and WPA key management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with user login name of ‘anonymous’ and password of ‘whatever’ • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e.,

	connection) PHY rate to 6 Mb/s • Set client security method to WPA-EAP-FAST with login name and password of ‘anonymous,’ and ‘whatever’ respectively • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	High
Test Type	Authentication

Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 015 WPA_LEAP

Title	Verify support of WPA security with LEAP network authentication
Purpose	Test the SUT for connectivity to WLAN clients using LEAP authentication, TKIP encryption, and WPA key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	WPA, TKIP, LEAP with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for LEAP support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support TKIP encryption and LEAP network authentication and WPA key management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with user login name of 'anonymous' and password of 'whatever' • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to WPA-LEAP with login name and password of 'anonymous' and 'whatever' respectively • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application

	2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Low
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 016 WPA2_PSK_And_WPA2_PSK_TKIP

Title	Verify support of WPA2-PSK security mode (WPA2 key management, TKIP or AES encryption, PSK authentication)
Purpose	Test the SUT for connectivity to WLAN clients using WPA-PSK security mode and AES or TKIP encryption. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.

SUT Feature(s) Tested	WPA2-PSK, AES, TKIP, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to support both TKIP and AES encryption with WPA2 key management and PSK authentication, with shared secret set to 'whatever', and to allow clients to use static IP addresses as well as DHCP • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with client security method set to WPA2-PSK and WPA2-PSK-TKIP, with shared secret set to 'whatever' • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above, starting with WPA2-PSK 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second

	11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses 18. Repeat steps 4 to 17 with WPA2-PSK-TKIP used as the security mode
Test Priority	Mandatory for WPA2-PSK; Medium for WPA2-PSK-TKIP
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 017 WPA2_EAP-TLS_And_WPA2_EAP-TLS_TKIP

Title	Verify support of WPA2 security mode with EAP/TLS network authentication
Purpose	Test the SUT for connectivity to WLAN clients using EAP/TLS authentication with AES or TKIP encryption and WPA2 key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	TKIP, AES, WPA2, EAP/TLS with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for EAP/TLS support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support both TKIP and AES encryption with EAP/TLS network authentication and WPA2 key management, and to allow clients to use static IP addresses as well as DHCP

	• Configure RADIUS server with valid root, client and CA certificates and private key, plus user login name of ‘anonymous’ and password of ‘whatever’ • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with client security method set to WPA2-EAP-TLS and WPA2-EAP-TLS-TKIP, with shared secret set to ‘whatever’, plus login name and password of ‘anonymous’ and ‘whatever’ respectively • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above, starting with WPA2-EAP-TLS 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients

	16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses 18. Repeat steps 4 to 17 with WPA2-EAP-TLS-TKIP used as the security mode
Test Priority	Mandatory for WPA2-EAP-TLS; Medium for WPA2-EAP-TLS-TKIP
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 018 WPA2_EAP-TTLS

Title	Verify support of WPA2 security mode with EAP/TTLS-GTC network authentication
Purpose	Test the SUT for connectivity to WLAN clients using EAP/TTLS-GTC authentication with AES encryption and WPA2 key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	AES, WPA2, EAP/TTLS-GTC with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for EAP/TTLS-GTC support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support AES encryption with EAP/TTLS-GTC network authentication and WPA2 key management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with valid root certificate, anonymous ID of ‘anonymous’, and user login name of ‘anonymous’ and password of ‘whatever’ • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to WPA2-EAP-TTLS-GTC with appropriate root certificate, plus anonymous ID, login name

	and password of 'anonymous,' 'anonymous,' and 'whatever' respectively • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 1. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Mandatory
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test

	conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 019 WPA2_PEAP-MSCHAPv2_And_WPA2_PEAP-MSCHAPv2_TKIP

Title	Verify support of WPA2 security mode with PEAP/MSCHAPv2 network authentication
Purpose	Test the SUT for connectivity to WLAN clients using PEAP/ MSCHAPv2 authentication with AES or TKIP encryption and WPA2 key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	AES, TKIP, WPA2, PEAP/MSCHAPv2 with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for PEAP/MSCHAPv2 support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support both TKIP and AES encryption with PEAP/ MSCHAPv2 network authentication and WPA2 key management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with valid root certificate, plus user login name of 'anonymous' and password of 'whatever' and anonymous ID of 'anonymous' • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with client security mode set to WPA2-PEAP-MSCHAPv2 or WPA2-PEAP-MSCHAPv2-TKIP, with a root certificate, plus user login name of 'anonymous' and password of 'whatever' and anonymous ID of 'anonymous' • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior

Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above, starting with WPA2-PEAP-MSCHAPv2 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses 18. Repeat steps 4 to 17 with WPA2-PEAP-MSCHAPv2-TKIP used as the security mode
Test Priority	Mandatory for WPA2-PEAP-MSCHAPv2; Medium for WPA2-PEAP-MSCHAPv2-TKIP
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client should authenticate successfully, acquire a DHCP address and then be able to pass traffic to the Ethernet client.

STC 020 WPA2_EAP-FAST

Title	Verify support of WPA2 security mode with EAP/FAST network authentication
Purpose	Test the SUT for connectivity to WLAN clients using EAP/FAST

	authentication with AES encryption and WPA2 key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	AES, WPA, EAP/FAST with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for EAP/FAST support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables • Configure the SUT to support AES encryption with EAP/FAST network authentication and WPA2 key management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with user login name of 'anonymous' and password of 'whatever' • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to WPA2-EAP-FAST with login name and password of 'anonymous,' and 'whatever' respectively • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning)

	7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	High
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 021 WPA2_LEAP

Title	Verify support of WPA2 security with LEAP network authentication
Purpose	Test the SUT for connectivity to WLAN clients using LEAP authentication, AES encryption, and WPA2 key management. Test traffic is sent from each associated client to the SUT in order to verify successful connectivity establishment including matching security parameters.
SUT Feature(s) Tested	WPA2, AES, LEAP with RADIUS, DHCP
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for LEAP support
Test Setup	• Connect the Wi-Fi WaveBlade to SUT via RF cables

	• Configure the SUT to support AES encryption and LEAP network authentication and WPA2 key management, and to allow clients to use static IP addresses as well as DHCP • Configure RADIUS server with user login name of ‘anonymous’ and password of ‘whatever’ • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set client security method to WPA2-LEAP with login name and password of ‘anonymous’ and ‘whatever’ respectively • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1 and 10 clients using the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSID and configure the client(s) to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 8. Set the initial number of Wi-Fi clients to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 clients

	16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	Low
Test Type	Authentication
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP address(es) in the correct subnet(s).

STC 022 Mixed_WPA_WPA2_PSK

Title	Verify support of a mix of clients using WPA2-PSK and WPA-PSK security modes
Purpose	Test the SUT for connectivity to WLAN clients using a combination of WPA-PSK and WPA2-PSK security modes (WPA and WPA2 key management respectively, TKIP and AES encryption respectively, PSK authentication in both cases). Test traffic will be sent from each associated client to the SUT in order to verify successful connectivity establishment, including matching security parameters.
SUT Feature(s) Tested	WPA-PSK, WPA2-PSK, AES, TKIP, DHCP, per-client encryption selection
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to support two different SSIDs with TKIP and AES encryption and both WPA and WPA2 key management respectively, with PSK authentication for both; set the WPA shared secret set to ‘whatever’ and the WPA2 shared secret to ‘nonesuch’; also set up SUT to allow clients to use static IP addresses as well as DHCP • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set up two groups of clients associated with the two SUT SSIDs; one group having WPA-PSK security mode with shared secred ‘whatever’, and the other group having WPA2-PSK security mode with shared secret ‘nonesuch’ • Set client flow PHY rate to 54 Mb/s and management (i.e.,

	connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with each of the two client groups containing 1 and 10 clients; all clients in a group should use the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSIDs and configure the two client groups to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 2 8. Set the initial number of Wi-Fi clients in each group to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 Wi-Fi clients in each group 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	High
Test Type	Authentication
Pass/Fail Criteria	All Wi-Fi clients should successfully associate with the SUT and

	pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP addresses in the correct subnet(s).

STC 023 Mixed_WPA_PSK_WPA2_EAP-TLS

Title	Verify support of a mix of clients using WPA-PSK and WPA2-EAP/TLS security modes
Purpose	Test the SUT for connectivity to WLAN clients using a combination of WPA-PSK and WPA2-EAP/TLS security modes (WPA and WPA2 key management respectively, TKIP and AES encryption respectively, PSK and EAP/TLS authentication respectively). Test traffic will be sent from each associated client to the SUT in order to verify successful connectivity establishment, including matching security parameters.
SUT Feature(s) Tested	WPA, WPA2, AES, TKIP, PSK, EAP/TLS, RADIUS integration, DHCP, coexistence of PSK and EAP types, per-client encryption selection
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT set up to operate in the IEEE 802.11b/g band, with static IP addressing as well as DHCP enabled • DHCP server connected to Ethernet port of SUT • RADIUS server set up for EAP/TLS support
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to support two different SSIDs with TKIP and AES encryption and both WPA and WPA2 key management respectively • Set the authentication method for the SUT SSID supporting WPA to PSK, with a shared secret set of 'whatever' • Set the authentication method for the SUT SSID supporting WPA2 to network authentication (i.e., RADIUS) • Configure RADIUS server with valid root, client and CA certificates and private key, plus user login name of 'anonymous' and password of 'whatever' • Also configure SUT to allow clients to use static IP addresses as well as DHCP • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set up two groups of clients associated with the two SUT SSIDs; one group having WPA-PSK security mode with shared secred 'whatever', and the other group having WPA2-EAP-TLS with shared secret set to 'whatever', plus login name and password of 'anonymous' and 'whatever' respectively • Set client flow PHY rate to 54 Mb/s and management (i.e.,

	connection) PHY rate to 6 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with each of the two client groups containing 1 and 10 clients; all clients in a group should use the same security parameters • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSIDs and configure the two client groups to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 2 8. Set the initial number of clients in each Wi-Fi client group to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 Wi-Fi clients in each group 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	High
Test Type	Authentication
Pass/Fail Criteria	All Wi-Fi clients should successfully associate with the SUT and

	pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP addresses in the correct subnet(s).

STC 024 Mixed_80211bg_WEP_WPA2_EAP-TLS

Title	Verify support of a mix of 802.11b-only and 802.11b/g clients using WEP-40 and WPA2-EAP/TLS security modes
Purpose	Test the SUT for connectivity to WLAN clients using a combination of static WEP-40 and WPA2-EAP/TLS security modes (WPA2 key management, AES encryption, EAP/TLS authentication). The client groups are further subdivided into 802.11b-only and 802.11b/g types, to verify that legacy 802.11b clients can coexist. Test traffic will be sent from each associated client to the SUT in order to verify successful connectivity establishment, including matching security parameters.
SUT Feature(s) Tested	WEP-40, WPA2, AES, EAP/TLS, RADIUS integration, DHCP, coexistence of 802.11b and 802.11b/g, coexistence of WEP and WPA2-EAP/TLS
Requirement(s)	• Wavemanager application running on host PC, 1xWi-Fi Waveblade, 1xEthernet Waveblade • SUT setup to support mixed 802.11b and g modes and mixed WPA/WPA2 security with AES-CCMP encryption using EAP/TLS network authentication • DHCP turned on the SUT • RADIUS server setup to support EAP/TLS
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to support two different SSIDs with WEP-40 and AES encryption, and Open-system and WPA2 key management respectively • Set the authentication method for the SUT SSID supporting WEP-40 to Open-system, and configure a hex key of ‘3031323334’ • Set the authentication method for the SUT SSID supporting WPA2 to network authentication (i.e., RADIUS) • Configure RADIUS server for EAP/TLS with valid root, client and CA certificates and private key, plus user login name of ‘anonymous’ and password of ‘whatever’ • Also configure SUT to allow clients to use static IP addresses as well as DHCP • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set up four groups of clients associated with the two SUT SSIDs, as follows: o Group 1 having WEP-40 security mode with hex key ’3031323334’ configured in 802.11b/g mode with a

	flow PHY rate of 54 Mb/s and management (i.e., connection) PHY rate of 6 Mb/s o Group 2 having WEP-40 security mode with hex key ’3031323334’ configured in 802.11b-only mode with a flow PHY rate of 11 Mb/s and management (i.e., connection) PHY rate of 1 Mb/s o Group 3 having WPA2-EAP-TLS with valid certificates, private key, plus login name and password set to ‘anonymous’ and ‘whatever’ respectively, configured in 802.11b/g mode with a flow PHY rate of 54 Mb/s and management (i.e., connection) PHY rate of 6 Mb/s o Group 4 having WPA2-EAP-TLS with valid certificates, private key, plus login name and password set to ‘anonymous’ and ‘whatever’ respectively, configured in 802.11b-only mode with a flow PHY rate of 11 Mb/s and management (i.e., connection) PHY rate of 1 Mb/s • Set offered test traffic load to 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set channel to 1 (2.4 GHz band) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with each of the four client groups containing 1 and 10 clients; all clients in a group should use the same security parameters and 802.11b-only settings • Run test with active scan (broadcast probing) and passive scan (no probing) client behavior.
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the channel to 1 4. Select SSIDs and configure the four client groups to use security parameters as indicated above 5. Configure the client to use static IP address(es) 6. Set client probe behavior to broadcast probing before association (active scanning) 7. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 2 8. Set the initial number of clients in each Wi-Fi client group to 1 9. Select the frame sizes as 88, 512 and 1518 bytes, and UDP traffic type 10. Set the ILOAD to 100 frames/second 11. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds

	12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 4 to 14 with 10 Wi-Fi clients in each group 16. Repeat steps 4 to 15 with no probing before association (passive scanning) 17. Repeat steps 4 to 16 with DHCP being used by clients instead of static IP addresses
Test Priority	High
Test Type	Authentication
Pass/Fail Criteria	All Wi-Fi clients should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions, and should also successfully acquire DHCP addresses in the correct subnet(s).

Basic Forwarding

The WLAN infrastructure must respond predictably and uniformly to different types of traffic, regardless of frame size, frame contents, offered load, application type, etc. Otherwise, network instability and high congestion or failure rates can occur. For example if the infrastructure equipment has a sensitivity to certain specific frame sizes (for example, corresponding to internal packet buffer thresholds) then bursts of traffic with these frame sizes can cause choke points or even system crashes.

These tests verify the ability of the SUT to handle forward packets consistently over a wide range of offered traffic levels and characteristics, including limited overloads. They also verify that the 802.11a and 802.11g datapaths within the SUT APs (which typically use separate MAC and buffering) function consistently. Note that these tests exercise the SUT over a very large number of test configurations (thousands of trials) and hence take a long time and should preferably be run in an automated manner.

BTC 001 Upstream_80211g_Packet_Loss_Sweep

Title	Verify upstream frame forwarding behavior over a range of frame sizes and offered loads for the 802.11g SUT datapaths
Purpose	Test the SUT to ensure that it processes and forwards wireless-to-Ethernet frames uniformly regardless of the specific frame size or the specific traffic load that is presented to it. Test traffic is injected into all of the SUT ports in the upstream direction and a sweep is performed over all legal frame sizes and a large number of offered loads. When plotted on a graph, the results will clearly indicate any anomalies or forwarding performance issues.

SUT Feature(s) Tested	Uniform traffic handling datapath, anomalous forwarding performance, instabilities
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic with static IP addressing • SUT configured with 802.11g APs
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with all UDP frame sizes ranging from 88 bytes to 1518 bytes inclusive in 1 byte steps (1431 values) • Run test with 1 and 10 clients per AP • Run test with intended load (ILOAD) values ranging from 1000 to 7000 frames/second (inclusive) per AP in 2000 byte steps (4 values).
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test, and note the number of APs as *N* 4. Select SSID and configure the client(s) to open authentication with no encryption and to use static IP address(es) 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select a frame size sweep ranging from 88 to 1518 bytes in steps of 1 byte, an ILOAD sweep ranging from (1000**N*) fps to (7000**N*) fps in steps of 1000 fps, and UDP traffic type 8. Set the trial duration to 10 seconds and allow 1 second for the SUT to settle between trials 9. Select Wireless to Ethernet (one-to-one, upstream) mapping 10. Run the test 11. Wait until test completes 12. Collect report and results data, and plot the forwarding rate and packet loss values versus frame size (one graph per ILOAD value) 13. Repeat steps 5 to 12 with 10 clients per AP configured on both Ethernet and Wi-Fi sides (one-to-one) 14. Repeat steps 5 to 13 with WPA-TKIP and WPA2-AES

	encryption modes
Test Priority	Mandatory
Test Type	Parameter sweep
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should not have any unexpected spikes or jumps (either positive or negative) in the forwarding rate vs. frame size graphs. The graphs should show either constant levels or smooth decreases as the frame size increases, with at most one knee in the curve.

BTC 002 Downstream_80211g_Packet_Loss_Sweep

Title	Verify downstream frame forwarding behavior over a range of frame sizes and offered loads for the 802.11g SUT datapaths
Purpose	Test the SUT to ensure that it processes and forwards Ethernet-to-wireless frames uniformly regardless of the specific frame size or the specific traffic load that is presented to it. Test traffic is injected into all of the SUT ports in the downstream direction and a sweep is performed over all legal frame sizes and a large number of offered loads. When plotted on a graph, the results will clearly indicate any anomalies or forwarding performance issues.
SUT Feature(s) Tested	Uniform traffic handling datapath, anomalous forwarding performance, instabilities
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic with static IP addressing • SUT configured with 802.11g APs
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with all UDP frame sizes ranging from 88 bytes to 1518 bytes inclusive in 1 byte steps (1431 values) • Run test with 1 and 10 clients per AP • Run test with intended load (ILOAD) values ranging from 1000 to 7000 frames/second (inclusive) per AP in 2000 byte steps (4 values).
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test, and note the number of APs as *N*

	4. Select SSID and configure the client(s) to open authentication with no encryption and to use static IP address(es) 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select a frame size sweep ranging from 88 to 1518 bytes in steps of 1 byte, an ILOAD sweep ranging from (1000*_N_) fps to (7000*_N_) fps in steps of 1000 fps, and UDP traffic type 8. Set the trial duration to 10 seconds and allow 1 second for the SUT to settle between trials 9. Select Ethernet to Wireless (one-to-one, downstream) mapping 10. Run the test 11. Wait until test completes 12. Collect report and results data, and plot the forwarding rate and packet loss values versus frame size (one graph per ILOAD value) 13. Repeat steps 5 to 12 with 10 clients per AP configured on both Ethernet and Wi-Fi sides (one-to-one) 14. Repeat steps 5 to 13 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Parameter sweep
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should not have any unexpected spikes or jumps (either positive or negative) in the forwarding rate vs. frame size graphs. The graphs should show either constant levels or smooth decreases as the frame size increases, with at most one knee in the curve.

BTC 003 Bidirectional_80211g_Packet_Loss_Sweep

Title	Verify bidirectional frame forwarding behavior over a range of frame sizes and offered loads for the 802.11g SUT datapaths
Purpose	Test the SUT to ensure that it processes and forwards concurrent Ethernet-to-wireless and wireless-to-Ethernet frames uniformly regardless of the specific frame size or the specific traffic load that is presented to it. Test traffic is injected into all of the SUT ports in both the downstream and upstream directions and a sweep is performed over all legal frame sizes and a large number of offered loads. When plotted on a graph, the results will clearly indicate any anomalies or forwarding performance issues. This test also indicates how well the SUT responds to contention over the entire range of frame sizes.

SUT Feature(s) Tested	Uniform traffic handling datapath, anomalous forwarding performance, instabilities, contention handling
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic with static IP addressing • SUT configured with 802.11g APs
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with all UDP frame sizes ranging from 88 bytes to 1518 bytes inclusive in 1 byte steps (1431 values) • Run test with 1 and 10 clients per AP • Run test with intended load (ILOAD) values ranging from 1000 to 7000 frames/second (inclusive) per AP in 2000 byte steps (4 values).
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test, and note the number of APs as *N* 4. Select SSID and configure the client(s) to open authentication with no encryption and to use static IP address(es) 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select a frame size sweep ranging from 88 to 1518 bytes in steps of 1 byte, an ILOAD sweep ranging from (1000*N) fps to (7000*N) fps in steps of 1000 fps, and UDP traffic type 8. Set the trial duration to 10 seconds and allow 1 second for the SUT to settle between trials 9. Select Wireless to Ethernet bidirectional (one-to-one) mapping with the bidirectional option checked 10. Run the test 11. Wait until test completes 12. Collect report and results data, and plot the forwarding rate and packet loss values versus frame size (one graph per ILOAD value) 13. Repeat steps 5 to 12 with 10 clients per AP configured on both Ethernet and Wi-Fi sides (one-to-one), and media contention

	turned on for the clients 14. Repeat steps 5 to 13 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Parameter sweep
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should not have any unexpected spikes or jumps (either positive or negative) in the forwarding rate vs. frame size graphs. The graphs should show either constant levels or smooth decreases as the frame size increases, with at most one knee in the curve.

BTC 004 Upstream_80211a_Packet_Loss_Sweep

Title	Verify upstream frame forwarding behavior over a range of frame sizes and offered loads for the 802.11a SUT datapaths
Purpose	Test the SUT to ensure that it processes and forwards wireless-to-Ethernet frames uniformly regardless of the specific frame size or the specific traffic load that is presented to it. Test traffic is injected into all of the SUT ports in the upstream direction and a sweep is performed over all legal frame sizes and a large number of offered loads. When plotted on a graph, the results will clearly indicate any anomalies or forwarding performance issues.
SUT Feature(s) Tested	Uniform traffic handling datapath, anomalous forwarding performance, instabilities
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic with static IP addressing • SUT configured with 802.11a APs
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with all UDP frame sizes ranging from 88 bytes to 1518 bytes inclusive in 1 byte steps (1431 values) • Run test with 1 and 10 clients per AP • Run test with intended load (ILOAD) values ranging from 1000 to 7000 frames/second (inclusive) per AP in 2000 byte steps (4 values).
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite

	3. Select the test port(s) (i.e., APs) to use for the test, and note the number of APs as *N* 4. Select SSID and configure the client(s) to open authentication with no encryption and to use static IP address(es) 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select a frame size sweep ranging from 88 to 1518 bytes in steps of 1 byte, an ILOAD sweep ranging from (1000*N) fps to (7000*N) fps in steps of 1000 fps, and UDP traffic type 8. Set the trial duration to 10 seconds and allow 1 second for the SUT to settle between trials 9. Select Wireless to Ethernet (one-to-one, upstream) mapping 10. Run the test 11. Wait until test completes 12. Collect report and results data, and plot the forwarding rate and packet loss values versus frame size (one graph per ILOAD value) 13. Repeat steps 5 to 12 with 10 clients per AP configured on both Ethernet and Wi-Fi sides (one-to-one) 14. Repeat steps 5 to 13 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Parameter sweep
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should not have any unexpected spikes or jumps (either positive or negative) in the forwarding rate vs. frame size graphs. The graphs should show either constant levels or smooth decreases as the frame size increases, with at most one knee in the curve. Finally, the results should be consistent with the corresponding upstream 802.11g packet loss sweep (if this has been performed).

BTC 002 Downstream_80211a_Packet_Loss_Sweep

Title	Verify downstream frame forwarding behavior over a range of frame sizes and offered loads for the 802.11a SUT datapaths
Purpose	Test the SUT to ensure that it processes and forwards Ethernet-to-wireless frames uniformly regardless of the specific frame size or the specific traffic load that is presented to it. Test traffic is injected into all of the SUT ports in the downstream direction and a sweep is performed over all legal frame sizes and a large number of offered loads. When plotted on a graph, the results will clearly indicate any anomalies or forwarding performance issues.

SUT Feature(s) Tested	Uniform traffic handling datapath, anomalous forwarding performance, instabilities
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic with static IP addressing • SUT configured with 802.11a APs
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with all UDP frame sizes ranging from 88 bytes to 1518 bytes inclusive in 1 byte steps (1431 values) • Run test with 1 and 10 clients per AP • Run test with intended load (ILOAD) values ranging from 1000 to 7000 frames/second (inclusive) per AP in 2000 byte steps (4 values).
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test, and note the number of APs as *N* 4. Select SSID and configure the client(s) to open authentication with no encryption and to use static IP address(es) 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select a frame size sweep ranging from 88 to 1518 bytes in steps of 1 byte, an ILOAD sweep ranging from (1000**N*) fps to (7000**N*) fps in steps of 1000 fps, and UDP traffic type 8. Set the trial duration to 10 seconds and allow 1 second for the SUT to settle between trials 9. Select Ethernet to Wireless (one-to-one, downstream) mapping 10. Run the test 11. Wait until test completes 12. Collect report and results data, and plot the forwarding rate and packet loss values versus frame size (one graph per ILOAD value) 13. Repeat steps 5 to 12 with 10 clients per AP configured on both Ethernet and Wi-Fi sides (one-to-one) 14. Repeat steps 5 to 13 with WPA-TKIP and WPA2-AES

	encryption modes
Test Priority	Mandatory
Test Type	Parameter sweep
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should not have any unexpected spikes or jumps (either positive or negative) in the forwarding rate vs. frame size graphs. The graphs should show either constant levels or smooth decreases as the frame size increases, with at most one knee in the curve. Finally, the results should be consistent with the corresponding upstream 802.11g packet loss sweep (if this has been performed).

BTC 003 Bidirectional_80211a_Packet_Loss_Sweep

Title	Verify bidirectional frame forwarding behavior over a range of frame sizes and offered loads for the 802.11a SUT datapaths
Purpose	Test the SUT to ensure that it processes and forwards concurrent Ethernet-to-wireless and wireless-to-Ethernet frames uniformly regardless of the specific frame size or the specific traffic load that is presented to it. Test traffic is injected into all of the SUT ports in both the downstream and upstream directions and a sweep is performed over all legal frame sizes and a large number of offered loads. When plotted on a graph, the results will clearly indicate any anomalies or forwarding performance issues. This test also indicates how well the SUT responds to contention over the entire range of frame sizes.
SUT Feature(s) Tested	Uniform traffic handling datapath, anomalous forwarding performance, instabilities, contention handling
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic with static IP addressing • SUT configured with 802.11a APs
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with all UDP frame sizes ranging from 88 bytes to 1518 bytes inclusive in 1 byte steps (1431 values) • Run test with 1 and 10 clients per AP • Run test with intended load (ILOAD) values ranging from 1000 to 7000 frames/second (inclusive) per AP in 2000 byte steps (4 values).
Procedure	1. Launch the WaveApps application

	2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test, and note the number of APs as *N* 4. Select SSID and configure the client(s) to open authentication with no encryption and to use static IP address(es) 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select a frame size sweep ranging from 88 to 1518 bytes in steps of 1 byte, an ILOAD sweep ranging from (1000**N*) fps to (7000**N*) fps in steps of 1000 fps, and UDP traffic type 8. Set the trial duration to 10 seconds and allow 1 second for the SUT to settle between trials 9. Select Wireless to Ethernet bidirectional (one-to-one) mapping with the bidirectional option checked 10. Run the test 11. Wait until test completes 12. Collect report and results data, and plot the forwarding rate and packet loss values versus frame size (one graph per ILOAD value) 13. Repeat steps 5 to 12 with 10 clients per AP configured on both Ethernet and Wi-Fi sides (one-to-one), and media contention turned on for the clients 14. Repeat steps 5 to 13 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Parameter sweep
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should not have any unexpected spikes or jumps (either positive or negative) in the forwarding rate vs. frame size graphs. The graphs should show either constant levels or smooth decreases as the frame size increases, with at most one knee in the curve. Finally, the results should be consistent with the corresponding upstream 802.11g packet loss sweep (if this has been performed).

Power Save

Mobile wireless clients implement different levels of power save depending on the application and battery life requirements. Handsets use aggressive sleep modes to conserve battery life, while a laptop may use a less aggressive power save level to deliver higher throughput performance. To support such clients, the SUT must buffer traffic intended for sleeping stations, and deliver it as quickly as possible when the stations wake up and request the data. Failure to implement these functions results in an inability to support battery-powered WLAN clients.

These tests verify the functionality implemented in the SUT to support clients in various sleep modes, ranging from fully awake (CAM, or Continuous Awake Mode) to deep sleep. Mixed mode tests are also specified to verify that the SUT can support sleeping clients even in the presence of large numbers of clients that do not enter power-save mode. Different security modes are also tested.

PTC 001 Power_Save_Baseline_CAM_Test

Title	Verify support of Continuous Awake Mode (CAM) functionality, to serve as a baseline
Purpose	Test the SUT for support of different numbers of WLAN clients with power-save mode turned off. Downstream test traffic will be sent to each associated client in order to verify that the SUT does not buffer traffic to stations not in power-save mode.
SUT Feature(s) Tested	CAM mode
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT setup to operate in the 802.11b/g band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to open authentication mode, using 802.11b/g channel 1 • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load to 100 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1, 10, and 100 clients (distributed evenly across the AP(s) in the SUT) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Launch the WaveDynamix application 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP’s channel on the test ports 4. Access the Client Tab and click on the “+” button to create 1 Wi-Fi clientgroup

	5. Right click on Clientgroup to edit Layer 2 network profile 6. Click the customize button to set the open security mode (no encryption) 7. Similarly, set up the Layer 3 network profile to use static IP addressing 8. Select the Client profile option to select “Enable Power Save Mode” option and disable the Power Save Mode option 9. Create an Ethernet client profile with static IP addressing 10. Create a traffic profile to send 1000 frames of fixed length at 100 frames/second 11. Set the initial frame size in the traffic profile to 88 bytes 12. Set the initial number of Wi-Fi clients to 1 13. Create a flow from Ethernet to Wireless using the above profiles, and the appropriate ports 14. Run the test by starting all flows, then stopping after approximately 30 seconds 15. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 16. Save the flow TX/RX packet transfer and latency results and inspect the data 17. Repeat steps 6 to 12 with 10 clients, setting the traffic profile to transmit 100 frames at 10 frames/second 18. Repeat steps 6 to 12 with 100 clients, setting the traffic profile to transmit 10 frames at 1 frames/second 19. Repeat steps 6 to 14 with frame sizes of 88, 512, 1518 bytes 20. Repeat steps 3 to 15 with WPA-PSK and WPA2-PSK security modes set in the Wi-Fi client profile
Test Priority	High
Test Type	Power Save
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and receive traffic from the Ethernet client with zero packet loss under all test conditions, and with latency under 50 milliseconds for all test conditions.

PTC 002 Power-Save_Legacy_PS_Poll

Title	Verify support of client power-save functionality using the legacy Power Save Poll (PS-Poll) mechanism
Purpose	Test the SUT for support of different numbers of WLAN clients using the PS-Poll based power-save handshake mode. Downstream traffic will be sent to each associated client in order

	to verify that the SUT correctly does the following: buffers traffic when the stations are in PS-mode, indicate the existence of buffered traffic using its beacons, and deliver the buffered frames properly when the clients wake up at different listen intervals. The test clients will request the frames via PS-Poll.
SUT Feature(s) Tested	Power save buffering and delivery, PS-Poll handling, announcement via TIM bitmaps in beacons
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT setup to operate in the 802.11b/g band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to open authentication mode, using 802.11b/g channel 1 • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load to 100 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1, 10, and 100 clients (distributed evenly across the AP(s) in the SUT) • Run test with listen intervals of 1, 5 and 10 beacon periods • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Launch the WaveDynamix application 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Access the Client Tab and click on the "+" button to create 1 Wi-Fi clientgroup 5. Right click on Clientgroup to edit Layer 2 network profile 6. Click the customize button to set the open security mode (no encryption) 7. Similarly, set up the Layer 3 network profile to use static IP addressing 8. Select the Client profile option to select "Enable Power Save Mode" option and set the listen interval to 1 beacon period 9. Create an Ethernet client profile with static IP addressing 10. Create a traffic profile to send 1000 frames of fixed length at

	100 frames/second 11. Set the initial frame size in the traffic profile to 88 bytes 12. Set the initial number of Wi-Fi clients to 1 13. Create a flow from Ethernet to Wireless using the above profiles, and the appropriate ports 14. Run the test by starting all flows, then stopping after approximately 30 seconds 15. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 16. Save the flow TX/RX packet transfer and latency results and inspect the data 17. Repeat steps 4 to 12 with listen intervals of 5 and 10 beacon periods 18. Repeat steps 4 to 13 with 10 clients, setting the traffic profile to transmit 100 frames at 10 frames/second 19. Repeat steps 4 to 13 with 100 clients, setting the traffic profile to transmit 10 frames at 1 frame/second 20. Repeat steps 4 to 15 with frame sizes of 88, 512, 1518 bytes 21. Repeat steps 4 to 15 with WPA-PSK and WPA2-PSK security modes set in the Wi-Fi client profile
Test Priority	High
Test Type	Power Save
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and receive traffic from the Ethernet client with zero packet loss under all test conditions. The average latency should not exceed 50% of the configured listen interval + 1 beacon period, and the maximum latency should not exceed the configured listen interval + 1 beacon period. (Note: the nominal beacon period is usually 102.4 msec.)

PTC 003 Power-Save_APSD

Title	Verify support of client power-save functionality using WMM Power Save (U-APSD)
Purpose	Test the SUT for support of different numbers of WLAN clients using WMM (802.11e) U-APSD based power-save handshake mode. Downstream traffic will be sent to each associated client in order to verify that the SUT correctly does the following: buffers traffic when the stations are in PS-mode, indicate the existence of buffered traffic using its beacons, and deliver the buffered frames properly when the clients wake up at different listen intervals. The test clients will request the frames via U-APSD trigger frames.
SUT Feature(s) Tested	Power save buffering and delivery, U-APSD protocol support,

	trigger frame handling, announcement via TIM bitmaps in beacons, U-APSD SP length support
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT setup to operate in the 802.11b/g band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to open authentication mode, using 802.11b/g channel 1 • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load to 100 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1, 10, and 100 clients (distributed evenly across the AP(s) in the SUT) • Run test with listen intervals of 1, 5 and 10 beacon periods • Run test with service periods (SP) of 0, 2, 4 and 6 frames • Run test with Open, WPA-PSK, and WPA2-PSK security modes • Run test with ACs of AC_BE, AC_BK, AC_VI and AC_VO
Procedure	1. Configure the WaveDynamix configuration parameters according to the trial being run, as per steps 2 through 8 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Access the Client Tab and click on the "+" button to create 1 Wi-Fi clientgroup 5. Right click on Clientgroup to edit Layer 2 network profile 6. Click the customize button to set the open security mode (no encryption) 7. Similarly, set up the Layer 3 network profile to use static IP addressing 8. Access the Client profile option and select "Enable Power Save Mode" option, select "Advertise WMM" and "WMM power save" 9. Set the initial AC to AC_BE 10. Set the initial listen interval to 1 beacon period

	11. Set the initial service period (SP) to 0 frames 12. Configure 1 Ethernet source client with static IP addressing 13. Configure the traffic parameters to send 1000 frames of fixed length at 100 frames/second with 88, 512 and 1512 byte frame sizes on successive iterations 14. Run the test by starting all flows, then stopping after approximately 30 seconds 15. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 16. Save the flow TX/RX packet transfer and latency information and inspect the data 17. Repeat steps 9 to 11 with service periods of 2, 4, and 6 frames 18. Repeat steps 9 to 12 with listen intervals of 5 and 10 beacon periods 19. Repeat steps 7 to 13 with AC set to AC_BK, AC_VI & AC_VO 20. Repeat steps 6 to 14 with 10 clients, setting the traffic parameters for 100 frames for each client at 10 frames/second 21. Repeat steps 6 to 14 with 100 clients, setting the traffic parameters for 10 frames for each client at 1 frames/second 22. Repeat steps 6 to 16 with WPA-PSK and WPA2-PSK security modes for the Wi-Fi client(s)
Test Priority	Medium
Test Type	Power Save
Pass/Fail Criteria	The Wi-Fi client(s) should successfully associate with the SUT and receive traffic from the Ethernet client with zero packet loss under all test conditions. The average latency should not exceed 50% of the configured listen interval + 1 beacon period, and the maximum latency should not exceed the configured listen interval + 1 beacon period. (Note: the nominal beacon period is usually 102.4 msec.) For non-zero service periods, the average latency should decrease as the service period increases.

PTC 004 Power-Save_Mixed_1

Title	Verify support of client power-save functionality using a mixture of legacy PS-Poll power-save and non-power-save (CAM) stations
Purpose	Test the SUT for support of mixed networks of WLAN clients using CAM (non-power-save) mode and legacy PS-Poll based power-save handshake mode. Downstream traffic will be sent to each associated client in order to verify that the SUT correctly does the following: does not buffer traffic to CAM stations, buffers traffic to the stations in PS-mode, indicates the existence of buffered traffic using its beacons, and delivers the buffered frames properly when

	the sleeping clients wake up at different listen intervals. The test clients will request the frames via PS-Poll.
SUT Feature(s) Tested	Power save buffering and delivery, per-client power save state maintenance, PS-Poll handling, selective announcement via TIM bitmaps in beacons
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT setup to operate in the 802.11b/g band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to open authentication mode, using 802.11b/g channel 1 • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load to 200 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1, 5, and 50 power-save clients and 1, 5 and 50 CAM clients (distributed evenly across the AP(s) in the SUT) • Run test with listen intervals of 1, 5 and 10 beacon periods • Run test with Open, WPA-PSK, and WPA2-PSK security modes for both power-save and CAM clients
Procedure	1. Launch the WaveDynamix application 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Access the Client Tab and click on the "+" button to create 2 Wi-Fi client groups 5. Setup both Clientgroups to use the open security mode (no encryption) and static IP addressing 6. Right click on Clientgroup1 to edit it and setup the client profile option to use CAM mode by unselecting "Enable Power Save Mode" option 7. Access the Client profile option of Clientgroup2 and select "Enable Power Save Mode" option, set the listen interval to 1 beacon period 8. Create an Ethernet client profile with static IP addressing 9. Create a traffic profile to send 1000 fixed length frames at 100 frames/second

	10. Set the initial frame size in the traffic profile to 88 bytes 11. Set the initial number of Wi-Fi clients to 1 in CAM and 1 in PS-mode 12. Create a flow from the Ethernet client to the CAM Wi-Fi client using the above profiles, and the appropriate ports 13. Create a second flow from the Ethernet client to the PS-mode Wi-Fi client, also using the above profiles, and the appropriate ports 14. Run the test by starting all flows 15. Wait for 10 seconds and then stop the traffic flows 16. Wait until the the counters have settled, save the flow TX/RX packet counts and latency results, and inspect the data 17. Repeat steps 7 to 14 with listen intervals of 5 and 10 beacon periods 18. Repeat steps 7 to 15 with 5 CAM and 5 PS-mode clients, setting the traffic profile to transmit 100 frames at 10 frames/second 19. Repeat steps 4 to 13 with 50 CAM and 50 PS-mode clients, setting the traffic profile to transmit 10 frames at 1 frame/second 20. Repeat steps 4 to 15 with frame sizes of 88, 512, 1518 bytes 21. Repeat steps 4 to 15 with WPA-PSK and WPA2-PSK security modes set in the two wireless client profiles
Test Priority	Medium
Test Type	Power Save
Pass/Fail Criteria	All of the Wi-Fi clients should successfully associate with the SUT and receive traffic from the Ethernet client with zero packet loss under all test conditions. The average latency for the CAM client traffic flows should not exceed 10 milliseconds. The average latency for the PS-mode clients should be substantially larger than the average latency of the CAM clients (i.e., at least 100% larger, and around 50% of the listen interval).

PTC 005 Power-Save_Mixed_2

Title	Verify support of client power-save functionality using a mixture of U-APSD power-save and non-power-save (CAM) stations
Purpose	Test the SUT for support of mixed networks of WLAN clients using CAM (non-power-save) mode and U-APSD power-save handshake mode. Downstream traffic will be sent to each associated client in order to verify that the SUT correctly does the following: does not buffer traffic to CAM stations, buffers traffic to the stations in PS-mode, indicates the existence of buffered traffic using its beacons, and delivers the buffered frames properly when the sleeping

	clients wake up at different listen intervals.
SUT Feature(s) Tested	Power save buffering and delivery, per-client U-APSD power save state maintenance, trigger frame handling, selective announcement via TIM bitmaps in beacons
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT setup to operate in the 802.11b/g band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to open authentication mode, using 802.11b/g channel 1 • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load to 200 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1, 5, and 50 power-save clients and 1, 5 and 50 CAM clients (distributed evenly across the AP(s) in the SUT) • Run test with listen intervals of 1, 5 and 10 beacon periods • Run test with service periods (SP) of 0, 2, 4 and 6 frames • Run test with Open, WPA-PSK, and WPA2-PSK security modes for both power-save and CAM clients • Run test with ACs of AC_BE, AC_BK, AC_VI and AC_VO
Procedure	1. Configure the WaveDynamix application parameters according to the trial being run, as per steps 2 through 9 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 Wi-Fi clientgroup with open security (no encryption), static IP addressing, and CAM mode 5. Configure 1 more Wi-Fi clientgroup with open security (no encryption), static IP addressing, and U-APSD PS mode 6. Set the initial AC for both the CAM and PS-mode Wi-Fi clients to AC_BE 7. Set the initial listen interval to 1 beacon period 8. Set the initial service period (SP) to 0 frames 9. Configure the traffic parameters to send 1000 frames of fixed length at 100 frames/second per flow, with 88, 512 and 1512 byte frame sizes on successive iterations

	10. Configure 1 Ethernet source clientgroup with static IP addressing 11. Run the test by starting all flows, then stopping after approximately 30 seconds 12. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 13. Save the flow TX/RX frame counts and latency information and inspect the data 14. Repeat steps 10 to 12 with service periods of 2, 4, and 6 frames 15. Repeat steps 9 to 13 with listen intervals of 5 and 10 beacon periods 16. Repeat steps 7 to 14 with the AC for both CAM and PS-mode clients set to AC_BK, AC_VI & AC_VO 17. Repeat steps 5 to 15 with 5 CAM and 5 PS-mode clients, setting the traffic parameters for each flow to 100 frames for each client at 10 frames/second 18. Repeat steps 5 to 15 with 50 CAM and 50 PS-mode clients, setting the traffic parameters for 10 frames for each client at 1 frames/second 19. Repeat steps 5 to 17 with WPA-PSK and WPA2-PSK security modes for all the Wi-Fi clients
Test Priority	Medium
Test Type	Power Save
Pass/Fail Criteria	All of the Wi-Fi clients should successfully associate with the SUT and receive traffic from the Ethernet client with zero packet loss under all test conditions. The average latency for the CAM client traffic flows should not exceed 10 milliseconds. The average latency for the PS-mode clients should be substantially larger than the average latency of the CAM clients (i.e., at least 100% larger, and around 50% of the listen interval).

PTC 006 Power-Save_Mixed_3

Title	Verify support of client power-save functionality using a mixture of non-power-save (CAM), legacy PS-Poll and U-APSD stations
Purpose	Test the SUT for support of mixed networks of WLAN clients using CAM (non-power-save) mode, legacy PS-Poll PS-mode, and U-APSD PS-mode. Downstream traffic will be sent to each associated client in order to verify that the SUT correctly does the following: does not buffer traffic to CAM stations, buffers traffic to the stations in PS-mode whether legacy PS-Poll or U-APSD, indicates the existence of buffered traffic using its beacons, and delivers the buffered frames properly when the sleeping clients

	wake up at different listen intervals.
SUT Feature(s) Tested	Power save buffering and delivery, per-client power save state maintenance, per-client distinction between U-APSD and legacy PS-mode states, concurrent PS-Poll and trigger frame handling, selective announcement via TIM bitmaps in beacons
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT setup to operate in the 802.11b/g band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to open authentication mode, using 802.11b/g channel 1 • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load to 200 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1, 3, and 33 legacy PS-Poll power-save clients, 1, 3 and 33 U-APSD clients, and 1, 3 and 33 CAM clients (distributed evenly across the AP(s) in the SUT) • Run test with listen intervals of 1, 5 and 10 beacon periods for both U-APSD and PS-Poll clients • Run test with service periods (SP) of 0, 2, 4 and 6 frames for U-APSD clients • Run test with Open, WPA-PSK, and WPA2-PSK security modes for both PS-mode and CAM clients • Run test with ACs of AC_BE, AC_BK, AC_VI and AC_VO
Procedure	1. Configure the WaveDynamix application parameters according to the trial being run, as per steps 2 through 10 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 Wi-Fi clientgroup with open security (no encryption), static IP addressing, and CAM mode 5. Configure 1 more Wi-Fi clientgroup with open security (no encryption), static IP addressing, and legacy PS-Poll PS mode 6. Configure a third Wi-Fi clientgroup with open security (no encryption), static IP addressing, and U-APSD PS mode 7. Set the initial AC for the CAM and PS-mode Wi-Fi clients to AC_BE

	8. Set the initial listen interval for the PS-mode clients to 1 beacon period 9. Set the initial service period (SP) to 0 frames 10. Configure the traffic parameters to send 1000 frames of fixed length at 100 frames/second per flow, with 88, 512 and 1512 byte frame sizes on successive iterations 11. Configure 1 Ethernet source clientgroup with static IP addressing 12. Run the test by starting all flows, then stopping after approximately 30 seconds 13. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 14. Save the flow TX/RX frame counts and latency information and inspect the data 15. Repeat steps 11 to 13 with service periods of 2, 4, and 6 frames for the U-APSD clients 16. Repeat steps 10 to 14 with listen intervals of 5 and 10 beacon periods for the PS-mode clients (both legacy and U-APSD) 17. Repeat steps 9 to 15 with the AC for all the Wi-Fi clients set to AC_BK, AC_VI and finally AC_VO 18. Repeat steps 5 to 16 with 3 CAM, 3 legacy PS-Poll, and 3 U-APSD clients, setting the traffic parameters for each flow to 100 frames for each client at 10 frames/second 19. Repeat steps 5 to 16 with 33 CAM, 33 legacy PS-Poll, and 33 U-APSD clients, setting the traffic parameters for 10 frames for each client at 1 frames/second 20. Repeat steps 5 to 18 with WPA-PSK and WPA2-PSK security modes for all the Wi-Fi clients
Test Priority	Medium
Test Type	Power Save
Pass/Fail Criteria	All of the Wi-Fi clients should successfully associate with the SUT and receive traffic from the Ethernet client with zero packet loss under all test conditions. The average latency for the CAM client traffic flows should not exceed 10 milliseconds. The average latency for the PS-mode clients should be substantially larger than the average latency of the CAM clients (i.e., at least 100% larger, and around 50% of the listen interval).

PTC 007 Power-Save_Mixed_4

Title	Verify support of client power-save functionality using a mixture of CAM mode for the Best Efforts Access Category (AC_BE) and U-APSD for the Voice Access Category (AC_VO)

Purpose	Test the SUT for support of mixed networks of WLAN clients using CAM (non-power-save) mode and U-APSD power-save handshake mode, where clients in different PS-modes use different WMM ACs. Downstream traffic will be sent to each associated client in order to verify that the SUT correctly does the following: does not buffer traffic to CAM stations, buffers traffic to the stations in PS-mode, indicates the existence of buffered traffic using its beacons, and delivers the buffered frames properly when the sleeping clients wake up at different listen intervals.
SUT Feature(s) Tested	Power save buffering and delivery, per-client U-APSD PS-mode state maintenance, per-AC PS-mode state maintenance and triggering, trigger frame handling, selective announcement via TIM bitmaps in beacons
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT setup to operate in the 802.11b/g band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to open authentication mode, using 802.11b/g channel 1 • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load to 200 frames/second, downstream • Set the AC for CAM clients to AC_BE and for PS-mode clients to AC_VO • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1, 5, and 50 power-save clients and 1, 5 and 50 CAM clients (distributed evenly across the AP(s) in the SUT) • Run test with listen intervals of 1, 5 and 10 beacon periods • Run test with service periods (SP) of 0, 2, 4 and 6 frames • Run test with Open, WPA-PSK, and WPA2-PSK security modes for both power-save and CAM clients
Procedure	1. Configure the WaveDynamix application parameters according to the trial being run, as per steps 2 through 9 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 Wi-Fi clientgroup with open security (no encryption), static IP addressing, CAM mode, and AC_BE

	5. Configure 1 more Wi-Fi clientgroup with open security (no encryption), static IP addressing, and U-APSD PS mode, and AC_VO 6. Set the initial listen interval to 1 beacon period 7. Set the initial service period (SP) to 0 frames 8. Configure the traffic parameters to send 1000 frames of fixed length at 100 frames/second per flow, with 88, 512 and 1512 byte frame sizes on successive iterations 9. Configure 1 Ethernet source clientgroup with static IP addressing 10. Run the test by starting all flows, then stopping after approximately 30 seconds 11. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 12. Save the flow TX/RX frame counts and latency information and inspect the data 13. Repeat steps 9 to 11 with service periods of 2, 4, and 6 frames 14. Repeat steps 8 to 12 with listen intervals of 5 and 10 beacon periods 15. Repeat steps 5 to 13 with 5 CAM and 5 PS-mode clients, setting the traffic parameters for each flow to 100 frames for each client at 10 frames/second 16. Repeat steps 5 to 13 with 50 CAM and 50 PS-mode clients, setting the traffic parameters for 10 frames for each client at 1 frames/second 17. Repeat steps 5 to 15 with WPA-PSK and WPA2-PSK security modes for all the Wi-Fi clients
Test Priority	Medium
Test Type	Power Save
Pass/Fail Criteria	All of the Wi-Fi clients should successfully associate with the SUT and receive traffic from the Ethernet client with zero packet loss under all test conditions. The average latency for the CAM client traffic flows should not exceed 10 milliseconds. The average latency for the PS-mode clients should be substantially larger than the average latency of the CAM clients (i.e., at least 100% larger, and around 50% of the listen interval).

PTC 008 Power-Save_Mixed_5

Title	Verify support of client power-save functionality using a mixture of legacy PS-Poll mode for the Best Efforts Access Category (AC_BE) and U-APSD for Voice Access Category (AC_VO)

Purpose	Test the SUT for support of mixed networks of WLAN clients using legacy PS-Poll mode and U-APSD power-save handshake mode, where clients in different PS-modes use different WMM ACs. Downstream traffic will be sent to each associated client in order to verify that the SUT correctly does the following: buffers traffic to only stations in PS-mode, indicate the existence of buffered traffic using its beacons, and deliver the buffered frames properly using the different ACs and delivery handshakes when the sleeping clients wake up at different listen intervals.
SUT Feature(s) Tested	Power save buffering and delivery, per-client U-APSD and legacy PS-mode state maintenance, per-AC PS-mode state maintenance and triggering, trigger frame handling, PS-Poll frame handling, selective announcement via TIM bitmaps in beacons
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with 1xWi-Fi Waveblade and 1xEthernet Waveblade • SUT setup to operate in the 802.11b/g band • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade to the SUT via RF cables • Configure the SUT to open authentication mode, using 802.11b/g channel 1 • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load to 200 frames/second, downstream • Set the AC for legacy PS-Poll clients to AC_BE and for U-APSD clients to AC_VO • Run test with UDP frame sizes 88, 512 and 1518 bytes • Run test with 1, 5, and 50 U-APSD clients and 1, 5 and 50 PS-Poll clients (distributed evenly across the AP(s) in the SUT) • Run test with listen intervals of 1, 5 and 10 beacon periods • Run test with service periods (SP) of 0, 2, 4 and 6 frames for U-APSD clients • Run test with Open, WPA-PSK, and WPA2-PSK security modes for both types of clients
Procedure	1. Configure the WaveDynamix application parameters according to the trial being run, as per steps 2 through 9 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 Wi-Fi clientgroup with open security (no encryption), static IP addressing, legacy PS-Poll PS-mode, and

	AC_BE 5. Configure 1 more Wi-Fi clientgroup with open security (no encryption), static IP addressing, and U-APSD PS-mode, and AC_VO 6. Set the initial listen interval to 1 beacon period 7. Set the initial service period (SP) to 0 frames for U-APSD 8. Configure the traffic parameters to send 1000 frames of fixed length at 100 frames/second per flow, with 88, 512 and 1512 byte frame sizes on successive iterations 9. Configure 1 Ethernet source clientgroup with static IP addressing 10. Run the test by starting all flows, then stopping after approximately 30 seconds 11. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 12. Save the flow TX/RX frame counts and latency information and inspect the data 13. Repeat steps 9 to 11 with service periods of 2, 4, and 6 frames for U-APSD clients 14. Repeat steps 8 to 12 with listen intervals of 5 and 10 beacon periods 15. Repeat steps 5 to 13 with 5 PS-Poll and 5 U-APSD clients, setting the traffic parameters for each flow to 100 frames for each client at 10 frames/second 16. Repeat steps 5 to 13 with 50 PS-Poll and 50 U-APSD clients, setting the traffic parameters for 10 frames for each client at 1 frames/second 17. Repeat steps 5 to 15 with WPA-PSK and WPA2-PSK security modes for all the Wi-Fi clients
Test Priority	Medium
Test Type	Power Save
Pass/Fail Criteria	All of the Wi-Fi clients should successfully associate with the SUT and receive traffic from the Ethernet client with zero packet loss under all test conditions. The average latency for all of the Wi-Fi clients should be close to each other (i.e., in the range of +/- 10% of the listen interval). The U-APSD clients should achieve the best forwarding rate in proportion with the Offered load.

QoS

Wireless clients in the WLAN network implement different levels of quality of service for traffic types depending on the application requirements for e.g. VoWLAN traffic carries higher priority to maintain low latencies and hence deliver high quality voice calls. The SUT ability to distinguish and prioritize different traffic types efficiently is critical to maintain high performance in the network.

QTC 001 Basic_WMM_Association

Title	Verify basic support for WMM clients
Purpose	Test the SUT's capability to accept connections by WMM-enabled clients. Bidirectional traffic is sent to and from the client(s) to verify that the connection is successful. This test also serves as a baseline for the remainder of the QoS functionality test cases.
SUT Feature(s) Tested	QoS, WMM
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic and WMM/802.11e QoS • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Configure static IP subnets in the SUT and related network • Configure the SUT with open-system authentication mode • Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four 802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load per AP to 1000 frames/second • Set the QoS configuration to adopt AC parameters from the AP(s) • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1, 10, and 100 clients per SUT AP • Run test with flow QoS priority values of 0 (AC_BE), 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Launch the WaveDynamix application 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports

	4. Configure 1 Wi-Fi client profile with open security mode (no encryption) and static IP addressing 5. Create an Ethernet client profile with static IP addressing 6. Create a traffic profile to send 1000 frames of fixed length at 500 frames/second 7. Create a flow QoS profile for the Wi-Fi client and configure it to adopt parameters from the BSS (i.e., SUT AP) 8. Set the initial frame size in the traffic profile to 88 bytes 9. Set the initial number of Wi-Fi clients per AP to 1 10. Set the initial flow QoS profile user priority to 0 (AC_BE) 11. Create one flow from the Ethernet client to each wireless client using the above client, traffic and QoS profiles, and the appropriate ports 12. Create another flow from each wireless client to the Ethernet client, also using the above client, traffic and QoS profiles, and the appropriate ports 13. Run the test by starting all flows, then stopping after approximately 30 seconds 14. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 15. Save the flow TX/RX packet transfer results and inspect the data 16. Repeat steps 10 to 14 with flow QoS profile user priority values set to 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) 17. Repeat steps 9 to 15 with 10 clients per AP, setting the traffic profile to transmit 100 frames at 50 frames/second 18. Repeat steps 9 to 15 with 100 clients per AP, setting the traffic profile to transmit 10 frames at 5 frames/second 19. Repeat steps 8 to 17 with frame sizes of 512 and 1518 bytes 20. Repeat steps 8 to 18 with WPA-PSK and WPA2-PSK security modes set in the Wi-Fi client profile
Test Priority	Mandatory
Test Type	QoS
Pass/Fail Criteria	All of the WMM Wi-Fi clients should successfully associate with the SUT and pass traffic to and from the Ethernet client. The packet loss must be less than 5% for any traffic flow.

QTC 002 Single_Station_Downstream_Fairness

Title	Verify fairness of downstream flows in same QoS level
Purpose	Tests the fairness of the SUT QoS mechanisms when sending flows

	to a single wireless station per AP when all flows possess the same user priority and WMM/802.11e TID. Multiple unidirectional (downstream) traffic flows are injected into the SUT and measured on the wireless side to verify that the SUT treats equal-priority flows equally.
SUT Feature(s) Tested	QoS, WMM/802.11e, 802.1D
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic, 802.1Q VLAN tagging, 802.1D priority and WMM/802.11e QoS • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Configure static IP subnets in the SUT and related network • Configure the SUT with open-system authentication mode • Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four 802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Configure VLAN tagging on the SUT Ethernet port • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load per AP to 5000 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1, 10, and 100 flows per wireless client • Run test with flow QoS priority values of 0 (AC_BE), 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Launch the WaveDynamix application 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 Wi-Fi client profile with open security mode (no encryption) and static IP addressing 5. Create an Ethernet client profile with static IP addressing and VLAN tagged packets with the appropriate VLAN ID 6. Create a traffic profile to send continuous traffic with fixed length UDP frames at 2500 frames/second

	7. Create a flow QoS profile for the Ethernet client and configure it to insert a priority tag of 0 (Best Effort) 8. Set the number of Wi-Fi clients per AP to 1 9. Set the initial frame size in the traffic profile to 88 bytes 10. Create two flows from the Ethernet client to each wireless client using the above client, traffic and QoS profiles, with 1:N mapping and the appropriate ports 11. Run the test by starting all flows, then stopping after approximately 30 seconds 12. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 13. Save the flow TX/RX packet transfer results and inspect the data (note: data to be collected for each flow are IP packets transmitted, IP packets received, and measured latency) 14. Repeat steps 10 to 12 with flow QoS profile user priority values set to 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) 15. Repeat steps 9 to 13 with 10 upstream and 10 downstream flows per wireless client, setting the traffic profile to transmit at 250 frames/second for each flow 16. Repeat steps 9 to 13 with 100 upstream and 100 downstream flows per wireless client, setting the traffic profile to transmit at 25 frames/second for each flow 17. Repeat steps 8 to 15 with frame sizes of 512 and 1518 bytes 18. Repeat steps 8 to 15 with WPA-PSK and WPA2-PSK security modes set in the Wi-Fi client profile
Test Priority	High
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should provide equal QoS treatment for all flows in the above test, as they are assigned equal 802.1D/802.11e priority classes. All flows should therefore have received frame values within 10% of each other, and should have latency values within 5% of each other.

QTC 003 Single_Station_Downstream_Priority

Title	Verify prioritization of downstream flows in different QoS levels
Purpose	Tests the functioning of the SUT QoS mechanisms when differentiating downstream flows at different priority levels that are being sent to a single wireless station per AP. Multiple unidirectional (downstream) traffic flows are injected into the SUT and measured on the wireless side to verify that the SUT handles different-priority flows according to their user priority levels.
SUT Feature(s) Tested	QoS, WMM/802.11e, 802.1D

Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic, 802.1Q VLAN tagging, 802.1D priority and WMM/802.11e QoS • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Configure static IP subnets in the SUT and related network • Configure the SUT with open-system authentication mode • Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four 802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Configure VLAN tagging on the SUT Ethernet port • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load per AP to 5000 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 1, 10, and 100 flows per wireless client • Run test with flow QoS priority values chosen from: 0 (AC_BE), 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Launch the WaveDynamix application 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 Wi-Fi client profile with open security mode (no encryption) and static IP addressing 5. Create an Ethernet client profile with static IP addressing and VLAN tagged packets with the appropriate VLAN ID 6. Create a traffic profile to send continuous traffic with fixed length UDP frames at 2500 frames/second 7. Create a flow QoS profile for the Ethernet client labeled QoS_A, and configure it with a priority tag of 0 (Best Effort) 8. Create a second flow QoS profile for the Ethernet client labeled QoS_B, and configure it with a priority tag of 6 (Voice)

	9. Set the number of Wi-Fi clients per AP to 1 10. Set the initial frame size in the traffic profile to 88 bytes 11. Create one flow from the Ethernet client to each wireless client using the above client and traffic profiles, and the appropriate ports; set the QoS profile for these flows to QoS_A 12. Create a second flow from the Ethernet client to each wireless client using the above client and traffic profiles, and the appropriate ports; set the QoS profile for these flows to QoS_B 13. Run the test by starting traffic, then stopping after approximately 30 seconds 14. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 15. Save the flow TX/RX packet transfer results and inspect the data (note: data to be collected for each flow are IP packets transmitted, IP packets received, and measured latency) 16. Repeat steps 12 to 14 for the following combinations of user priority values in the QoS profiles: a. QoS_A = Background (1), QoS_B = Best Effort (0) b. QoS_A = Background (1), QoS_B = Video (4) c. QoS_A = Best Effort (0), QoS_B = Video (4) d. QoS_A = Best Effort (0), QoS_B = Voice (6) e. QoS_A = Video (4), QoS_B = Voice (6) 17. Repeat steps 10 to 15 with 10 upstream and 10 downstream flows per wireless client, setting the traffic profile to transmit at 250 frames/second for each flow 18. Repeat steps 10 to 15 with 100 upstream and 100 downstream flows per wireless client, setting the traffic profile to transmit at 25 frames/second for each flow 19. Repeat steps 10 to 17 with frame sizes of 512 and 1518 bytes 20. Repeat steps 10 to 18 with WPA-PSK and WPA2-PSK security modes set in the Wi-Fi client profile
Test Priority	High
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should clearly differentiate between flows with different 802.1D/802.11e priority classes. Flows assigned to higher-priority QoS classes should have at least 10% more frames forwarded and at least 5% lower latency than any flow in a lower-priority QoS class.

QTC 004 Multi_Station_Downstream_Fairness

Title	Verify fairness of downstream flows in same QoS level destined for

	different wireless clients
Purpose	Tests the fairness of the SUT QoS mechanisms when sending flows to multiple wireless stations per AP, when all flows possess the same user priority and WMM/802.11e TID. Multiple unidirectional (downstream) traffic flows are injected into the SUT and measured on the wireless side to verify that the SUT treats equal-priority flows destined for different clients equally.
SUT Feature(s) Tested	QoS, WMM/802.11e, 802.1D
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic, 802.1Q VLAN tagging, 802.1D priority and WMM/802.11e QoS • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Configure static IP subnets in the SUT and related network • Configure the SUT with open-system authentication mode • Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four 802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Configure VLAN tagging on the SUT Ethernet port • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load per AP to 5000 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 2, 10, and 100 wireless clients per AP • Run test with flow QoS priority values of 0 (AC_BE), 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Launch the WaveDynamix application 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 Wi-Fi clientgroup with open security mode (no encryption) and static IP addressing 5. Create an Ethernet clientgroup with static IP addressing and

	VLAN tagged packets with the appropriate VLAN ID 6. Create a traffic profile to send continuous traffic with fixed length UDP frames at 2500 frames/second 7. Create a flowgroup "flowgroup1" QoS profile and configure it to insert a priority tag of 0 (Best Effort) 8. Choose flowgroup1 to originate from the Ethernet clientgroup 9. Set the initial number of Wi-Fi clients per AP to 2 10. Set the initial frame size in the traffic profile to 88 bytes 11. Choose flowgroup1 to source from the Ethernet clientgroup and sent to wireless clientgroup using the above client, traffic and QoS profiles, and the appropriate ports 12. Run the test by starting traffic, then stopping after approximately 30 seconds 13. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 14. Save the flow TX/RX packet transfer results and inspect the data (note: data to be collected for each flow are IP packets transmitted, IP packets received, and measured latency 15. Repeat steps 10 to 12 with flow QoS profile user priority values set to 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) 16. Repeat steps 10 to 13 with 10 wireless clients per AP, setting the traffic profile to transmit at 250 frames/second for each flow 17. Repeat steps 10 to 13 with 100 wireless clients per AP, setting the traffic profile to transmit at 25 frames/second for each flow 18. Repeat steps 8 to 15 with frame sizes of 512 and 1518 bytes 19. Repeat steps 8 to 15 with WPA-PSK and WPA2-PSK security modes set in the Wi-Fi client profile
Test Priority	Mandatory
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT must provide equal QoS treatment for all flows in the above test, as they are assigned equal 802.1D/802.11e priority classes (even though they terminate on different wireless clients). All flows should therefore have received frame values within 10% of each other, and should have latency values within 5% of each other.

QTC 005 Multi_Station_Downstream_Priority

Title	Verify prioritization of downstream flows in different QoS levels destined for different wireless clients

Purpose	Tests the functioning of the SUT QoS mechanisms when differentiating downstream flows at different priority levels that are being sent to multiple wireless stations per AP. Multiple unidirectional (downstream) traffic flows are injected into the SUT and measured on the wireless side to verify that the SUT handles different-priority flows according to their user priority levels.
SUT Feature(s) Tested	QoS, WMM/802.11e, 802.1D
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic, 802.1Q VLAN tagging, 802.1D priority and WMM/802.11e QoS • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Configure static IP subnets in the SUT and related network • Configure the SUT with open-system authentication mode • Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four 802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Configure VLAN tagging on the SUT Ethernet port • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load per AP to 5000 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 2, 10, and 100 wireless clients per AP • Run test with flow QoS priority values chosen from: 0 (AC_BE), 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Launch the WaveDynamix application 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 Wi-Fi client profile with open security mode (no encryption) and static IP addressing 5. Create an Ethernet client profile with static IP addressing and VLAN tagged packets with the appropriate VLAN ID 6. Create a traffic profile to send continuous traffic with fixed

	length UDP frames at 2500 frames/second 7. Create a flow QoS profile for the Ethernet client labeled QoS_A, and configure it with a priority tag of 0 (Best Effort) 8. Create a second flow QoS profile for the Ethernet client labeled QoS_B, and configure it with a priority tag of 6 (Voice) 9. Set the number of Wi-Fi clients per AP to 2 10. Set the initial frame size in the traffic profile to 88 bytes 11. Create one flowgroup from the Ethernet clientgroup to the first wireless client on each SUT AP using the above client and traffic profiles, and the appropriate ports; set the QoS profile for these flows to QoS_A 12. Create a second flowgroup from the Ethernet client to the second wireless client on each SUT AP using the above client and traffic profiles, and the appropriate ports; set the QoS profile for these flows to QoS_B 13. Run the test by starting traffic, then stopping after approximately 30 seconds 14. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 15. Save the flow TX/RX packet transfer results and inspect the data (note: data to be collected for each flow are IP packets transmitted, IP packets received, and measured latency) 16. Repeat steps 12 to 14 for the following combinations of user priority values in the QoS profiles: a. QoS_A = Background (1), QoS_B = Best Effort (0) b. QoS_A = Background (1), QoS_B = Video (4) c. QoS_A = Best Effort (0), QoS_B = Video (4) d. QoS_A = Best Effort (0), QoS_B = Voice (6) e. QoS_A = Video (4), QoS_B = Voice (6) 17. Repeat steps 10 to 15 with 10 wireless clients (2 groups of 5), setting the traffic profile to transmit at 250 frames/second for each flow 18. Repeat steps 10 to 15 with 100 wireless clients (2 groups of 50), setting the traffic profile to transmit at 25 frames/second for each flow 19. Repeat steps 10 to 17 with frame sizes of 512 and 1518 bytes 20. Repeat steps 10 to 18 with WPA-PSK and WPA2-PSK security modes set in the Wi-Fi client profile
Test Priority	High
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should clearly differentiate between flows with different 802.1D/802.11e priority classes. Flows assigned to higher-priority QoS classes should have

	at least 10% more frames forwarded and at least 5% lower latency than any flow in a lower-priority QoS class, regardless of which client terminates the flows.

QTC 006 Multi_Station_Upstream_Fairness

Title	Verify fairness of upstream flows in same QoS level originating from different wireless clients
Purpose	Tests the fairness of the SUT QoS mechanisms when forwarding flows received from multiple wireless stations per AP, when all flows possess the same user priority and WMM/802.11e TID. Multiple unidirectional (downstream) traffic flows are injected into the SUT and measured on the wireless side to verify that the SUT treats equal-priority flows destined for different clients equally.
SUT Feature(s) Tested	QoS, WMM/802.11e, 802.1D
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic, 802.1Q VLAN tagging, 802.1D priority and WMM/802.11e QoS • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Configure static IP subnets in the SUT and related network • Configure the SUT with open-system authentication mode • Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four 802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Configure VLAN tagging on the SUT Ethernet port • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load per AP to 5000 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 2, 10, and 100 wireless clients per AP • Run test with flow QoS priority values of 0 (AC_BE), 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Launch the WaveDynamix application 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use

	for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 Wi-Fi client profile with open security mode (no encryption) and static IP addressing 5. Create an Ethernet client profile with static IP addressing and VLAN tagged packets with the appropriate VLAN ID 6. Create a traffic profile to send continuous traffic with fixed length UDP frames at 2500 frames/second 7. Create a flowgroup QoS profile for the wireless clients and configure it use priority of 0 (Best Effort) and WMM/802.11e QoS with parameters being adopted from the AP 8. Set the initial number of Wi-Fi clients per AP to 2 9. Set the initial frame size in the traffic profile to 88 bytes 10. Create one flowgroup from each wireless client to the Ethernet client using the above client, traffic and QoS profiles, and the appropriate ports 11. Run the test by starting traffic, then stopping after approximately 30 seconds 12. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 13. Save the flow TX/RX packet transfer results and inspect the data (note: data to be collected for each flow are IP packets transmitted, IP packets received, and measured latency 14. Repeat steps 10 to 12 with flow QoS profile user priority values set to 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) 15. Repeat steps 10 to 13 with 10 wireless clients per AP, setting the traffic profile to transmit at 250 frames/second for each flow 16. Repeat steps 10 to 13 with 100 wireless clients per AP, setting the traffic profile to transmit at 25 frames/second for each flow 17. Repeat steps 8 to 15 with frame sizes of 512 and 1518 bytes 18. Repeat steps 8 to 15 with WPA-PSK and WPA2-PSK security modes set in the Wi-Fi client profile
Test Priority	High
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT must provide equal QoS treatment for all flows in the above test, as they are assigned equal 802.1D/802.11e priority classes (even though they originate from different wireless clients). All flows should therefore have received frame values within 10% of each other, and should have latency values within 5% of each other.

QTC 007 Multi_Station_Upstream_Priority

Title	Verify prioritization of upstream flows in different QoS levels originating from different wireless clients
Purpose	Tests the functioning of the SUT QoS mechanisms when differentiating upstream flows received from different wireless clients at different priority levels. Multiple unidirectional (upstream) traffic flows are injected into the SUT and measured on the Ethernet side to verify that the SUT handles different-priority flows according to their user priority levels.
SUT Feature(s) Tested	QoS, WMM/802.11e, 802.1D
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic, 802.1Q VLAN tagging, 802.1D priority and WMM/802.11e QoS • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Configure static IP subnets in the SUT and related network • Configure the SUT with open-system authentication mode • Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four 802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Configure VLAN tagging on the SUT Ethernet port • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load per AP to 5000 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 2, 10, and 100 wireless clients per AP • Run test with flow QoS priority values chosen from: 0 (AC_BE), 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Launch the WaveDynamix application 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 Wi-Fi client profile with open security mode (no

encryption) and static IP addressing

5. Create an Ethernet client profile with static IP addressing and VLAN tagged packets with the appropriate VLAN ID
6. Create a traffic profile to send continuous traffic with fixed length UDP frames at 2500 frames/second
7. Create a flow QoS profile for the wireless client labeled QoS_A, and configure it with a user priority of 0 (Best Effort), WMM enabled, adopt parameters from the AP, and no CAC handshake
8. Create a second flow QoS profile for the Ethernet client labeled QoS_B, and configure it with a user priority of 6 (Voice), WMM enabled, adopt parameters from the AP, and no CAC handshake
9. Set the number of Wi-Fi clients per AP to 2
10. Set the initial frame size in the traffic profile to 88 bytes
11. Create one flowgroup from the first wireless client on each SUT AP to the Ethernet client using the above client and traffic profiles, and the appropriate ports; set the QoS profile for these flows to QoS_A
12. Create a second flowgroup from the second wireless client on each SUT AP to the Ethernet client using the above client and traffic profiles, and the appropriate ports; set the QoS profile for these flows to QoS_B
13. Run the test by starting traffic, then stopping after approximately 30 seconds
14. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test
15. Save the flow TX/RX packet transfer results and inspect the data (note: data to be collected for each flow are IP packets transmitted, IP packets received, and measured latency)
16. Repeat steps 12 to 14 for the following combinations of user priority values in the QoS profiles:
    a. QoS_A = Background (1), QoS_B = Best Effort (0)
    b. QoS_A = Background (1), QoS_B = Video (4)
    c. QoS_A = Best Effort (0), QoS_B = Video (4)
    d. QoS_A = Best Effort (0), QoS_B = Voice (6)
    e. QoS_A = Video (4), QoS_B = Voice (6)
17. Repeat steps 10 to 15 with 10 wireless clients (2 groups of 5), setting the traffic profile to transmit at 250 frames/second for each flow
18. Repeat steps 10 to 15 with 100 wireless clients (2 groups of 50), setting the traffic profile to transmit at 25 frames/second for each flow
19. Repeat steps 10 to 17 with frame sizes of 512 and 1518 bytes
20. Repeat steps 10 to 18 with WPA-PSK and WPA2-PSK security

	modes set in the Wi-Fi client profile
Test Priority	High
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should clearly differentiate between flows with different 802.1D/802.11e priority classes originating from different clients. Flows assigned to higher-priority QoS classes should have at least 10% more frames forwarded and at least 5% lower latency than any flow in a lower-priority QoS class, regardless of which client originates the flows.

QTC 008 Legacy_QoS_Coexistence

Title	Verify coexistence of QoS and non-QoS (legacy) clients
Purpose	Tests the SUT to verify that it can properly differentiate traffic to and from a mixed environment of WMM/802.11e QoS and non-QoS stations.
SUT Feature(s) Tested	QoS, WMM/802.11e, 802.1D, legacy interworking
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic, 802.1Q VLAN tagging, 802.1D priority and WMM/802.11e QoS • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Configure static IP subnets in the SUT and related network • Configure the SUT with open-system authentication mode • Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four WMM/802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Configure the SUT to map traffic to/from non-QoS clients to the best-efforts traffic class • Configure VLAN tagging on the SUT Ethernet port • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the aggregate offered test traffic load per AP to 4500 frames/second, downstream • Run test with UDP frame sizes: 88, 512, 1518 bytes • Run test with 3, 30, and 90 wireless clients per AP • Run test with flow QoS priority values of 0 (AC_BE), 1

	(AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Launch the WaveDynamix application 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 Wi-Fi client profile with open security mode (no encryption) and static IP addressing 5. Create an Ethernet client profile with static IP addressing and VLAN tagged packets with the appropriate VLAN ID 6. Create a flow group to send continuous traffic with fixed length UDP frames at 1500 frames/second 7. Create the flow QoS profile for the Ethernet client labeled QoS_A, and configure it with a user priority of 0 (Best Effort) 8. Create a second flow QoS profile for the Ethernet client labeled QoS_B, and configure it with a user priority of 6 (Voice) 9. Create a flow QoS profile for the wireless clients labeled QoS_C, and configure it with a user priority of 0 (Best Effort) and WMM/802.11e QoS with parameters being adopted from the AP 10. Create a second flow QoS profile for the wireless clients labeled QoS_D, and configure it with a user priority of 6 (Voice) and WMM/802.11e QoS with parameters being adopted from the AP 11. Set the initial number of Wi-Fi clients per AP to 3 (i.e., 2 QoS and 1 non-QoS) 12. Set the initial frame size in the traffic profile to 88 bytes 13. Create one downstream flowgroup from the Ethernet client to the first wireless client on each SUT AP using the above client and traffic profiles, and the appropriate ports; set the QoS profile for these flows to QoS_A 14. Create one downstream flowgroup from the Ethernet client to the second wireless client on each SUT AP using the above client and traffic profiles, and the appropriate ports; set the QoS profile for these flows to QoS_B 15. Create one downstream flowgroup from the Ethernet client to the third wireless client on each SUT AP using the above client and traffic profiles, and the appropriate ports; set no QoS profile on these flows 16. Create one upstream flowgroup from the first wireless client on each SUT AP to the Ethernet client using the above client and traffic profiles, and the appropriate ports; set the QoS

	profile for these flows to QoS_C 17. Create one upstream flowgroup from the second wireless client on each SUT AP to the Ethernet client using the above client and traffic profiles, and the appropriate ports; set the QoS profile for these flows to QoS_D 18. Create one upstream flowgroup from the second wireless client on each SUT AP to the Ethernet client using the above client and traffic profiles, and the appropriate ports; set the no QoS profile on these flows, to configure the flow/client as non-QoS 19. Run the test by starting all flows, then stopping after approximately 30 seconds 20. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 21. Save the flow TX/RX packet transfer results and inspect the data (note: data to be collected for each flow are IP packets transmitted, IP packets received, and measured latency) 22. Repeat steps 12 to 14 for the following combinations of user priority values in the QoS profiles: a. QoS_A, QoS_C = Background (1), QoS_B, QoS_D = Best Effort (0) b. QoS_A, QoS_C = Background (1), QoS_B, QoS_D = Video (4) c. QoS_A, QoS_C = Best Effort (0), QoS_B, QoS_D = Video (4) d. QoS_A, QoS_C = Best Effort (0), QoS_B, QoS_D = Voice (6) e. QoS_A, QoS_C = Video (4), QoS_B, QoS_D = Voice (6) 23. Repeat steps 10 to 15 with 30 wireless clients (3 groups of 10), setting the traffic profile to transmit at 150 frames/second for each flow 24. Repeat steps 10 to 15 with 90 wireless clients (3 groups of 30), setting the traffic profile to transmit at 50 frames/second for each flow 25. Repeat steps 10 to 17 with frame sizes of 512 and 1518 bytes 26. Repeat steps 10 to 18 with WPA-PSK and WPA2-PSK security modes set in the Wi-Fi client profile
Test Priority	Medium
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should efficiently support mixes of QoS and non-QoS clients. Flows within the same QoS class should have received frame values within 10% of each other, and should have latency values within 5% of each other. Flows assigned to higher-priority QoS classes should have at least 10% more frames forwarded and at least 5% lower latency than any

	flow in a lower-priority QoS class, regardless of which client originates the flows. Flows to or from a non-QoS station should be treated as Best Efforts and should be differentiated properly compared to traffic to or from QoS stations.

QTC 009 Basic_Call_Admission_Control

Title	Verify basic call admission control support via WMM/802.11e
Purpose	Test the SUT's ability to limit the number of WMM-enabled clients according to the advertised bandwidth requirements of these clients. Upstream traffic is sent from the connected WMM clients to verify that admitted clients can maintain their QoS and bandwidth needs. This test also serves as a baseline for the remainder of the CAC functionality test cases.
SUT Feature(s) Tested	QoS, WMM/802.11e, CAC
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic and WMM/802.11e QoS with CAC • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Configure static IP subnets in the SUT and related network • Configure the SUT with open-system authentication mode • Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four 802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Enable CAC on the SUT and set limits as follows: o AC_BE: maximum data rate = 5 Mb/s o AC_BK: maximum data rate = 5 Mb/s o AC_Vi: maximum data rate = 7 Mb/s o AC_VO: maximum data rate = 3 Mb/s • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the QoS configuration (i.e., TSPEC parameters) in the WaveDynamix "Flowgroup properties->QoS profile" section to match those of the SUT with the exception of mean data rate • Run test with UDP frame sizes: 512, 1024, 1518 bytes • Run test with 1, 10, and 100 WMM clients per SUT AP

	• Run test with QoS values of 0 (AC_BE), 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Configure the WaveDynamix application parameters according to the trial being run, as per steps 2 through 16 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 group of Wi-Fi clients per AP with WMM/CAC enabled by selecting the "Advertise WMM" option in the Client profile 5. Configure the initial security mode for the clients in the group to Open 6. Configure the initial number of clients per group to be 1 7. Create new flow group "flowgroup1" by clicking on the "+" button in the "Traffic" tab 8. Right click on flowgroup1 to edit it 9. In the QoS profile selection and under the TSPEC parameters section the initial AC by specifying the TID for the group to be 0 (AC_BE) 10. Configure the traffic type for the group as UDP with a frame size of 512 bytes 11. Configure the aggregate mean data rate for the client(s) in the group to be ((*MDR* – 500 kb/s) / *N*), where *MDR* is the maximum data rate defined for the corresponding AC in the SUT (see above) and *N* is the number of clients in the group 12. Run the test by starting all flows, then stopping after approximately 30 seconds 13. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 14. Save the flow TX/RX packet transfer results and inspect the data (note: data to be collected for each flow are IP packets transmitted, IP packets received, and measured latency) 15. Now configure the aggregate mean data rate for the client(s) in the group to be ((*MDR* + 2000 kb/s) / *N*), where *MDR* and *N* are as above (i.e., exceed the data rate allocated) 16. Run the test again and record the output 17. Repeat steps 8 to 11 with frame sizes of 1024 and 1518 bytes 18. Repeat steps 7 to 12 with AC set to 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) 19. Repeat steps 6 to 13 with the number of clients in the group

	set to 10 and 100 20. Repeat steps 5 to 14 with WPA-PSK and WPA2-PSK security modes
Test Priority	High
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should implement CAC. All of the wireless clients should successfully associate with the SUT and pass traffic when their aggregate mean data rate is less than the configured maximum data rate in the SUT for that traffic class. Some of the wireless clients should fail to associate with the SUT when their aggregate mean data rate is greater than the configured maximum data rate for that traffic class. The packet loss must be less than 5% in the situation where all of the wireless clients associate (i.e., when they satisfy the CAC requirements).

QTC 010 Call_Admission_Control_Denial_PHY_Rate

Title	Verify that CAC operates to deny admission based on minimum PHY rate
Purpose	Test the SUT's ability to deny admission to WMM-enabled clients based on the advertised minimum PHY rate requirements of these clients. Upstream traffic is sent from the connected WMM clients to verify that admitted clients can maintain their QoS and bandwidth needs.
SUT Feature(s) Tested	QoS, WMM/802.11e, CAC, admission denial based on PHY rate
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic and WMM/802.11e QoS with CAC • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Configure static IP subnets in the SUT and related network • Configure the SUT with open-system authentication mode • Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four 802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Enable CAC on the SUT and set the Minimum PHY Rate TSPEC parameter to 12 Mb/s • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e.,

	connection) PHY rate to 6 Mb/s • Set the QoS configuration (i.e., TSPEC parameters) in the WaveDynamix “Flowgroup properties->QoS profile” section to match those of the SUT with the exception of minimum PHY rate • Run test with UDP frame sizes: 512, 1024, 1518 bytes • Run test with 1, 10, and 100 WMM clients per SUT AP • Run test with QoS values of 0 (AC_BE), 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Configure the WaveDynamix application parameters according to the trial being run, as per steps 2 through 15 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP’s channel on the test ports 4. Configure 1 group of Wi-Fi clients per AP with WMM/CAC enabled 5. Configure the initial security mode for the clients in the group to Open 6. Configure the initial number of clients per group to be 1 7. Create new flow group “flowgroup1” by clicking on the “+” button in the “Traffic” tab 8. Right click on flowgroup1 to edit it 9. In the QoS profile selection and under the TSPEC parameters section configure the initial AC by specifying the TID for the group to be 0 (AC_BE) 10. Configure the traffic type for the group as UDP with a frame size of 512 bytes 11. Configure the aggregate mean data rate for the client(s) in the group to be ((*MDR* – 500 kb/s) / *N*), where *MDR* is the maximum data rate configured for the corresponding AC in the SUT and *N* is the number of clients in the group 12. Configure the minimum PHY rate for the client(s) in the group to be 12 Mb/s 13. Run the test by starting all flows, then stopping after approximately 30 seconds 14. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 15. Save the flow TX/RX packet transfer results and inspect the data (note: data to be collected for each flow are IP packets transmitted, IP packets received, and measured latency)

	16. Now configure the minimum PHY rate for the client(s) in the group to be 6 Mb/s 17. Run the test again and record the output 18. Repeat steps 8 to 12 with frame sizes of 1024 and 1518 bytes 19. Repeat steps 7 to 13 with AC set to 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) 20. Repeat steps 6 to 14 with the number of clients in the group set to 10 and 100 21. Repeat steps 5 to 15 with WPA-PSK and WPA2-PSK security modes
Test Priority	Low
Test Type	QoS
Pass/Fail Criteria	All of the wireless clients should successfully associate with an Enterprise Class / Carrier Grade SUT and pass traffic when the requested minimum PHY data rate is greater than the configured minimum PHY data rate in the SUT for that traffic class. All of the wireless clients should fail to associate with the SUT when the configured PHY data rate is greater than the configured minimum PHY data rate. The packet loss must be less than 5% in the situation where all of the wireless clients associate (i.e., when they satisfy the CAC requirements).

QTC 011 Call_Admission_Control_Denial_Utilization

Title	Verify that CAC operates to deny admission based on actual bandwidth utilization within the SUT
Purpose	Test the SUT's ability to limit the number of WMM-enabled clients according to the advertised bandwidth requirements of these clients, when SUT forwarding bandwidth is being occupied by a mixture of QoS/CAC and QoS/non-CAC clients. Upstream traffic is sent from the connected WMM clients to verify that admitted clients can maintain their QoS and bandwidth needs.
SUT Feature(s) Tested	QoS, WMM/802.11e, CAC, bandwidth management
Requirement(s)	• WaveDynamix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic and WMM/802.11e QoS with CAC • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Configure static IP subnets in the SUT and related network • Configure the SUT with open-system authentication mode

	• Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four 802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Enable CAC on the SUT and set limits as follows: o AC_BE: maximum data rate = 5 Mb/s o AC_BK: maximum data rate = 5 Mb/s o AC_VI: maximum data rate = 7 Mb/s o AC_VO: maximum data rate = 3 Mb/s • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the QoS configuration (i.e., TSPEC parameters) in the WaveDynamix "Flowgroup properties->QoS profile" section to match those of the SUT • Set 400 candidate WMM/CAC clients per SUT AP • Set 10 WMM/non-CAC clients per SUT AP • Run test with UDP frame sizes: 512, 1024, 1518 bytes • Run test with QoS values of 0 (AC_BE), 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Configure the WaveDynamix application parameters according to the trial being run, as per steps 2 through 16 2. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 3. Perform a channel scan to acquire the appropriate AP's channel on the test ports 4. Configure 1 group of 400 Wi-Fi clients per AP with WMM/CAC enabled 5. Configure a second group of 10 Wi-Fi clients per AP with WMM enabled without CAC (i.e., QoS but no TSPEC handshake) 6. Configure the initial security mode for the clients in both groups to Open 7. Create 2 new flow groups ("flowgroup1", "flowgroup2") by clicking twice on the "+" button in the "Traffic" tab 8. Right click on the respective flowgroups to edit them 9. In the QoS profile selection and under the TSPEC parameters section the initial AC by specifying the TID for the group to be 0 (AC_BE) 10. Configure the traffic type for both groups as UDP with a frame

	size of 512 bytes 11. Configure the aggregate mean data rate for the client in the WMM group to be (*MDR* / 400), where *MDR* is the maximum data rate defined for the corresponding AC in the SUT (see above) 12. Configure the aggregate mean data rate for the clients in the WMM/non-CAC group to be 2000 kb/s 13. Run the test by starting all flows, then stopping after approximately 30 seconds 14. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 15. Save the flow TX/RX packet transfer results and inspect the data (note: data to be collected for each flow are IP packets transmitted, IP packets received, and measured latency) 16. Record the output, specifically the number of WMM/CAC clients that failed to connect and the total bandwidth consumed by the connected clients 17. Repeat steps 8 to 10 with frame sizes of 1024 and 1518 bytes 18. Repeat steps 7 to 11 with AC set to 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) 19. Repeat steps 6 to 12 with WPA-PSK and WPA2-PSK security modes
Test Priority	Medium
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should not admit further WMM/CAC clients if the admission would utilize more bandwidth than the configured maximum data rate for that traffic class. The packet loss must be less than 5% for all of the connected wireless clients (i.e., those that satisfy the CAC requirements).

QTC 012 Call_Admission_Control

Title	Measure the number of voice calls the SUT can admit using WMM Admission Control mechanism
Purpose	Test the SUT's ability to limit the number of WMM-enabled clients according to the advertised bandwidth requirements of these clients, when SUT forwarding bandwidth is being occupied by WMM/VoIP clients. Upstream traffic sent from the connected WMM clients helps verify that admitted clients can maintain their QoS and bandwidth needs.
SUT Feature(s) Tested	QoS, WMM/802.11e, CAC, bandwidth management, VoIP
Requirement(s)	• WiMix application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and

	Ethernet Waveblade(s) • SUT set up to support UDP traffic and WMM/802.11e QoS with CAC • Static IP addressing configured in the SUT
Test Setup	• Connect the Wi-Fi WaveBlade(s) to the SUT via RF cables • Enable DHCP in the SUT network • Configure the SUT with open-system authentication mode • Configure the SUT to map four 802.1D priority classes (0, 1, 4, 6) to four 802.11e ACs (AC_BE, AC_BK, AC_VI, and AC_VO respectively) • Enable CAC on the SUT and set limits as follows: o AC_VI: maximum data rate = 5 Mb/s o AC_VO: maximum data rate = 3 Mb/s • Set Basic Rate Set on SUT AP(s) to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Set the QoS configuration (i.e., TSPEC parameters) in the WiMix "Traffic->QoS Properties" section to match those of the SUT • Set 400 candidate WMM/VoIP clients per SUT AP, with CAC enabled • Set 10 WMM/data clients per SUT AP, without CAC enabled • Run test with UDP frame sizes: 512, 1024, 1518 bytes • Run test with codec types of: G.711, G.723, G.729 • Run test with QoS values of 0 (AC_BE), 1 (AC_BK), 4 (AC_VI), and 6 (AC_VO) • Run test with Open, WPA-PSK, and WPA2-PSK security modes
Procedure	1. Select the VoIP Admission Control Test from the list under "Application Suites" 2. Configure the WiMix VoIP Admission Control Test parameters according to the trial being run, as per steps 3 through 10 3. Select the test port(s) (i.e., AP(s) in SUT) and channel(s) to use for the test 4. Perform a channel scan to acquire the appropriate AP's channel on the test ports 5. Configure a first group of 400 Wi-Fi clients per AP with WMM/CAC enabled and an AC of 6 (AC_VO) 6. Configure a second group of 10 Wi-Fi clients per AP with WMM enabled, no CAC, and an AC of 4 (AC_VI) 7. Configure the initial security mode for the clients in both

	groups to Open 8. Configure the traffic type for the first group as RTP/VoIP with a codec type of G.711 9. Configure the traffic type for the second group as UDP with a frame size of 512 bytes and an aggregate mean data rate of 500 kb/s 10. Run the test by starting all flows, then stopping after approximately 30 seconds 11. Wait for 2 secs to let the counters settle, then terminate the test iteration by disconnecting all clients in test 12. Save the flow TX/RX packet transfer results and inspect the data (note: data to be collected for each flow are IP packets transmitted, IP packets received, and measured latency) 13. Record the output, specifically the number of WMM/CAC (VoIP) clients that failed to connect and the total number of calls that were successfully established 14. Repeat step 8 with frame sizes of 1024 and 1518 bytes 15. Repeat steps 7 to 9 with codec types of G.723 and G.729 16. Repeat steps 6 to 10 with WPA-PSK and WPA2-PSK security modes
Test Priority	Medium
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should not admit further VoIP handsets using CAC if the admission would jeopardize the call quality of the currently connected handsets, after taking existing bandwidth requirements into accounts. The packet loss must be less than 1% for all of the connected VoIP clients (i.e., those that satisfy the CAC requirements).
Test Priority	Low
Test Type	QoS
Pass/Fail Criteria	A Carrier Grade SUT should not admit further WMM/CAC clients if the admission would utilize more bandwidth than the configured maximum data rate for that traffic class. The packet loss must be less than 5% for all of the connected wireless clients (i.e., those that satisfy the CAC requirements).

802.11n Basic Operational Modes

The following tests verify the basic 802.11n specific functionality of the SUT supporting HT clients.

BOTC 001 80211n_Spatial-Stream_Operation

Title	Verify HT Receive operation with different number of spatial streams (MCS Rates), Guard Intervals and Channel Widths.
Purpose	Test basic support of multiple spatial streams and MCS rates on the SUT while transferring different data frame types and sizes
SUT Feature(s)	Higher performance with more spatial streams
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1x Ethernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • Static IP addressing configured in the SUT
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use ports A and B on Wi-Fi WaveBlade if SUT supports just 2 antenna ports o Use ports A, B and C on Wi-Fi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set HT client management (i.e., connection) PHY rate to highest basic rate set on AP, usually 24Mbps • Set offered test traffic load to 500 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations for each client • Run test using IEEE 802.11g channel 1 and/or IEEE 802.11a channel 36 • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 1 and 10 clients.
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the initial channel to channel 1 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address(es) 5. Set Channel Model to use to "Bypass" 6. For the HT client set Guard Interval mode to LGI 7. For the HT client set Channel Width to 20MHz 8. Set HT client flow PHY rate to MCS = 7 9. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1

	10. Set the initial number of Wi-Fi clients to 1 11. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 12. Set the ILOAD to 500 frames/second 13. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 14. Run the test 15. Wait until test completes 16. Collect report and results data 17. Repeat steps 9 to 16 for MCS = 15 18. Repeat steps 9 to 17 with 10 clients 19. Repeat steps 9 to 18 with Guard Interval set to SGI 20. Repeat steps 9 to 19 with Channel Width set to 40MHz 21. Repeat steps 9 to 20 with Channel Model A, B, C, D, E and F
Test Priority	Mandatory
Test Type	Basic 802.11n
Pass/Fail Criteria	HT clients should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss and also show increased forwarding rates wherever applicable at appropriate MCS rates under all test conditions.

BOTC 002 80211n_Mixed_Spatial-Stream_Operation

Title	Verify HT Receive operation with simultaneous client connections using different no. of spatial streams.
Purpose	Test basic HT support for multiple clients using different spatial streams and MCS rates concurrently on the SUT while transferring different data frame types and sizes
SUT Feature(s)	Simultaneous support for clients with differing no. of spatial streams
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • Static IP addressing configured in the SUT
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use ports A and B on Wi-Fi WaveBlade if SUT supports just 2 antenna ports

	o Use ports A, B and C on Wi-Fi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set HT client management (i.e., connection) PHY rate to highest AP supported Basic rate set • Start with an offered test traffic load of 100 frames/second • Set client association timeout to 20 seconds and permit 2 retries for failed associations for each client • Run test using IEEE 802.11g channel 1 and/or IEEE 802.11a channel 36 • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 2 and 10 clients with equal number of clients using 1 and 2 spatial streams.
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the initial channel to channel 1 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address(es) 5. Select Channel Model “Bypass” to use 6. Set HT client Channel Width to 20MHz 7. Set HT client Guard Interval mode to LGI 8. Set one set of HT clients to a flow PHY rate of MCS = 0 9. Set another set of HT clients to a flow PHY rate of MCS = 8 10. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 2 11. Set the initial number of Wi-Fi clients to 2 12. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 13. Set the ILOAD to 300 frames/second 14. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 15. Run the test 16. Wait until test completes 17. Collect report and results data 18. Repeat steps 10 to 17 with MCS values 1 to 7 for one set of HT clients and with MCS values of 9 to 15 for another set of HT clients 19. Repeat steps 10 to 19 with 10 clients
Test Priority	Mandatory
Test Type	Basic 802.11n

Pass/Fail Criteria	Both set of HT clients using 1 and 2 spatial streams respectively should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss and show increased forwarding rates corresponding to increased MCS rates under all test conditions.

BOTC 003 80211n_Mixed_SGI-and-LGI_Operation

Title	Verify concurrent connections from SGI and LGI clients
Purpose	Tests the SUT for concurrent support of SGI and LGI clients by verifying that non aggregate frames are received and counted properly.
SUT Feature(s)	Concurrent support for clients using different Guard Intervals
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • Static IP addressing configured in the SUT
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set one set of HT clients flow PHY rate to LGI, MCS 7 and management (i.e., connection) PHY rate to the highest supported basic rate on the AP • Set another set of HT clients flow PHY rate to SGI, MCS 15 and management (i.e., connection) PHY rate to the highest supported basic rate on the AP • Set client Channel Width to 20MHz • Set client "HT mode" to "HT mixed" • Set Channel Model to use to "Bypass" mode • Set offered test traffic load to 100 frames/second; higher load to stress the AP • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Run test using IEEE 802.11g channel 1 and/or IEEE 802.11a channels 36 • Run test with UDP frame sizes: 88, 1518 bytes • Run test with 2 and 10 clients

	• Run test with broadcast active scan (probing) client functionality
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the initial channel to channel 1 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address(es) 5. Set Client Channel Model to use to “Bypass” mode 6. Set HT client Channel Width to 20MHz 7. Set one set of HT clients to a flow PHY rate of MCS = 7 8. Set another set of HT clients to a flow PHY rate of MCS = 15 9. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 2 10. Set the initial number of Wi-Fi clients to 2 11. Select the frame sizes as 88 and 1518 bytes, and UDP traffic type 12. Set the ILOAD to 100 frames/second 13. Select Ethernet to Wireless (one-to-one, downstream) mapping and a trial duration of 30 seconds 14. Run the test 15. Wait until test completes 16. Collect report and results data 17. Repeat steps 10 to 16 with traffic loads of 400 fps for HT clients with MCS value 7 and 800 fps for HT client with MCS value 15 18. Repeat steps 10 to 17 with 10 clients 19. Repeat steps 10 to 18 with Channel Width set to 40MHz 20. Repeat steps 10 to 19 with any Channel Model A, B, C, D, E or F
Test Priority	Mandatory
Test Type	Basic 802.11n
Pass/Fail Criteria	Open packet capture and verify that SGI frames were received only by HT clients using SGI. Both SGI mode and LGI mode client(s) should successfully associate with the SUT and pass traffic to the Ethernet client with zero loss under all test conditions.

The following tests verify the basic transmit and receive functionality of the SUT supporting HT clients that use different forms of aggregation.

BOTC 004 80211n_AMPDU_Aggregate_Receive

Title	Verify AMPDU Receive function
Purpose	Tests the SUT for support of Aggregate MPDU receive functionality by verifying that aggregate MPDU data frames are received and counted properly for different data frame types and sizes.
SUT Feature(s)	IEEE 802.11n MIMO AMPDU Receive support for data frames.
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • Static IP addressing configured in the SUT
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set HT clients flow PHY rate to MCS 15 and management (i.e., connection) PHY rate to 6Mbps • Set client "PLCP Configuration" to "HT mixed" • Enable "Aggregation" operation, if disabled previously • Set Channel Model to use to "Bypass" mode • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set ILOAD to about 50% theoretical maximum throughput rates for different frame lengths • Run test using IEEE 802.11g channel 11 and/or IEEE 802.11a channel 161 • Run test with UDP packet sizes: 88, 1518 bytes • Run test with 1 and 10 clients • Run test with broadcast active scan (probing)
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the initial channel to channel 1 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address 5. Set HT client channel width to 20MHz

	6. Select AMPDU Aggregation 7. Set the initial number of Wi-Fi clients to 1 8. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 9. Select UDP traffic type and packet size of 88 bytes and ILOAD to 55000 frames/second 10. Select Wireless to Ethernet (one-to-one, upstream) mapping and a trial duration of 30 seconds 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 7 to 13 with UDP packet size of 1518 bytes and ILOAD of 5500 frames/second 15. Repeat steps 7 to 13 with channel width set to 40MHz and ILOAD of 83000 frames/second for 88 byte frames and 11000 frames/second for 1518 byte frames 16. Repeat steps 7 to 13 with 10 clients 17. Repeat steps 7 to 13 with any Channel Model A, B, C, D, E or F
Test Priority	Mandatory
Test Type	Basic Functionality
Pass/Fail Criteria	HT client(s) should successfully associate with the SUT Open packet capture and make sure that clients receive Block Acks from AP. The appropriate counter, if any, on the SUT for AMPDU frame type should be incremented appropriately.. HT client(s) should successfully pass traffic to the Ethernet client with zero loss on all 802.11g and/or 802.11a band channels and under all test conditions. The avg. forwarding rate should be higher than 200 Mbps for 1518 byte frames and 40MHz operation, and greater than 100 Mbps for all other test conditions.

BOTC 005 80211n_AMPDU_Aggregate_Transmit

Title	Verify AMPDU Transmit function
Purpose	Tests the SUT for support of Aggregate MPDU transmit functionality by verifying that aggregate MPDU data frames are transmitted and counted properly for different data frame types and sizes.
SUT Feature(s)	IEEE 802.11n MIMO AMPDU Transmit support for data frames.
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade

	(WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • Static IP addressing configured in the SUT
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2 Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set HT clients flow PHY rate to MCS 15 and management (i.e., connection) PHY rate to 6Mbps • Set client "PLCP Configuration" to "HT mixed" • Enable "Aggregation" operation, if disabled previously • Set Channel Model to use to "Bypass" mode • Set client association timeout to 20 seconds and permit 2 retries for failed associations • Set ILOAD to about 50% theoretical maximum throughput rates for different frame lengths • Run test using IEEE 802.11g channel 11 and/or IEEE 802.11a channel 161 • Run test with UDP packet sizes: 88, 1518 bytes • Run test with 1 and 10 clients • Run test with broadcast active scan (probing)
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP in SUT) to use for the test and set the initial channel to channel 1 4. Select SSID and configure the client(s) to open authentication with no encryption and static IP address 5. Set HT client channel width to 20MHz 6. Select AMPDU Aggregation 7. Set the initial number of Wi-Fi clients to 1 8. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 9. Select UDP traffic type and packet size of 88 bytes and ILOAD to 55000 frames/second 10. Select Ethernet to Wireless (one-to-one, downstream) mapping and a trial duration of 30 seconds 11. Run the test 12. Wait until test completes

	13. Collect report and results data 14. Repeat steps 7 to 13 with UDP packet size of 1518 bytes and ILOAD of 5500 frames/second 15. Repeat steps 7 to 13 with channel width set to 40MHz and ILOAD of 83000 frames/second for 88 byte frames and 11000 frames/second for 1518 byte frames 16. Repeat steps 7 to 13 with 10 clients
Test Priority	Optional
Test Type	Basic Functionality
Pass/Fail Criteria	HT client(s) should successfully associate with the SUT Open packet capture and make sure that clients receive AMPDU frames from SUT. The appropriate counter, if any, on the SUT for AMPDU frame type should be incremented appropriately. Ethernet client(s) should successfully pass traffic to HT client(s) with zero loss on all 802.11g and/or 802.11a band channels and under all test conditions. The avg. forwarding rate should be higher than 200 Mbps for 1518 byte frames and 40MHz operation, and greater than 100 Mbps for all other test conditions.

Performance and Capacity Benchmarks

Once basic operation is verified the typical approach is to subject the system under test to Benchmark Testing. Industry-standard methods, such as RFC 2544 provide a simple methodology for benchmarking performance of network equipment. These Test plans that can start small and grow to encompass every combination of feature selection desired. The usual progression is to establish baseline performance metrics in the areas of Throughput, Frame Loss, and Latency with frame sizes of 88 bytes, 512 bytes and 1518 bytes and one client, and Maximum Client Capacity at 88 byte frame length. The log files captured in these tests, and the configuration settings recorded, are invaluable for duplicating and analyzing problems found during this initial benchmarking. The more exhaustive benchmarking that is pursued after establishing initial baselines typically includes:

- Throughput with one client at every frame length from 88 to 1518 bytes, inclusive.
- Throughput with one client at every PHY rate at 88 byte frame length.
- Throughput with max number of clients at multiple frame lengths.
- Throughput with max number of clients with each security/encryption type
- Latency with max number of clients at multiple frame lengths and security/encryption types
- TCP goodput with max number of clients at multiple frame lengths and security/encryption types.
- Rate vs. Range at multiple frame lengths

- Roaming performance of many clients across multiple access points
- VoIP QoS performance
- Maximum client capacity

This section covers test cases that are essential to quantifying the performance and capacity of the SUT. Test case results either indicate that the specific performance metric is at, above or below acceptable performance levels. Better than acceptable performance and capacity levels is good indicator that the SUT is capable of operating effectively in actual deployment conditions.

Capacity and Coverage Benchmarking

It is critical for network design engineers to know the capacity of the network that they're deploying. Understanding the maximum client capacity of the SUT as well as the area coverage offered by the APs will provide an indication of how dense each AP cell can be allowed to grow, and hence determine the number of APs needed to provide sufficient coverage and capacity for any deployment. Knowing the VoIP capacity of the network will help traffic planning to determine not only the maximum number of calls that can be supported while maintaining sufficient voice quality but also the maximum data traffic that can be allowed while operating these high-quality voice calls.

Client/Call Capacity

The client capacity and VoIP call capacity tests determine the maximum number of mobile clients or handsets that can feasibly be supported by the SUT. Note that this is quite different from the datasheet specifications of association database size. In order to successfully support a client or handset, the SUT must not merely associate (register) it, but also needs to support the client's minimum data transfer requirements. Failure to support a minimum level of requirements creates situations where users can easily connect to the WLAN but their applications fail to work well (or time out entirely), leading to serious issues with the user experience.

The capacity tests therefore present the SUT with an increasing number of clients (data or VoIP, depending on the specific test). After connection, each client attempts to transfer a predetermined amount of data per second, or establish a VoIP call with a specified minimum quality level. A threshold is set on the data transfer performance. If the SUT fails to sustain the desired level of data performance, the test tries a lower number of clients; otherwise, the test tries a higher number of clients. The test ends when the maximum number of clients have been connected consistent with the predetermined performance threshold.

The tests are conducted with different options to explore the SUT capacity in different dimensions.

CBTC 001 Max_Client_Capacity

Title	Assess maximum client capacity with static IP addresses

Purpose	Measure the maximum number of wireless clients that can be supported by the SUT with each client being able to transfer a pre-set minimum amount of data per second. DHCP is not used.
SUT Feature(s) Tested	Client database capacity, security context capacity, queueing and buffer allocation limits
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP disabled (static IP addressing)
Test Setup	• Configure the SUT with security modes to: Open, WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode APs) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode APs) • Set client PHY rate to 54 Mb/s • Run test with no cipher, WEP-128, TKIP (WPA) and AES-CCMP (WPA2) encryption
Procedure	1. Launch the WaveApps application 2. Select the Client Capacity Test under the IEEE Benchmark Test suite 3. Select the test port(s) (i.e., APs) to use for the test and configure each port into 802.11g or 802.11a mode as required 4. Create an Ethernet client group on the correct port(s) with the number of Ethernet clients set to 1, using static IP 5. Create WLAN client group(s) as required to fill 150% of the expected client capacity of the SUT 6. Select the SSID(s) for the WLAN clients and configure the clients to use static IP 7. Configure an initial wireless client security mode of Open (no security or encryption) for all clients 8. Select UDP as the traffic type 9. Set the frame size to 512 bytes and the ILOAD per client to 10 frames per second (~41 kb/s per client); set the search maximum to the total number of clients created in step 5 10. Run the test and wait until it completes 11. Examine and record the results 12. Repeat steps 8 to 11 with WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-

	EAP-FAST security modes
Test Priority	Mandatory
Test Type	Client Capacity
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should support at least 100 clients per AP, and be capable of transferring data to every connected client at a sustained rate of at least 40 kb/s.

CBTC 002 Max_Client_Capacity_DHCP

Title	Assess maximum client capacity with DHCP active
Purpose	Measure the maximum number of DHCP-based wireless clients that can be supported by the SUT with each client being able to transfer a pre-set minimum amount of data per second. Note that the capabilities of the DHCP server are included in those of the SUT.
SUT Feature(s) Tested	Client database capacity, security context capacity, queueing and buffer allocation limits, DHCP capacity
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled, with a DHCP server present and serving a sufficient number of IP addresses
Test Setup	• Configure the SUT with security modes to: Open, WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST • Configure DHCP in the SUT and related network • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode APs) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode APs) • Set client PHY rate to 54 Mb/s • Run test with no cipher, WEP-128, TKIP (WPA) and AES-CCMP (WPA2) encryption
Procedure	1. Launch the WaveApps application 2. Select the Client Capacity Test under the IEEE Benchmark Test suite 3. Select the test port(s) (i.e., APs) to use for the test and configure each port into 802.11g or 802.11a mode as required 4. Create an Ethernet client group on the correct port(s) with the number of Ethernet clients set to 1, using static IP 5. Create WLAN client group(s) as required to fill 150% of the

	expected client capacity of the SUT 6. Select the SSID(s) for the WLAN clients and configure the clients to obtain their IP addresses via DHCP 7. Configure an initial wireless client security mode of Open (no security or encryption) for all clients 8. Select UDP as the traffic type 9. Set the frame size to 512 bytes and the ILOAD per client to 10 frames per second (~41 kb/s per client); set the search maximum to the total number of clients created in step 5 10. Run the test and wait until it completes 11. Examine and record the results 12. Repeat steps 8 to 11 with WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST security modes
Test Priority	Mandatory
Test Type	Client Capacity
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should support at least 100 DHCP-based clients per AP, and be capable of transferring data to every connected client at a sustained rate of at least 40 kb/s.

CBTC 003 Max_VoIP_Call_Capacity

Title	Assess maximum voice call capacity in presence of data
Purpose	Measure the maximum number of voice calls that can be supported by the SUT in the presence of a fixed amount of best-efforts data traffic without degrading call quality below a pre-set service level agreement (SLA) threshold. Different codec types are used to determine the impact of the codec on the call capacity. The SLA is expressed in terms of an objective voice quality measure (R-value). DHCP is not used.
SUT Feature(s) Tested	Maximum number of voice calls, voice/data prioritization capabilities, QoS implementation efficacy, packet inspection capacity
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support 2 (or more) QoS levels and UDP traffic with static IP addresses
Test Setup	• Configure the SUT with security modes to: Open, WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-

	PEAP-MSCHAPv2, WPA2-EAP-FAST • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Enable WMM/802.11e and 802.1Q prioritization on the SUT with the number of QoS classes being at least 2 (Best Efforts and Voice); each WMM/802.11e AC should correspond to a different SSID configured on the SUT • Set the SLA for the test as: minimum R-value of 78 • Run test with no cipher, WEP-128, TKIP (WPA), and AES-CCMP (WPA2) • Run test with Best Efforts TCP traffic frame sizes: 88, 128, 256, 512, 1024 and 1518 bytes • Run test with background traffic rates of: 10, 50, 100 and 500 frames/second per AP • Run test with G.711, G.723 and G.729 voice codec types
Procedure	1. Launch the WaveApps application 2. Select the Service Capacity Test under the VoIP QoS test suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure WLAN clients with static IP addresses 5. Create an Ethernet client group on the correct port(s) with the number of Ethernet clients set to 1, and using static IP 6. Set the voice call traffic for WLAN QoS with user priority 6 and the background traffic for WLAN QoS with user priority 0 7. Set the other traffic QoS settings (TOS, DSCP, port numbers) to match the SUT requirements, and set the SLA threshold to an R-value of 78 8. Set the initial Wi-Fi security mode to open (no security) 9. Select the initial background traffic frame size as 88 bytes, TCP traffic type 10. Set the initial codec type to G.711 11. Set the initial background traffic rate to 10 frames/second per AP 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 12 to 14 with 50, 100 and 500 frames/second of background data traffic per AP 16. Repeat steps 11 to 15 with G.723 and G.729 codec types

	17. Repeat steps 10 to 16 with frame sizes 128, 256, 512, 1024 and 1518 bytes 18. Repeat steps 9 to 17 with WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST security modes
Test Priority	Mandatory
Test Type	Client Capacity
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should support at least 30 voice calls, irrespective of codec type, with an average R-value greater than 78 at the specified background traffic loading

CBTC 004 Max_VoIP_Call_Capacity_DHCP

Title	Assess maximum voice call capacity in presence of data with DHCP active
Purpose	Measure the maximum number of voice calls that can be supported by the SUT in the presence of a fixed amount of best-efforts data traffic without degrading call quality below a pre-set service level agreement (SLA) threshold. Different codec types are used to determine the impact of the codec on the call capacity. The SLA is expressed in terms of an objective voice quality measure (R-value). DHCP is used to supply IP addresses.
SUT Feature(s) Tested	Maximum number of voice calls, voice/data prioritization capabilities, QoS implementation efficacy, packet inspection capacity, DHCP capacity
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support 2 (or more) QoS levels and UDP traffic • DHCP enabled, with a DHCP server present and serving a sufficient number of IP addresses
Test Setup	• Configure the SUT with security modes to: Open, WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST • Configure DHCP in the SUT and related network • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present) • Enable WMM/802.11e and 802.1Q prioritization on the SUT with the number of QoS classes being at least 2 (Best Efforts and Voice); each WMM/802.11e AC should correspond to a

	different SSID configured on the SUT • Set the SLA for the test as: minimum R-value of 78 • Run test with no cipher, WEP-128, TKIP (WPA), and AES-CCMP (WPA2) • Run test with Best Efforts TCP traffic frame sizes: 88, 128, 256, 512, 1024 and 1518 bytes • Run test with background traffic rates of: 10, 50, 100 and 500 frames/second per AP • Run test with G.711, G.723 and G.729 voice codec types
Procedure	1. Launch the WaveApps application 2. Select the Service Capacity Test under the VoIP QoS test suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure WLAN clients to obtain their IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the number of Ethernet clients set to 1, and obtaining IP addresses via DHCP 6. Set the voice call traffic for WLAN QoS with user priority 6 and the background traffic for WLAN QoS with user priority 0 7. Set the other traffic QoS settings (TOS, DSCP, port numbers) to match the SUT requirements, and set the SLA threshold to an R-value of 78 8. Set the initial Wi-Fi security mode to open (no security) 9. Select the initial background traffic frame size as 88 bytes, TCP traffic type 10. Set the initial codec type to G.711 11. Set the initial background traffic rate to 10 frames/second per AP 12. Run the test 13. Wait until test completes 14. Collect report and results data 15. Repeat steps 12 to 14 with 50, 100 and 500 frames/second of background data traffic per AP 16. Repeat steps 11 to 15 with G.723 and G.729 codec types 17. Repeat steps 10 to 16 with frame sizes 128, 256, 512, 1024 and 1518 bytes 18. Repeat steps 9 to 17 with WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST security modes
Test Priority	Mandatory

Test Type	Client Capacity
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should support at least 30 voice calls, irrespective of codec type, with an average R-value greater than 78 at the specified background traffic loading

Rate vs. Range

The Rate vs. Range test measures the variation in the forwarded traffic rate through the SUT as a function of path loss (which in turn is a function of the range, or the distance between AP and client). Increasing range is simulated by reducing the transmit power and increasing the perceived frame error ratio; this matches what is seen by the SUT when client stations move away from it. The forwarding rate at the specified offered load is measured while range effects are being increased.

This test characterizes the ability of the SUT to cover a large area in an actual deployment. A higher value for range at a specified rate indicates a SUT that can cover a larger area without losing network capacity. Alternatively, the test can be used to determine the offered capacity of the SUT in a fixed coverage region. In addition, this test exercises the rate adaptation algorithm used by the SUT to maximize transfer efficiency as the client moves further away.

For the Rate vs. Range tests, the SUT must be directly connected (via RF cables) to the WLAN WaveBlade, and external attenuation (typically around 70dB) must be placed in the RF path. This is done to ensure that the received power level at the WLAN WaveBlade is between -45 to -55 dBm.

CBTC 010 Rate_vs_Range_80211b

Title	Measure Rate vs Range in 802.11b mode
Purpose	Measures the forwarding rate sustained by the SUT as a function of path loss while the SUT is operating in 802.11b-only mode
SUT Feature(s) Tested	SUT coverage area, SUT rate adaptation capability
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled • External attenuation in RF path (typically 70dB)
Test Setup	• Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 11Mbps • Set client PHY rate to 11 Mb/s in 802.11b-only mode

	- Run test with no security (open authentication, no encryption) - Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes - Add external attenuation between antenna port and AP so RSSI power at the station is between -45 and -55 dBm; typically 70 dB of attenuation is needed
Procedure	1. Launch the WaveApps application 2. Select the Rate vs. Range Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port with the number of Ethernet clients set to 1 6. Set the number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Enter the amount of external attenuation 9. Run the test 10. Wait until test completes 11. Collect report and results data
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	There are no pass/fail criteria for this test. Maintenance of a high data forwarding rate for a longer period (i.e., a higher degree of path loss) indicates a more capable SUT. The rate vs. range (path loss) graph should not show any discontinuities or irregularities that denote instabilities in the rate management algorithms.

CBTC 011 Rate_vs_Range_80211g

Title	Measure Rate vs Range in 802.11g mode
Purpose	Measures the forwarding rate sustained by the SUT as a function of path loss while the SUT is operating in 802.11g-only mode
SUT Feature(s) Tested	SUT coverage area, SUT rate adaptation capability
Requirement(s)	- WaveApps application running on host PC - WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) - SUT set up to support UDP traffic - DHCP enabled

	• External attenuation in RF path (typically 70dB)
Test Setup	• Configure the SUT with open authentication • Set Basic Rate Set on SUT to 6 Mbps, 12 Mbps, 24 Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no security (open authentication, no encryption) • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Add external attenuation between antenna port and AP so RSSI power at the station is between -45 and -55 dBm; typically 70 dB of attenuation is needed
Procedure	1. Launch the WaveApps application 2. Select the Rate vs. Range Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port with the number of Ethernet clients set to 1 6. Set the number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Enter the amount of external attenuation 9. Run the test 10. Wait until test completes 11. Collect report and results data
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	There are no pass/fail criteria for this test. Maintenance of a high data forwarding rate for a longer period (i.e., a higher degree of path loss) indicates a more capable SUT. The rate vs. range (path loss) graph should not show any discontinuities or irregularities that denote instabilities in the rate management algorithms.

CBTC 012 Rate_vs_Range_80211a

Title	Measure Rate vs Range in 802.11a mode
Purpose	Measures the forwarding rate sustained by the SUT as a function of path loss while the SUT is operating in 802.11g-only mode
SUT Feature(s) Tested	SUT coverage area, SUT rate adaptation capability

Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled • External attenuation in RF path (typically 70dB)
Test Setup	• Configure the SUT with open authentication • Set Basic Rate Set on SUT to 6 Mbps, 12 Mbps, 24 Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no security (open authentication, no encryption) • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Add external attenuation between antenna port and AP so RSSI power at the station is between -45 and -55 dBm; typically 70 dB of attenuation is needed
Procedure	1. Launch the WaveApps application 2. Select the Rate vs. Range Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port (i.e., AP) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port with the number of Ethernet clients set to 1 6. Set the number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Enter the amount of external attenuation 9. Run the test 10. Wait until test completes 11. Collect report and results data
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	There are no pass/fail criteria for this test. Maintenance of a high data forwarding rate for a longer period (i.e., a higher degree of path loss) indicates a more capable SUT. The rate vs. range (path loss) graph should not show any discontinuities or irregularities that denote instabilities in the rate management algorithms.

Performance Benchmarking

For a WLAN to be able to scale and successfully support various applications running a variety of traffic types and sizes it has to maintain a high throughput, low packet loss, and minimal latency/jitter on both non-encrypted and encrypted networks. It is critical to drive WLAN traffic at link capacity while also scaling-up the number of clients to make these performance measurements. In addition to that the WLAN needs to meet stringent mobility requirements in terms of minimal roaming delays while supporting complex security types and roaming patterns.

Throughput

The following throughput tests measure the maximum rate which the SUT can forward packets without packet loss. Throughput tests are a key measurement of the performance of the SUT and will help determine how much traffic and how many users the SUT can support. Also, unexpected levels of packet loss detected during throughput tests can be indicative of internal issues with the SUT.

The throughput tests are conducted with a variety of frame sizes, numbers of clients, security modes, operating bands, and directions (i.e., Upstream, Downstream and bi-directional). They are also carried out with different traffic types (i.e., UDP and TCP).

PBTC 001 Upstream_UDP_80211g_Throughput

Title	Measure upstream UDP 802.11g throughput
Purpose	Measure the upstream UDP throughput that can be achieved on the SUT operating in 802.11g-only mode
SUT Feature(s) Tested	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients
Procedure	1. Launch the WaveApps application

	2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes 14.
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames >= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

PBTC 002 Downstream_UDP_80211g_Throughput

Title	Measure downstream UDP 802.11g throughput
Purpose	Measure the downstream UDP throughput that can be achieved on the SUT operating in 802.11g-only mode
SUT Feature(s) Tested	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic

	• DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Ethernet to Wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 7 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 7 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following downstream throughput: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames >= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

PBTC 003 Bidirectional_UDP_80211g_Throughput

Title	Measure bidirectional UDP 802.11g throughput
Purpose	Measure the bidirectional UDP throughput that can be achieved on the SUT operating in 802.11g-only mode
SUT Feature(s) Tested	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one) mapping with the bidirectional option checked 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 7 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 7 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory

Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve a bidirectional throughput that is at least 75% of the unidirectional throughput values, namely: >= 22.5 Mbps for 1518 byte frames >= 18.8 Mbps for 1024 byte frames >= 12 Mbps for 512 byte frames >= 7.4 Mbps for 256 byte frames >= 4.1 Mbps for 128 byte frames >= 2.8 Mbps for 88 byte frames

PBTC 004 Upstream_UDP_80211a_Throughput

Title	Measure upstream UDP 802.11a throughput
Purpose	Measure the UDP throughput that can be achieved on the SUT operating in 802.11a mode
SUT Feature(s) Tested	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping

	9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 7 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 7 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames >= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

PBTC 005 Downstream_UDP_80211a_Throughput

Title	Measure downstream UDP 802.11a throughput
Purpose	Measure the UDP throughput that can be achieved on the SUT operating in 802.11a mode
SUT Feature(s) Tested	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test

	4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Ethernet to Wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 7 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 7 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following downstream throughput: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames >= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

PBTC 006 Bidirectional_UDP_80211a_Throughput

Title	Measure bidirectional UDP 802.11a throughput
Purpose	Measure the bidirectional UDP throughput that can be achieved on the SUT operating in 802.11a mode
SUT Feature(s) Tested	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode

	• Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one) mapping with the bidirectional option checked 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 7 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 7 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve a bidirectional throughput that is at least 75% of the unidirectional throughput values, namely: >= 22.5 Mbps for 1518 byte frames >= 18.8 Mbps for 1024 byte frames >= 12 Mbps for 512 byte frames >= 7.4 Mbps for 256 byte frames >= 4.1 Mbps for 128 byte frames >= 2.8 Mbps for 88 byte frames

PBTC 007 Upstream_TCP_80211g_Throughput

Title	Measure upstream TCP 802.11g throughput
Purpose	Measure the stateful TCP throughput that can be achieved on the SUT in 802.11g mode with traffic flowing in the upstream direction

SUT Feature(s) Tested	Maximum reliable TCP data forwarding rate
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with TCP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients (NOTE: 100- and 500-client configurations should be run with a multi-AP SUT)
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and TCP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 7 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 7 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	High
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream stateful TCP throughput: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames

	>= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

PBTC 008 Downstream_TCP_80211g_Throughput

Title	Measure downstream TCP 80211g throughput
Purpose	Measure the stateful TCP throughput that can be achieved on the SUT operating in 802.11g mode with traffic flowing in the downstream direction
SUT Feature(s) Tested	Maximum reliable TCP data forwarding rate
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with TCP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients (NOTE: 100- and 500-client configurations should be run with a multi-AP SUT)
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and TCP traffic type 8. Select Ethernet to Wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes

	11. Collect report and results data 12. Repeat steps 7 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 7 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	High
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following downstream stateful TCP throughput: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames >= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

PBTC 009 Upstream_TCP_80211a_Throughput

Title	Measure upstream TCP 80211a Throughput
Purpose	Measure the stateful TCP throughput that can be achieved on the SUT operating in 802.11a mode with traffic flowing in the upstream direction
SUT Feature(s) Tested	Maximum reliable TCP data forwarding rate
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with TCP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients (NOTE: 100- and 500-client configurations should be run with a multi-AP SUT)
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication

	with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 7 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 7 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	High
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream stateful TCP throughput: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames >= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

PBTC 010 Downstream_TCP_80211a_Throughput

Title	Measure downstream TCP 80211a throughput
Purpose	Measure the stateful TCP throughput that can be achieved on the SUT operating in 802.11a mode with traffic flowing in the downstream direction
SUT Feature(s) Tested	Maximum reliable TCP data forwarding rate
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP

	• Run test with TCP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients (NOTE: 100- and 500-client configurations should be run with a multi-AP SUT)
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and TCP traffic type 8. Select Ethernet to Wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 7 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 7 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	High
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following downstream stateful TCP throughput: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames >= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

802.11n Throughput

The following throughput tests measure the maximum rate which an 802.11n SUT can forward packets without packet loss with a variety of frame sizes. The test is repeated for a variety of client sizes, modes (LGI, SGI, AMPDU etc.), and for upstream, downstream and bi-directional traffic. Throughput tests are a key measurement of the performance of the SUT and will help determine how much traffic and how many users the SUT can support. The "Pass" criterion for all test cases is set at 95% of the theoretical medium capacity which enterprise class 802.11n SUTs are expected to achieve since the 802.11abg SUTs meet or beat that threshold.

PBTC 100 Upstream_HT-non-Aggregate_Throughput

Title	Measure upstream UDP non-aggregate HT throughput
Purpose	Measure the upstream UDP throughput that can be achieved on the SUT supporting HT clients using non-aggregate frames
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 7 • Set client Guard Interval to LGI • Set client Channel bandwidth to 20MHz • Set client HT mode to "HT mixed" • Set client Channel Model to "Bypass" • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with

	the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20 and 30 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes 14. Repeat steps 5 to 13 with MCS rates 15 15. Repeat steps 5 to 14 with Guard Interval set to SGI 16. Repeat steps 5 to 15 with Channel Bandwidth set to 40MHz 17. Repeat steps 5 to 16 with any Channel Model – B, D, E or F
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput: >= 56.04 Mbps for 1518 byte frames >= 40.49 Mbps for 1024 byte frames >= 21.79 Mbps for 512 byte frames >= 11.33 Mbps for 256 byte frames >= 5.78 Mbps for 128 byte frames >= 3.975 Mbps for 88 byte frames

PBTC 101 Downstream_ HT-non-Aggregate _Throughput

Title	Measure downstream UDP non-aggregate HT throughput
Purpose	Measure the downstream UDP throughput that can be achieved on the SUT supporting HT clients using non-aggregate frames
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to

	SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 7 • Set client Guard Interval to LGI • Set client Channel bandwidth to 20MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Ethernet to Wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes 14. Repeat steps 5 to 13 with MCS = 15 15. Repeat steps 5 to 14 with Guard Interval set to SGI 16. Repeat steps 5 to 15 with Channel Bandwidth set to 40MHz
Test Priority	Mandatory

Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput: >= 56.04 Mbps for 1518 byte frames >= 40.49 Mbps for 1024 byte frames >= 21.79 Mbps for 512 byte frames >= 11.33 Mbps for 256 byte frames >= 5.78 Mbps for 128 byte frames >= 3.975 Mbps for 88 byte frames

PBTC 102 Bidirectional_ HT-non-Aggregate _Throughput

Title	Measure downstream UDP non-aggregate HT throughput
Purpose	Measure the downstream UDP throughput that can be achieved on the SUT supporting HT clients using non-aggregate frames
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 7 • Set client Guard Interval to LGI • Set client Channel bandwidth to 20MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption, WPA-TKIP and WPA2-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2

	Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one) mapping with the bidirectional option checked 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (1-to-1) 13. Repeat steps 5 to 12 with WPA2-AES encryption mode 14. Repeat steps 5 to 13 with MCS = 15 15. Repeat steps 5 to 14 with Guard Interval set to SGI 16. Repeat steps 5 to 15 with Channel Bandwidth set to 40MHz 17. Repeat steps 5 to 16 with any Channel Model – B, D, E or F
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput: >= 56.04 Mbps for 1518 byte frames >= 40.49 Mbps for 1024 byte frames >= 21.79 Mbps for 512 byte frames >= 11.33 Mbps for 256 byte frames >= 5.78 Mbps for 128 byte frames >= 3.975 Mbps for 88 byte frames

PBTC 103 Upstream_HT-AMPDU_20MHz_Throughput

Title	Measure upstream HT AMPDU Throughput
Purpose	Measure the upstream AMPDU throughput that can be achieved on the SUT supporting HT clients
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade

	(WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support AMPDU aggregation w/ BlockAck operation • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS = 15 • Set client Guard Interval to LGI • Set client Channel bandwidth to 20MHz • Set client HT mode to "HT mixed" • Set client Channel Model to "Bypass" • Run test with no encryption and WPA2-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024,and 1518 bytes • Run test with 1, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20 and 30 clients configured on both Ethernet and Wi-Fi sides (one-to-one)

	13. Repeat steps 5 to 12 with WPA2-AES encryption mode 14. Repeat steps 5 to 13 with Channel Models A and C
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following minimum upstream throughput:

	1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
20MHz	118 Mbps	116 Mbps	112 Mbps	103 Mbps	90 Mbps	130 Mbps

PBTC 104 Downstream_ HT-AMPDU_20MHz_Throughput

Title	Measure downstream HT AMPDU Throughput
Purpose	Measure the downstream AMPDU throughput that can be achieved on the SUT supporting HT clients
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support AMPDU aggregation w/ BlockAck operation • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS = 15 • Set client Guard Interval to LGI • Set client Channel bandwidth to 20MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption and WPA2-AES

	• Run test with UDP frame sizes: 88, 128, 256, 512, 1024,and 1518 bytes • Run test with 1, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024 and 1518 bytes and UDP traffic type 8. Select Ethernet to Wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following minimum downstream throughput:

	1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
20MHz	118 Mbps	116 Mbps	112 Mbps	103 Mbps	90 Mbps	130 Mbps

PBTC 105 Bidirectional_ HT-AMPDU _20MHz_Throughput

Title	Measure bi-directional HT AMPDU Throughput
Purpose	Measure the bi-directional AMPDU Throughput that can be achieved on the SUT supporting HT clients
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC

	• WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support AMPDU aggregation w/ BlockAck operation • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to LGI • Set client Channel bandwidth to 20MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption and WPA2-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, and 1518 bytes • Run test with 1, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one) mapping with the bidirectional option checked 9. Run the test 10. Wait until test completes 11. Collect report and results data

	12. Repeat steps 5 to 11 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA2-AES encryption mode 14. Repeat steps 5 to 13 with Channel Models – A and C
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following minimum bi-directional throughput:

	1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
20MHz	118 Mbps	116 Mbps	112 Mbps	103 Mbps	90 Mbps	130 Mbps

PBTC 106 Upstream_HT-AMPDU_40MHz_Throughput

Title	Measure upstream HT AMPDU Throughput
Purpose	Measure the upstream HT AMPDU throughput that can be achieved on the SUT supporting HT clients
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support AMPDU aggregation w/ BlockAck operation • SUT set up to support 40MHz channel bandwidth • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to LGI • Set client Channel bandwidth to 40MHz • Set client HT mode to "HT mixed"

	• Set client Channel Model to "Bypass" • Run test with no encryption and WPA2-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024 and 1518 bytes • Run test with 1, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20 and 30 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA2-AES encryption mode 14. Repeat steps 5 to 13 with Channel Models A and C
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following minimum bi-directional throughput:

	1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
40MHz	232 Mbps	232 Mbps	213 Mbps	185 Mbps	149 Mbps	82 Mbps

PBTC 107 Downstream_ HT-AMPDU _40MHz_Throughput

Title	Measure downstream AMPDU HT throughput
Purpose	Measure the downstream AMPDU throughput that can be achieved on the SUT supporting HT clients
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance

Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support AMPDU aggregation w/ BlockAck operation • SUT set up to support 40MHz channel bandwidth • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS = 15 • Set client Guard Interval to LGI • Set client Channel bandwidth to 20MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption and WPA2-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024 and 1518 bytes • Run test with 1, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, and 1518 bytes and UDP traffic type 8. Select Ethernet to Wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes

	11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA2-AES encryption mode
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following minimum bi-directional throughput:

	1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
40MHz	232 Mbps	232 Mbps	213 Mbps	185 Mbps	149 Mbps	82 Mbps

PBTC 108 Bidirectional_ HT-AMPDU _40MHz_Throughput

Title	Measure bi-directional HT AMPDU Throughput
Purpose	Measure the bi-directional AMPDU throughput that can be achieved on the SUT supporting HT clients
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support AMPDU aggregation w/ BlockAck operation • SUT set up to support 40MHz channel bandwidth • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to LGI • Set client Channel bandwidth to 40MHz • Set client HT mode to “HT mixed”

	• Set client Channel Model to “Bypass” • Run test with no encryption and WPA2-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024 and 1518 bytes • Run test with 1, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one) mapping with the bidirectional option checked 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA2-AES encryption modes 14. Repeat steps 5 to 13 with Channel Models – A and C
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following minimum bi-directional throughput:

	1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
40 MHz	232 Mbps	232 Mbps	213 Mbps	185 Mbps	149 Mbps	82 Mbps

PBTC 109 Upstream_HT-AMPDU_40MHz_SGI_Throughput

Title	Measure upstream HT AMPDU Throughput using 40MHz signals and SGI operational mode
Purpose	Measure the upstream AMPDU throughput that can be achieved

	on the SUT supporting HT clients operating 40MHz signals and using SGI mode.
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support AMPDU aggregation w/ BlockAck operation • SUT set up to support 40MHz channel bandwidth • SUT set up to support SGI operation • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to SGI • Set client Channel bandwidth to 40MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption WPA2-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024 and 1518 bytes • Run test with 1, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024 and 1518 bytes and UDP traffic type

	8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 WPA2-AES encryption mode 14. Repeat steps 5 to 13 with Channel Models A and C
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput:

	1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
40 MHz	254 Mbps	247 Mbps	232 Mbps	200 Mbps	162 Mbps	136 Mbps

PBTC 110 Downstream_ HT-AMPDU _40MHz_SGI_Throughput

Title	Measure downstream HT AMPDU Throughput using 40MHz signals and SGI operational mode
Purpose	Measure the downstream AMPDU throughput that can be achieved on the SUT supporting HT clients operating 40MHz signals and using SGI mode.
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support AMPDU aggregation w/ BlockAck operation • SUT set up to support 40MHz channel bandwidth • SUT set up to support SGI operation • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports

	o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to SGI • Set client Channel bandwidth to 40MHz • Set client HT mode to "HT mixed" • Set client Channel Model to "Bypass" • Run test with no encryption and WPA2-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, and 1518 bytes • Run test with 1, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024 and 1518 bytes and UDP traffic type 8. Select Ethernet to Wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 12 with WPA2-AES encryption mode 13. Repeat steps 5 to 11 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one)
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput:

	1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes

	40 MHz	254 Mbps	247 Mbps	232 Mbps	200 Mbps	162 Mbps	136 Mbps

PBTC 111 Bidirectional_ HT-AMPDU _40MHz_SGI_Throughput

Title	Measure bi-directional HT AMPDU Throughput using 40MHz signals and SGI operational mode
Purpose	Measure the downstream AMPDU throughput that can be achieved on the SUT supporting HT clients operating 40MHz signals and using SGI mode.
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support AMPDU aggregation w/ BlockAck operation • SUT set up to support 40MHz channel bandwidth • SUT set up to support SGI operation • SUT setup to support simultaneous operation of HT and Legacy clients • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to SGI • Set client Channel bandwidth to 40MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption WPA2-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, and 1518 bytes • Run test with 2, 10, 20 and 50 clients; distributed equally between HT and non-HT clients

Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one) mapping with the bidirectional option checked 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 12 with WPA2-AES encryption modes 13. Repeat steps 5 to 12 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 14. Repeat steps 5 to 13 with Channel Models A and C
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput:

	1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
40 MHz	254 Mbps	247 Mbps	232 Mbps	200 Mbps	162 Mbps	136 Mbps

PBTC 112 Upstream_20MHz_LGI_Mixed-mode_Throughput

Title	Measure upstream throughput in mixed mode with non-HT (legacy) and HT clients operating 20MHz signals and LGI mode.
Purpose	Measure the upstream throughput that can be achieved on the SUT supporting HT and non-HT (legacy) clients operating signals with 20MHz channel width and guard interval set to LGI.
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade

	(WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to LGI • Set client Channel bandwidth to 20MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption and WPA-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, and 1518 bytes • Run test with 2, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 2 6. Set the initial number of Wi-Fi clients to 2 7. Select frame sizes of 88, 128, 256, 512, 1024, and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with WPA2-AES encryption mode 13. Repeat steps 5 to 12 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one)
Test Priority	Mandatory

Test Type	Performance						
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput:						
		1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
	20 MHz	108.89 Mbps	108.58 Mbps	99.28 Mbps	88.77 Mbps	67.95 Mbps	56.11 Mbps

PBTC 113 Downstream_ 20MHz_LGI_Mixed-mode_Throughput

Title	Measure downstream throughput in mixed mode with non-HT (legacy) and HT clients operating 20MHz signals and LGI mode.
Purpose	Measure the downstream throughput that can be achieved on the SUT supporting HT and non-HT (legacy) clients operating signals with 20MHz channel width and guard interval set to LGI.
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to LGI • Set client Channel bandwidth to 20MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption WPA-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024 and 1518 bytes • Run test with 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application

	2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024 and 1518 bytes and UDP traffic type 8. Select Ethernet to Wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 WPA2-AES encryption mode 13. Repeat steps 5 to 12 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one)
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput:

	1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
20 MHz	107.3 Mbps	106.96 Mbps	96.72 Mbps	80.7 Mbps	60.4 Mbps	49.23 Mbps

PBTC 114 Bidirectional_20MHz_LGI_Mixed-mode_Throughput

Title	Measure bi-directional mixed mode throughput in mixed mode with non-HT (legacy) and HT clients operating 20MHz signals and LGI mode.
Purpose	Measure the downstream throughput that can be achieved on the SUT supporting HT and non-HT (legacy) clients operating signals with 20MHz channel width and guard interval set to LGI.
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band

	• SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to LGI • Set client Channel bandwidth to 20MHz • Set client HT mode to "HT mixed" • Set client Channel Model to "Bypass" • Run test with no encryption and WPA-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, and 1518 bytes • Run test with 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one) mapping with the bidirectional option checked 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with WPA2-AES encryption mode 13. Repeat steps 5 to 12 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one)
Test Priority	Mandatory

Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput

	1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
20 MHz	105.76 Mbps	105.38 Mbps	94.28 Mbps	77.37 Mbps	56.73 Mbps	45.74 Mbps

PBTC 115 Upstream_40MHz_SGI_Mixed-mode_Throughput

Title	Measure upstream throughput in mixed mode with non-HT (legacy) and HT clients operating 40MHz signals and SGI mode.
Purpose	Measure the upstream throughput that can be achieved on the SUT supporting HT and non-HT (legacy) clients operating signals with 40MHz channel width and guard interval set to SGI.
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to SGI • Set client Channel bandwidth to 40MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption and WPA-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, and 1518 bytes • Run test with 2, 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application

	2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 2 6. Set the initial number of Wi-Fi clients to 2 7. Select frame sizes of 88, 128, 256, 512, 1024, and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with WPA2-AES encryption mode 13. Repeat steps 5 to 12 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one)
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput:

	1518	1024	512	256	128	88
40 MHz	218.62 Mbps	221.42 Mbps	192.38 Mbps	150.71 Mbps	104.77 Mbps	82.47 Mbps

PBTC 116 Downstream_ 40MHz_SGI_Mixed-mode_Throughput

Title	Measure downstream throughput in mixed mode with non-HT (legacy) and HT clients operating 40MHz signals and SGI mode.
Purpose	Measure the downstream throughput that can be achieved on the SUT supporting HT and non-HT (legacy) clients operating signals with 40MHz channel width and guard interval set to SGI..
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support UDP traffic • DHCP enabled

Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to SGI • Set client Channel bandwidth to 40MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption and WPA-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024 and 1518 bytes • Run test with 10, 20 and 50 clients
Procedure	1. Launch the WaveApps application 2. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024 and 1518 bytes and UDP traffic type 8. Select Ethernet to Wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with WPA2-AES encryption mode 13. Repeat steps 5 to 12 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one)
Test Priority	Mandatory
Test Type	Performance

Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput:						
		1518 bytes	1024 bytes	512 bytes	256 bytes	128 bytes	88 bytes
	40 MHz	212.30 Mbps	214.77 Mbps	182.98 Mbps	139.49 Mbps	94.24 Mbps	73.11 Mbps

PBTC 117 Bidirectional_40MHz_SGI_Mixed-mode_Throughput

Title	Measure bi-directional mixed mode throughput in mixed mode with non-HT (legacy) and HT clients operating 40MHz signals and SGI mode.
Purpose	Measure the downstream throughput that can be achieved on the SUT supporting HT and non-HT (legacy) clients operating signals with 40MHz channel width and guard interval set to SGI.
SUT Feature(s)	Maximum reliable data forwarding capacity, basic performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with 1x 802.11n WiFi Waveblade (WBW2000) and 1xEthernet Waveblade • SUT set up to operate in the 2.4GHz or 5GHz band • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Connect antenna ports on the 802.11n Wi-Fi WaveBlade to SUT via RF cables. This will vary depending on the SUT o Use 2 Ports A and B on WiFi WaveBlade if SUT supports just 2 antenna ports o Use 3 Ports A, B and C on WiFi WaveBlade if SUT supports 3 antenna ports • Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to MCS 15 • Set client Guard Interval to SGI • Set client Channel bandwidth to 40MHz • Set client HT mode to “HT mixed” • Set client Channel Model to “Bypass” • Run test with no encryption and WPA-AES • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, and 1518 bytes • Run test with 10, 20 and 50 clients
Procedure	Launch the WaveApps application

<table>
<tr><td></td><td>1. Select the Throughput Test under the IEEE 802.11.2 Benchmark Test Suite
2. Select the test port(s) (i.e., APs) to use for the test
3. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP
4. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1
5. Set the initial number of Wi-Fi clients to 1
6. Select frame sizes of 88, 128, 256, 512, 1024, and 1518 bytes and UDP traffic type
7. Select Wireless to Ethernet (one-to-one) mapping with the bidirectional option checked
8. Run the test
9. Wait until test completes
10. Collect report and results data
11. Repeat steps 5 to 11 with WPA2-AES encryption mode
12. Repeat steps 5 to 12 with 10, 20 and 50 clients configured on both Ethernet and Wi-Fi sides (one-to-one)</td></tr>
<tr><td>Test Priority</td><td>Mandatory</td></tr>
<tr><td>Test Type</td><td>Performance</td></tr>
<tr><td>Pass/Fail Criteria</td><td>An Enterprise Class/Carrier Grade SUT should achieve the following upstream throughput
<table>
<tr><td></td><td>1518 bytes</td><td>1024 bytes</td><td>512 bytes</td><td>256 bytes</td><td>128 bytes</td><td>88 bytes</td></tr>
<tr><td>40 MHz</td><td>206.35 Mbps</td><td>208.51 Mbps</td><td>174.47 Mbps</td><td>129.82 Mbps</td><td>85.62 Mbps</td><td>65.66 Mbps</td></tr>
</table></td></tr>
</table>

Packet Latency

The following latency tests measure the delay required for packets to be forwarded through the SUT using a variety of frame sizes under increasing client load. Delay-sensitive services such as streaming video and VoIP require low latency for a high-quality user experience. The latency tests present the SUT with an intended load for each frame size and measures the time it takes for each packet to travel from the source port to the destination port through the SUT.

The intended load is divided equally between SUT ports, and should be adjusted to be just below the SUT throughput (i.e., the value measured using a previous throughput test). The latency tests are conducted with a variety of frame sizes, numbers of clients, security modes, operating bands, and directions (i.e., upstream and downstream).

PBTC 015 Upstream_80211g_Packet_Latency

Title	Measure upstream packet latency
Purpose	Measure the packet latencies imposed on the WLAN client traffic by the SUT
SUT Feature(s) Tested	Buffering efficiency, datapath and forwarding performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients • Set intended load (ILOAD) for each frame size to 90% of the throughput of the SUT as obtained from the throughput tests. If the SUT throughput is unknown, use 802.3 defaults
Procedure	1. Launch the WaveApps application 2. Select the Latency Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Adjust the intended load (ILOAD) table to target traffic load as per test setup details above, with frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES

	encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should not impose a packet latency of more than 10 milliseconds under the specified loading in order to support delay-sensitive multimedia traffic.

PBTC 016 Downstream_80211g_Packet_Latency

Title	Measure downstream packet latency
Purpose	Measure the packet latencies imposed on the WLAN client traffic by the SUT
SUT Feature(s) Tested	Buffering efficiency, datapath and forwarding performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients • Set intended load (ILOAD) for each frame size to 90% of the throughput of the SUT as obtained from the throughput tests. If the SUT throughput is unknown, use 802.3 defaults
Procedure	1. Launch the WaveApps application 2. Select the Latency Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Adjust the intended load (ILOAD) table to target traffic load as per test setup details above, with frame sizes of 88, 128, 256,

	512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Ethernet to wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should not impose a packet latency of more than 10 milliseconds under the specified loading in order to support delay-sensitive multimedia traffic.

PBTC 017 Upstream_80211a_Packet_Latency

Title	Measure upstream packet latency
Purpose	Measure the packet latencies imposed on the WLAN client traffic by the SUT
SUT Feature(s) Tested	Buffering efficiency, datapath and forwarding performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients • Set intended load (ILOAD) for each frame size to 90% of the throughput of the SUT as obtained from the throughput tests. If the SUT throughput is unknown, use 802.3 defaults
Procedure	1. Launch the WaveApps application 2. Select the Latency Test under the IEEE 802.11.2 Benchmark Test Suite

	3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Adjust the intended load (ILOAD) table to target traffic load as per test setup details above, with frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should not impose a packet latency of more than 10 milliseconds under the specified loading in order to support delay-sensitive multimedia traffic.

PBTC 018 Downstream_80211a_Packet_Latency

Title	Measure downstream packet latency
Purpose	Measure the packet latencies imposed on the WLAN client traffic by the SUT
SUT Feature(s) Tested	Buffering efficiency, datapath and forwarding performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT to open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280

	and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients • Set intended load (ILOAD) for each frame size to 90% of the throughput of the SUT as obtained from the throughput tests. If the SUT throughput is unknown, use 802.3 defaults
Procedure	1. Launch the WaveApps application 2. Select the Latency Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Adjust the intended load (ILOAD) table to target traffic load as per test setup details above, with frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Ethernet to wireless (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should not impose a packet latency of more than 10 milliseconds under the specified loading in order to support delay-sensitive multimedia traffic.

Packet Loss

The packet loss tests measure the performance of the SUT at specific load factors for a variety of frame sizes. Two metrics are measured during a packet loss test: the forwarding rate and the packet loss ratio. The forwarding rate quantifies the rate at which packets are successfully received, while the packet loss ratio provides the percentage of dropped packets as a fraction of the injected packets. These measurements quantify the ability of the SUT to forward packets with low or zero loss over the entire range of traffic loads that may be placed upon it in an actual network.

The offered load is divided equally across SUT ports, and ranges from 20% to 100% of the (previously measured) throughput performance of the SUT at that frame size. That is, if the SUT throughput was measured at 10,000 frames/second at a specific frame size, the offered load should be set to 2,000, 4,000, 6,000, 8,000 and 10,000 frames/second. The packet loss tests are conducted with a variety of frame sizes, numbers of clients, security modes, operating bands, and directions (i.e., upstream and downstream).

PBTC 019 Upstream_80211g_Packet_Loss

Title	Measure upstream UDP packet loss
Purpose	Measure the forwarding rate and packet loss ratios for a range of offered loads over the traffic handling capacity of the SUT
SUT Feature(s) Tested	Uniform traffic handling capacity of datapath, anomalous forwarding performance at lower loads, instabilities
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients • For each frame size, set intended load (ILOAD) values to 10%, 20%, 40%, 60%, 80% and 100% of the throughput of the SUT as obtained from the throughput tests. If the SUT throughput is unknown, use the theoretical maximum medium capacity of the 802.11g channel for the specified frame size, multiplied by the number of SUT ports, as the throughput.
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1

	7. Select the initial frame size as 88 bytes, and UDP traffic type 8. Set up the ILOAD table values as described in the Test Setup section above 9. Select Wireless to Ethernet (one-to-one, upstream) mapping 10. Run the test 11. Wait until test completes 12. Collect report and results data 13. Repeat steps 7 to 12 with frame sizes of 128, 256, 512, 1024 and 1518 bytes 14. Repeat steps 7 to 13 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 15. Repeat steps 7 to 14 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should show under 1% packet loss at all frame sizes equal to or less than the measured throughput performance.

PBTC 020 Downstream_80211g_Packet_Loss

Title	Measure downstream UDP Packet Loss
Purpose	Measure the forwarding rate and packet loss ratios for a range of offered loads over the traffic handling capacity of the SUT
SUT Feature(s) Tested	Uniform traffic handling capacity of datapath, anomalous forwarding performance at lower loads, instabilities
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients • For each frame size, set intended load (ILOAD) values to 10%,

	20%, 40%, 60%, 80% and 100% of the throughput of the SUT as obtained from the throughput tests. If the SUT throughput is unknown, use the theoretical maximum medium capacity of the 802.11g channel for the specified frame size, multiplied by the number of SUT ports, as the throughput.
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select the initial frame size as 88 bytes, and UDP traffic type 8. Set up the ILOAD table values as described in the Test Setup section above 9. Select Wireless to Ethernet (one-to-one, downstream) mapping 10. Run the test 11. Wait until test completes 12. Collect report and results data 13. Repeat steps 7 to 12 with frame sizes of 128, 256, 512, 1024 and 1518 bytes 14. Repeat steps 7 to 13 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 15. Repeat steps 7 to 14 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should show under 1% packet loss at all frame sizes equal to or less than the measured throughput performance.

PBTC 021 Upstream_80211a_Packet_Loss

Title	Measure upstream UDP packet loss with
Purpose	Measure the forwarding rate and packet loss ratios for a range of offered loads over the traffic handling capacity of the SUT
SUT Feature(s) Tested	Uniform traffic handling capacity of datapath, anomalous forwarding performance at lower loads, instabilities

Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients • For each frame size, set intended load (ILOAD) values to 10%, 20%, 40%, 60%, 80% and 100% of the throughput of the SUT as obtained from the throughput tests. If the SUT throughput is unknown, use the theoretical maximum medium capacity of the 802.11g channel for the specified frame size, multiplied by the number of SUT ports, as the throughput.
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select the initial frame size as 88 bytes, and UDP traffic type 8. Set up the ILOAD table values as described in the Test Setup section above 9. Select Wireless to Ethernet (one-to-one, upstream) mapping 10. Run the test 11. Wait until test completes 12. Collect report and results data 13. Repeat steps 7 to 12 with frame sizes of 128, 256, 512, 1024 and 1518 bytes 14. Repeat steps 7 to 13 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 15. Repeat steps 7 to 14 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory

Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should show under 1% packet loss at all frame sizes equal to or less than the measured throughput performance.

PBTC 022 Downstream_80211a_Packet_Loss

Title	Measure downstream UDP Packet Loss
Purpose	Measure the forwarding rate and packet loss ratios for a range of offered loads over the traffic handling capacity of the SUT
SUT Feature(s) Tested	Uniform traffic handling capacity of datapath, anomalous forwarding performance at lower loads, instabilities
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients • For each frame size, set intended load (ILOAD) values to 10%, 20%, 40%, 60%, 80% and 100% of the throughput of the SUT as obtained from the throughput tests. If the SUT throughput is unknown, use the theoretical maximum medium capacity of the 802.11g channel for the specified frame size, multiplied by the number of SUT ports, as the throughput.
Procedure	1. Launch the WaveApps application 2. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select the initial frame size as 88 bytes, and UDP traffic type 8. Set up the ILOAD table values as described in the Test Setup section above

	9. Select Wireless to Ethernet (one-to-one, downstream) mapping 10. Run the test 11. Wait until test completes 12. Collect report and results data 13. Repeat steps 7 to 12 with frame sizes of 128, 256, 512, 1024 and 1518 bytes 14. Repeat steps 7 to 13 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 15. Repeat steps 7 to 14 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should show under 1% packet loss at all frame sizes equal to or less than the measured throughput performance.

Maximum Forwarding Rate

The maximum forwarding rate tests determine the absolute maximum rate (irrespective of packet losses) at which the SUT can receive and forward frames, for a variety of frame sizes and client counts. This test characterizes the ultimate capacity limits of the SUT datapath and queuing functions. The test results provide the maximum forwarding rates, in frames per second, for each tested frame size, plus the packet loss at that offered traffic load.

The offered load is divided equally across the SUT ports. That is, if the SUT throughput was measured at 10,000 frames/second at a specific frame size, the offered load should be set to 2,000, 4,000, 6,000, 8,000 and 10,000 frames/second. The maximum forwarding rate tests are conducted with a variety of frame sizes, numbers of clients, security modes, operating bands, and directions (i.e., upstream and downstream).

PBTC 023 Upstream_80211g_Max_Forwarding Rate

Title	Measure upstream UDP maximum forwarding rate
Purpose	Measure the maximum forwarding rate of the SUT for different frame sizes
SUT Feature(s) Tested	Absolute maximum traffic handling capacity of datapath and associated functions (MAC, queueing, switching, etc.)
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and

	Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients
Procedure	1. Launch the WaveApps application 2. Select the Maximum Forwarding Rate Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream maximum forwarding rate: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames >= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

PBTC 024 Downstream_80211g_Max_Forwarding Rate

Title	Measure downstream UDP maximum forwarding rate
Purpose	Measure the maximum forwarding rate of the SUT for different frame sizes
SUT Feature(s) Tested	Absolute maximum traffic handling capacity of datapath and associated functions (MAC, queueing, switching, etc.)
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients
Procedure	1. Launch the WaveApps application 2. Select the Maximum Forwarding Rate Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory

Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream maximum forwarding rate: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames >= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

PBTC 025 Upstream_80211a_Max_Forwarding Rate

Title	Measure upstream UDP maximum forwarding rate
Purpose	Measure the maximum forwarding rate of the SUT for different frame sizes
SUT Feature(s) Tested	Absolute maximum traffic handling capacity of datapath and associated functions (MAC, queueing, switching, etc.)
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients
Procedure	1. Launch the WaveApps application 2. Select the Maximum Forwarding Rate Test under the IEEE 802.11.2 Benchmark Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, upstream) mapping

	9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream maximum forwarding rate: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames >= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

PBTC 026 Downstream_80211a_Max_Forwarding Rate

Title	Measure downstream UDP maximum forwarding rate
Purpose	Measure the maximum forwarding rate of the SUT for different frame sizes
SUT Feature(s) Tested	Absolute maximum traffic handling capacity of datapath and associated functions (MAC, queueing, switching, etc.)
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Run test with no encryption, TKIP and AES-CCMP • Run test with UDP frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with 1, 10, 20, 100 and 500 clients
Procedure	1. Launch the WaveApps application 2. Select the Maximum Forwarding Rate Test under the IEEE 802.11.2 Benchmark Test Suite

	3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Wireless to Ethernet (one-to-one, downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve the following upstream maximum forwarding rate: >= 30 Mbps for 1518 byte frames >= 25 Mbps for 1024 byte frames >= 16 Mbps for 512 byte frames >= 9.9 Mbps for 256 byte frames >= 5.5 Mbps for 128 byte frames >= 3.8 Mbps for 88 byte frames

Maximum Stateful TCP Goodput

The TCP Goodput test measures the maximum number of bytes of TCP payload data that can be transferred per second by the SUT, at a fixed window size but using different maximum segment sizes (MSS). The test is performed with client counts in order to assess TCP performance at different network loading levels.

The TCP Goodput test expands on traditional MAC/IP (Layer 2 / Layer 3) throughput tests by measuring application throughput when using TCP over wireless LAN. For example, a frame that was successfully delivered at Layer 2 or Layer 3 may be dropped at Layer 4 because it was a duplicate or out-of-sequence TCP packet. Thus the TCP goodput (valid payload bytes per second) may be less than the Layer 2/3 throughput. As TCP is the most commonly observed WLAN traffic, the TCP Goodput test results enable users to determine the capacity of the SUT under real-world conditions..

The offered load is divided equally across the SUT ports; with multiple clients, each client presents the same load as all other clients. The TCP Goodput tests are conducted with a variety of maximum segment sizes, numbers of clients, security modes, operating bands and directions (i.e., upstream and downstream)..

PBTC 027 Upstream_80211g_Max_TCP_Goodput

Title	Measure maximum upstream TCP goodput
Purpose	Measure the maximum upstream TCP goodput of the SUT for different frame sizes and numbers of clients
SUT Feature(s) Tested	Application-level data handling performance with TCP traffic
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Set maximum number of sessions per client to 1 • Run test with no encryption, TKIP and AES-CCMP • Run test with TCP maximum segment sizes (MSS): 88, 216, 536, 984 and 1460 bytes • Run test with 1, 10, 20, 100 and 500 clients.
Procedure	1. Launch the WaveApps application 2. Select the TCP Goodput Test Test under the TCP Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select maximum segment sizes of 88, 216, 536, 984 and 1460 bytes 8. Set the number of sessions per client to 1 and the TCP window size to 65535 9. Select Wireless to Ethernet (one-to-one, upstream) mapping 10. Run the test 11. Wait until test completes

	12. Collect report and results data 13. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 14. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve an upstream TCP Goodput of at least 80% of the theoretical max with 1 client: >= 23.7 Mbps for 1460 byte MSS >= 19.3 Mbps for 984 byte MSS >= 13.3 Mbps for 536 byte MSS >= 6.6 Mbps for 216 byte MSS >= 2.9 Mbps for 88 byte MSS Multi-client results are generally expected to be lower than the above due to TCP windowing effects and contention.

PBTC 028 Downstream_80211g_Max_TCP_Goodput

Title	Measure maximum downstream TCP goodput
Purpose	Measure the maximum downstream TCP goodput of the SUT for different frame sizes and numbers of clients
SUT Feature(s) Tested	Application-level data handling performance with TCP traffic
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g-only mode • Set maximum number of sessions per client to 1 • Run test with no encryption, TKIP and AES-CCMP • Run test with TCP maximum segment sizes (MSS): 88, 216, 536, 984 and 1460 bytes • Run test with 1, 10, 20, 100 and 500 clients.
Procedure	1. Launch the WaveApps application 2. Select the TCP Goodput Test Test under the TCP Test Suite

	3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select maximum segment sizes of 88, 216, 536, 984 and 1460 bytes 8. Set the number of sessions per client to 1 and the TCP window size to 65535 9. Select Wireless to Ethernet (one-to-one, downstream) mapping 10. Run the test 11. Wait until test completes 12. Collect report and results data 13. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 14. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve an upstream TCP Goodput of at least 80% of the theoretical max with 1 client: >= 23.7 Mbps for 1460 byte MSS >= 19.3 Mbps for 984 byte MSS >= 13.3 Mbps for 536 byte MSS >= 6.6 Mbps for 216 byte MSS >= 2.9 Mbps for 88 byte MSS Multi-client results are generally expected to be lower than the above due to TCP windowing effects and contention.

PBTC 029 Upstream_80211a_Max_TCP_Goodput

Title	Measure maximum upstream TCP goodput
Purpose	Measure the maximum upstream TCP goodput of the SUT for different frame sizes and numbers of clients
SUT Feature(s) Tested	Application-level data handling performance with TCP traffic
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s)

	• SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Set maximum number of sessions per client to 1 • Run test with no encryption, TKIP and AES-CCMP • Run test with TCP maximum segment sizes (MSS): 88, 216, 536, 984 and 1460 bytes • Run test with 1, 10, 20, 100 and 500 clients.
Procedure	1. Launch the WaveApps application 2. Select the TCP Goodput Test Test under the TCP Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select maximum segment sizes of 88, 216, 536, 984 and 1460 bytes 8. Set the number of sessions per client to 1 and the TCP window size to 65535 9. Select Wireless to Ethernet (one-to-one, upstream) mapping 10. Run the test 11. Wait until test completes 12. Collect report and results data 13. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 14. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve an upstream TCP Goodput of at least 80% of the theoretical max with 1 client: >= 23.7 Mbps for 1460 byte MSS >= 19.3 Mbps for 984 byte MSS >= 13.3 Mbps for 536 byte MSS >= 6.6 Mbps for 216 byte MSS >= 2.9 Mbps for 88 byte MSS

	Multi-client results are generally expected to be lower than the above due to TCP windowing effects and contention.

PBTC 030 Downstream_80211a_Max_TCP_Goodput

Title	Measure maximum downstream TCP goodput
Purpose	Measure the maximum downstream TCP goodput of the SUT for different frame sizes and numbers of clients
SUT Feature(s) Tested	Application-level data handling performance with TCP traffic
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT with open authentication mode • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Set maximum number of sessions per client to 1 • Run test with no encryption, TKIP and AES-CCMP • Run test with TCP maximum segment sizes (MSS): 88, 216, 536, 984 and 1460 bytes • Run test with 1, 10, 20, 100 and 500 clients.
Procedure	1. Launch the WaveApps application 2. Select the TCP Goodput Test Test under the TCP Test Suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select maximum segment sizes of 88, 216, 536, 984 and 1460 bytes 8. Set the number of sessions per client to 1 and the TCP window size to 65535 9. Select Wireless to Ethernet (one-to-one, downstream) mapping 10. Run the test 11. Wait until test completes 12. Collect report and results data

	13. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 14. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should achieve an upstream TCP Goodput of at least 80% of the theoretical max with 1 client: >= 23.7 Mbps for 1460 byte MSS >= 19.3 Mbps for 984 byte MSS >= 13.3 Mbps for 536 byte MSS >= 6.6 Mbps for 216 byte MSS >= 2.9 Mbps for 88 byte MSS Multi-client results are generally expected to be lower than the above due to TCP windowing effects and contention.

Roaming Performance

The roaming performance tests measure the roaming delay, roaming failures and packet loss when the SUT is stressed with mobile clients transitioning between APs at a specified rate and security setup. The roaming measurement results therefore quantify the SUT's ability to support enterprise-class roaming traffic loads, such as large numbers of VoIP handsets.

The roaming clients continuously perform data transfers as they transition between APs in order to ensure a realistic traffic loading scenario. The test is conducted with a variety of roaming rates (i.e., roaming loads), numbers of clients, security modes and operating bands. A baseline roaming measurement is taken, after which variations are tested.

A set of "accelerated" measurements are also specified. These measurements test the efficacy of various roaming speedup mechanisms – proactive key caching, preauthentication, and PMKID caching – that may be implemented in the SUT. Note that these tests are only valid if the SUT actually implements one or more of the specified speedup mechanisms.

PBTC 031 Roaming_Delay_80211g_Baseline

Title	Establish baseline roaming delay, failures, and loss ratio
Purpose	Measures the minimum, maximum and average roaming delay, total number of roaming failures, and average packets lost per roam for the SUT when configured in 802.11g mode, and stressed with a roaming rate of 0.1 roams per second with 1 client using open security and no DHCP

SUT Feature(s) Tested	Basic roaming support and performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP disabled (static IP addressing)
Test Setup	• Configure the SUT with open authentication mode • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g mode • Set number of WLAN clients to 1 • Set security to none (open authentication, no encryption) • Set roaming rate to 0.1 roams/second
Procedure	1. Launch the WaveApps application 2. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Select SSID and configure 1 client for open authentication with no encryption, using a fixed IP address 5. Create an Ethernet client group on the correct port 6. Set the roam sequence to roam the client uniformly across all test ports 7. Set the roaming rate to 0.1 roams/second (for the entire SUT) and the test duration to 600 seconds (i.e., 60 roams) 8. Set the data traffic flow from Ethernet to wireless, with a frame size of 256 bytes and a flow rate of 100 pps (per client) 9. Run the test 10. Wait until test completes 11. Collect report and results data
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class SUT should complete this test with zero failed roams, packet loss ratio of under 1%, and an average roam delay of 10 milliseconds or less. The maximum roam delay should not exceed 50 milliseconds.

PBTC 032 Roaming_Delay_80211a_Baseline

Title	Establish baseline roaming delay, failures, and loss ratio
Purpose	Measures the minimum, maximum and average roaming delay, total number of roaming failures, and average packets lost per roam for the SUT when configured in 802.11g mode, and stressed with a roaming rate of 0.1 roams per second with 1 client using open security and no DHCP
SUT Feature(s) Tested	Basic roaming support and performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP disabled (static IP addressing)
Test Setup	• Configure the SUT with open authentication mode • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Set number of WLAN clients to 1 • Set security to none (open authentication, no encryption) • Set roaming rate to 0.1 roams/second
Procedure	1. Launch the WaveApps application 2. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Select SSID and configure 1 client for open authentication with no encryption, using a fixed IP address 5. Create an Ethernet client group on the correct port 6. Set the roam sequence to roam the client uniformly across all test ports 7. Set the roaming rate to 0.1 roams/second (for the entire SUT) and the test duration to 600 seconds (i.e., 60 roams) 8. Set the data traffic flow from Ethernet to wireless, with a frame size of 256 bytes and a flow rate of 100 pps (per client) 9. Run the test 10. Wait until test completes 11. Collect report and results data
Test Priority	Mandatory
Test Type	Performance

Pass/Fail Criteria	An Enterprise Class SUT should complete this test with zero failed roams, packet loss ratio of under 1%, and an average roam delay of 10 milliseconds or less. The maximum roam delay should not exceed 50 milliseconds.

PBTC 033 Roaming_Delay_80211g_Secure

Title	Determine variation of roaming delay, failures, and loss ratio with security modes and client counts
Purpose	Measures the minimum, maximum and average roaming delay, total number of roaming failures, and average packets lost per roam for the SUT when configured in 802.11g mode, and stressed with different numbers of clients, security modes and rates
SUT Feature(s) Tested	Roaming scalability with security
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP disabled (static IP addressing) • RADIUS server supporting LEAP, EAP/TLS, PEAP/MSCHAPv2, EAP/TTLS and EAP/FAST
Test Setup	• Configure the SUT with security modes to: WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g mode • Set WLAN client counts to: 10, 50, 100 and 500 • Set roaming rates to: 0.5, 1, and 5 roams/second
Procedure	1. Launch the WaveApps application 2. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Set the initial number of clients to 10 5. Select SSID and initially configure the clients for WEP-128 6. For TLS or TTLS security types, configure certificates on tester and SUT to match; for username/password types, configure a matching username and password. 7. Create an Ethernet client group on the correct port

	8. Set the roam sequence to roam all clients uniformly across all test ports, with a uniform initial client distribution 9. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams) 10. Set the data traffic flow from Ethernet to wireless, with a frame size of 256 bytes and a flow rate of 100 pps (per client) 11. Run the test 12. Wait until test completes 13. Collect reports and results data 14. Repeat steps 4 to 12 with 50, 100 and 500 clients 15. Repeat steps 4 to 13 with WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST security modes 16. Repeat steps 4 to 14 with 1 and 5 roams/second
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class SUT should complete this test with zero failed roams, packet loss ratio of under 10%, and an average roam delay of 100 milliseconds or less for any EAP type and 25 milliseconds or less for any PSK/WEP type. The maximum roam delay should not exceed 200 milliseconds for any client during any run.

PBTC 034 Roaming_Delay_80211a_Secure

Title	Determine variation of roaming delay, failures, and loss ratio with security modes and client counts
Purpose	Measures the minimum, maximum and average roaming delay, total number of roaming failures, and average packets lost per roam for the SUT when configured in 802.11a mode, and stressed with with different numbers of clients, security modes and rates
SUT Feature(s) Tested	Roaming scalability with security
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP disabled (static IP addressing) • RADIUS server supporting LEAP, EAP/TLS, PEAP/MSCHAPv2, EAP/TTLS and EAP/FAST
Test Setup	• Configure the SUT with security modes to: WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-

	MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Set WLAN client counts to: 10, 50, 100 and 500 • Set roaming rates to: 0.5, 1, and 5 roams/second
Procedure	1. Launch the WaveApps application 2. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Set the initial number of clients to 10 5. Select SSID and initially configure the clients for WEP-128 6. For TLS or TTLS security types, configure certificates on tester and SUT to match; for username/password types, configure a matching username and password. 7. Create an Ethernet client group on the correct port 8. Set the roam sequence to roam all clients uniformly across all test ports, with a uniform initial client distribution 9. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams) 10. Set the data traffic flow from Ethernet to wireless, with a frame size of 256 bytes and a flow rate of 100 pps (per client) 11. Run the test 12. Wait until the test completes 13. Collect reports and results data 14. Repeat steps 4 to 12 with 50, 100 and 500 clients 15. Repeat steps 4 to 13 with WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST security modes 16. Repeat steps 4 to 14 with 1 and 5 roams/second
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class SUT should complete this test with zero failed roams, packet loss ratio of under 10%, and an average roam delay of 100 milliseconds or less for any EAP type and 25 milliseconds or less for any PSK/WEP type. The maximum roam delay should not exceed 200 milliseconds for any client during any run.

PBTC 035 Roaming_Delay_80211g_DHCP

Title	Determine variation of roaming delay, failures, and loss ratio with security modes and client counts when using DHCP
Purpose	Measures the minimum, maximum and average roaming delay, total number of roaming failures, and average packets lost per roam for the SUT when configured in 802.11g mode with DHCP, and stressed with different numbers of clients and security modes
SUT Feature(s) Tested	Roaming scalability with DHCP support
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP server • RADIUS server supporting EAP/TLS and PEAP/MSCHAPv2
Test Setup	• Configure the SUT with security modes to: WPA-PSK, WPA2-PSK, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2 • Configure WLAN and Ethernet clients to use DHCP • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g mode • Set WLAN client counts to: 10, 50, 100 and 500 (Note: for 500 clients, subnet collision must be checked) • Set roaming rates to: 0.5, 1, and 4 roams/second
Procedure	1. Launch the WaveApps application 2. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Set the initial number of clients to 10 5. Select SSID and initially configure the clients for WPA-PSK and DHCP 6. For TLS or TTLS security types, configure certificates on tester and SUT to match; for username/password types, configure a matching username and password. 7. Create an Ethernet client group on the correct port 8. Set the roam sequence to roam all clients uniformly across all test ports, with a uniform initial client distribution 9. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams) 10. Set the data traffic flow from Ethernet to wireless, with a frame

	size of 256 bytes and a flow rate of 100 pps (per client) 11. Run the test 12. Wait until the test completes 13. Collect reports and results data 14. Repeat steps 4 to 12 with 50, 100 and 500 clients 15. Repeat steps 4 to 13 with WPA2-PSK, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2 security modes 16. Repeat steps 4 to 14 with 1 and 4 roams/second
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class SUT should complete this test with zero failed roams, packet loss ratio of under 10%, and an average roam delay of 100 milliseconds or less for any EAP type and 25 milliseconds or less for any PSK/WEP type. The maximum roam delay should not exceed 250 milliseconds for any client during any run.

PBTC 036 Roaming_Delay_80211a_DHCP

Title	Determine variation of roaming delay, failures, and loss ratio with security modes and client counts when using DHCP
Purpose	Measures the minimum, maximum and average roaming delay, total number of roaming failures, and average packets lost per roam for the SUT when configured in 802.11a mode with DHCP, and stressed with different numbers of clients and security modes
SUT Feature(s) Tested	Roaming scalability with DHCP support
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP server • RADIUS server supporting EAP/TLS and PEAP/MSCHAPv2
Test Setup	• Configure the SUT with security modes to: WPA-PSK, WPA2-PSK, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2 • Configure WLAN and Ethernet clients to use DHCP • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Set WLAN client counts to: 10, 50, 100 and 500 (Note: for 500 clients, subnet collision must be checked) • Set roaming rates to: 0.5, 1, and 4 roams/second

Procedure	1. Launch the WaveApps application 2. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Set the initial number of clients to 10 5. Select SSID and initially configure the clients for WPA-PSK and DHCP 6. For TLS or TTLS security types, configure certificates on tester and SUT to match; for username/password types, configure a matching username and password. 7. Create an Ethernet client group on the correct port 8. Set the roam sequence to roam all clients uniformly across all test ports, with a uniform initial client distribution 9. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams) 10. Set the data traffic flow from Ethernet to wireless, with a frame size of 256 bytes and a flow rate of 100 pps (per client) 11. Run the test 12. Wait until the test completes 13. Collect reports and results data 14. Repeat steps 4 to 12 with 50, 100 and 500 clients 15. Repeat steps 4 to 13 with WPA2-PSK, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2 security modes 16. Repeat steps 4 to 14 with 1 and 4 roams/second
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class SUT should complete this test with zero failed roams, packet loss ratio of under 10%, and an average roam delay of 100 milliseconds or less for any EAP type and 25 milliseconds or less for any PSK/WEP type. The maximum roam delay should not exceed 250 milliseconds for any client during any run.

PBTC 037 Roaming_Delay_80211g_Accel

Title	Determine variation of roaming delay, failures, and loss ratio with various security modes using various speedup mechanisms
Purpose	Measures the minimum, maximum and average roaming delay, total number of roaming failures, and average packets lost per roam for the SUT when configured in 802.11g mode and stressed

	with different numbers of clients and security modes. Different acceleration strategies: proactive key caching (PKC), preauthentication and PMKID caching are enabled to permit roaming delays to be reduced considerably.
SUT Feature(s) Tested	Performance improvements gained from roaming accelerations
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP server • RADIUS server supporting EAP/TLS and PEAP/MSCHAPv2
Test Setup	• Configure the SUT with security modes to: WPA-PSK, WPA2-PSK, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-TTLS • Configure static IP subnets in the SUT and related network • Configure one or more of the SUT speedup mechanisms such as proactive key caching, preauthentication and PMKID caching • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g mode • Set WLAN client counts to: 10, 50, 100 and 500 (Note: for 500 clients, subnet collision must be checked) • Set roaming rates to: 0.5, 1, and 4 roams/second • Set proactive key caching, preauthentication and PMKID caching during different trials
Procedure	1. Launch the WaveApps application 2. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Set the initial number of clients to 10 5. Select SSID and initially configure the clients for WPA-PSK and a fixed IP (set as per SUT requirements) 6. For TLS or TTLS security types, configure certificates on tester and SUT to match; for username/password types, configure a matching username and password. 7. Create an Ethernet client group on the correct port 8. Set the roam sequence to roam all clients uniformly across all test ports, with a uniform initial client distribution 9. Enable proactive key caching for all clients 10. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams)

	11. Set the data traffic flow from Ethernet to wireless, with a frame size of 256 bytes and a flow rate of 100 pps (per client) 12. Run the test 13. Wait until the test completes 14. Collect reports and results data 15. Repeat steps 4 to 13 with 50, 100 and 500 clients 16. Repeat steps 4 to 14 with WPA2-PSK, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-TTLS security modes 17. Repeat steps 4 to 15 with 1 and 4 roams/second 18. Disable proactive key caching, enable preauthentication, and repeat steps 4 to 16 19. Disable preauthentication, enable PMKID caching, and repeat steps 4 to 16
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class SUT should implement at least one accelerated roaming mode, and should demonstrate a significant improvement in the accelerated results as compared to the unaccelerated results. More specifically, it should complete this test with at least one set of trials showing zero failed roams, packet loss ratio of under 1%, and an average roam delay of 20 milliseconds or less for any EAP or PSK type tested. The maximum roam delay should not exceed 25 milliseconds for any client during this same trial.

PBTC 038 Roaming_Delay_80211a_Accel

Title	Determine variation of roaming delay, failures, and loss ratio with various security modes using various speedup mechanisms
Purpose	Measures the minimum, maximum and average roaming delay, total number of roaming failures, and average packets lost per roam for the SUT when configured in 802.11a mode and stressed with different numbers of clients and security modes. Different acceleration strategies: proactive key caching (PKC), preauthentication and PMKID caching are enabled to permit roaming delays to be reduced considerably.
SUT Feature(s) Tested	Performance improvements gained from roaming accelerations
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP server

	• RADIUS server supporting EAP/TLS and PEAP/MSCHAPv2
Test Setup	• Configure the SUT with security modes to: WPA-PSK, WPA2-PSK, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-TTLS • Configure static IP subnets in the SUT and related network • Configure one or more of the SUT speedup mechanisms such as proactive key caching, preauthentication and PMKID caching • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Set WLAN client counts to: 10, 50, 100 and 500 (Note: for 500 clients, subnet collision must be checked) • Set roaming rates to: 0.5, 1, and 4 roams/second • Set proactive key caching, preauthentication and PMKID caching during different trials
Procedure	1. Launch the WaveApps application 2. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Set the initial number of clients to 10 5. Select SSID and initially configure the clients for WPA-PSK and a fixed IP (set as per SUT requirements) 6. For TLS or TTLS security types, configure certificates on tester and SUT to match; for username/password types, configure a matching username and password. 7. Create an Ethernet client group on the correct port 8. Set the roam sequence to roam all clients uniformly across all test ports, with a uniform initial client distribution 9. Enable proactive key caching for all clients 10. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams) 11. Set the data traffic flow from Ethernet to wireless, with a frame size of 256 bytes and a flow rate of 100 pps (per client) 12. Run the test 13. Wait until the test completes 14. Collect reports and results data 15. Repeat steps 4 to 13 with 50, 100 and 500 clients 16. Repeat steps 4 to 14 with WPA2-PSK, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-TTLS security modes 17. Repeat steps 4 to 15 with 1 and 4 roams/second

	18. Disable proactive key caching, enable preauthentication, and repeat steps 4 to 16 19. Disable preauthentication, enable PMKID caching, and repeat steps 4 to 16
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class SUT should implement at least one accelerated roaming mode, and should demonstrate a significant improvement in the accelerated results as compared to the unaccelerated results. More specifically, it should complete this test with at least one set of trials showing zero failed roams, packet loss ratio of under 1%, and an average roam delay of 20 milliseconds or less for any EAP or PSK type tested. The maximum roam delay should not exceed 25 milliseconds for any client during this same trial.

PBTC 039 Roaming_Delay_80211g_MultiSSID

Title	Determine variation of roaming delay, failures, and loss ratio with multiple concurrently active security modes
Purpose	Measures the minimum, maximum and average roaming delay, total number of roaming failures, and average packets lost per roam for the SUT when configured in 802.11g mode and stressed with different numbers of clients and security modes. Multiple SSIDs associated with different security modes are configured to represent actual conditions in a live network.
SUT Feature(s) Tested	Sustained performance with multiple overlay WLANs with different traffic types
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP server • RADIUS server supporting EAP/TLS and PEAP/MSCHAPv2
Test Setup	• Configure the SUT with 2 different SSIDs supporting combinations of 6 different security modes matching: Open (no security), WEP-128, WPA2-PSK, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g mode • Set total WLAN client counts to: 10, 50, 100 and 500 (Note: for 500 clients, subnet collision must be checked)

	• Set roaming rates to: 0.5, 1, and 4 roams/second • Set proactive key caching, preauthentication and PMKID caching during different trials
Procedure	1. Launch the WaveApps application 2. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Set the initial number of clients to 10 in 2 groups of 5 each 5. Configure two different SSIDs in the SUT, referred to here as “SSID-A” and “SSID-B”; set up IP subnets and VLANs as appropriate to support these two SSIDs 6. Set SSID-A in the SUT to initially support Open, configure one client group to match this SSID and security, and configure a fixed IP (per SUT requirements) for this group 7. Set SSID-B in the SUT to initially support WPA-PEAP-MSCHAPv2, configure the second client group to match this SSID and security, and configure a fixed IP (per SUT requirements) for this group 8. If TLS or TTLS security types are set per above, configure certificates on tester and SUT to match; for username/ password types, configure a matching username and password. 9. Create an Ethernet client group on the correct port 10. Set the roam sequence to roam all clients uniformly across all test ports, with a uniform initial client distribution 11. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams) 12. Set the data traffic flow from Ethernet to wireless, with a frame size of 256 bytes and a flow rate of 100 pps (per client) 13. Run the test 14. Wait until the test completes 15. Collect reports and results data 16. Repeat steps 4 to 15 with 50, 100 and 500 clients, organized in 2 groups of 25, 50 and 250 clients, respectively 17. Repeat steps 4 to 16 with 1 and 4 roams/second 18. Repeat steps 4 to 17 with SSID-A set to WEP-128 and SSID-B set to WPA2-EAP-TLS 19. Repeat steps 4 to 17 with SSID-A set to WPA2-PSK and SSID-B set to WPA2-EAP-TTLS
Test Priority	Mandatory

Test Type	Performance
Pass/Fail Criteria	An Enterprise Class SUT should complete this test with zero failed roams, packet loss ratio of under 10%, and an average roam delay of 100 milliseconds or less for any EAP type and 25 milliseconds or less for any PSK/WEP type. The maximum roam delay should not exceed 200 milliseconds for any client during any run.

PBTC 040 Roaming_Delay_80211a_MultiSSID

Title	Determine variation of roaming delay, failures, and loss ratio with multiple concurrently active security modes
Purpose	Measures the minimum, maximum and average roaming delay, total number of roaming failures, and average packets lost per roam for the SUT when configured in 802.11a mode and stressed with different numbers of clients and security modes. Multiple SSIDs associated with different security modes are configured to represent actual conditions in a live network.
SUT Feature(s) Tested	Sustained performance with multiple overlay WLANs with different traffic types
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP server • RADIUS server supporting EAP/TLS and PEAP/MSCHAPv2
Test Setup	• Configure the SUT with 2 different SSIDs supporting combinations of 6 different security modes matching: Open (no security), WEP-128, WPA2-PSK, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Set total WLAN client counts to: 10, 50, 100 and 500 (Note: for 500 clients, subnet collision must be checked) • Set roaming rates to: 0.5, 1, and 4 roams/second • Set proactive key caching, preauthentication and PMKID caching during different trials
Procedure	1. Launch the WaveApps application 2. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Set the initial number of clients to 10 in 2 groups of 5 each

	5. Configure two different SSIDs in the SUT, referred to here as “SSID-A” and “SSID-B”; set up IP subnets and VLANs as appropriate to support these two SSIDs 6. Set SSID-A in the SUT to initially support Open, configure one client group to match this SSID and security, and configure a fixed IP (per SUT requirements) for this group 7. Set SSID-B in the SUT to initially support WPA-PEAP-MSCHAPv2, configure the second client group to match this SSID and security, and configure a fixed IP (per SUT requirements) for this group 8. If TLS or TTLS security types are set per above, configure certificates on tester and SUT to match; for username/ password types, configure a matching username and password. 9. Create an Ethernet client group on the correct port 10. Set the roam sequence to roam all clients uniformly across all test ports, with a uniform initial client distribution 11. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams) 12. Set the data traffic flow from Ethernet to wireless, with a frame size of 256 bytes and a flow rate of 100 pps (per client) 13. Run the test 14. Wait until the test completes 15. Collect reports and results data 16. Repeat steps 4 to 15 with 50, 100 and 500 clients, organized in 2 groups of 25, 50 and 250 clients, respectively 17. Repeat steps 4 to 16 with 1 and 4 roams/second 18. Repeat steps 4 to 17 with SSID-A set to WEP-128 and SSID-B set to WPA2-EAP-TLS 19. Repeat steps 4 to 17 with SSID-A set to WPA2-PSK and SSID-B set to WPA2-EAP-TTLS
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Class SUT should complete this test with zero failed roams, packet loss ratio of under 10%, and an average roam delay of 100 milliseconds or less for any EAP type and 25 milliseconds or less for any PSK/WEP type. The maximum roam delay should not exceed 200 milliseconds for any client during any run.

Mesh Per-Hop and Aggregate Throughput

The following mesh throughput tests measure the maximum rate at which the mesh SUT can forward packets without loss, both on a per-hop basis (i.e., individually for each mesh AP) and an aggregate basis (i.e., collectively for all mesh APs taken as a whole). These throughput tests are key measurements of the performance of a mesh SUT under real-world conditions. For example, even small amounts of packet loss can cause TCP sessions to ratchet down their goodput considerably, and sometimes even enter slow-start mode (with very low transfer rates). These tests are hence indicative of how much traffic and how many users the SUT can support, and also of internal issues with the SUT forwarding datapaths and routing algorithms.

Also see the section dealing with tests on interference effects. Note that interference effects are not applied to the tests in this section.

The mesh throughput tests are conducted with different frame sizes, numbers of clients, security modes, and directions (i.e., upstream, downstream and bi-directional). They are also carried out with different traffic types (i.e., UDP and TCP).

Note that the test cases must be performed in the appropriate band used for client and subscriber access to the SUT. In many cases, this is the 802.11b/g channel set (2.4 GHz).

PBTC 041 Upstream_UDP_Per-Hop_Throughput

Title	Measure upstream UDP mesh throughput per-hop
Purpose	Measure the upstream UDP per-hop mesh throughput that can be achieved by the SUT; this gives the sustainable uplink bandwidth per subscriber AP
SUT Feature(s) Tested	Maximum per-hop mesh data forwarding capacity, mesh routing performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/sPHY rate • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application

	2. Select the Mesh Per-Hop Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Mesh Hops to Mesh Gateway (upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve an upstream throughput per hop that is at least 50% of the theoretical maximum for the channel: >= 15 Mbps for 1518 byte frames >= 12.5 Mbps for 1024 byte frames >= 8 Mbps for 512 byte frames >= 4.5 Mbps for 256 byte frames >= 2.75 Mbps for 128 byte frames >= 1.9 Mbps for 88 byte frames

PBTC 042 Downstream_UDP_Per-Hop_Throughput

Title	Measure downstream UDP mesh throughput per-hop
Purpose	Measure the downstream UDP per-hop mesh throughput that can be achieved by the SUT; this provides the sustainable downlink capacity of the mesh system as seen by each subscriber AP
SUT Feature(s) Tested	Maximum per-hop mesh data forwarding capacity, mesh routing performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s)

	• SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/sPHY rate • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Per-Hop Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Mesh Gateway to Mesh Hops (downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve a downstream throughput per hop that is at least 75% of the theoretical maximum for the channel: >= 22.5 Mbps for 1518 byte frames >= 18.8 Mbps for 1024 byte frames >= 12 Mbps for 512 byte frames >= 7.4 Mbps for 256 byte frames

	>= 4.1 Mbps for 128 byte frames >= 2.9 Mbps for 88 byte frames

PBTC 043 Bidirectional_UDP_Per-Hop_Throughput

Title	Measure bidirectional UDP mesh throughput per-hop
Purpose	Measure the bidirectional UDP per-hop mesh throughput that can be achieved by the SUT; this gives the sustainable uplink bandwidth per subscriber AP
SUT Feature(s) Tested	Maximum per-hop mesh data forwarding capacity, mesh routing performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Per-Hop Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Mesh Hops to Mesh Gateway traffic mapping with bidirectional mode 9. Run the test 10. Wait until test completes

	11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve a bidirectional throughput per hop that is at least 50% of the theoretical maximum for the channel: >= 15 Mbps for 1518 byte frames >= 12.5 Mbps for 1024 byte frames >= 8 Mbps for 512 byte frames >= 4.5 Mbps for 256 byte frames >= 2.75 Mbps for 128 byte frames >= 1.9 Mbps for 88 byte frames Note that bidirectional throughput may be lower than downstream throughput due to contention effects.

PBTC 044 Upstream_TCP_Per-Hop_Throughput

Title	Measure upstream TCP mesh throughput per-hop
Purpose	Measure the upstream TCP per-hop mesh throughput that can be achieved by the SUT; this gives the uplink bandwidth per subscriber AP as seen by TCP applications.
SUT Feature(s) Tested	Maximum per-hop mesh data forwarding capacity, mesh TCP performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/sPHY rate • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application

	2. Select the Mesh Per-Hop Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and TCP traffic type 8. Select Mesh Hops to Mesh Gateway (upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve an upstream throughput per hop that is at least 50% of the theoretical maximum for the channel: >= 15 Mbps for 1518 byte frames >= 12.5 Mbps for 1024 byte frames >= 8 Mbps for 512 byte frames >= 4.5 Mbps for 256 byte frames >= 2.75 Mbps for 128 byte frames >= 1.9 Mbps for 88 byte frames

PBTC 045 Downstream_TCP_Per-Hop_Throughput

Title	Measure downstream TCP mesh throughput per-hop
Purpose	Measure the downstream TCP per-hop mesh throughput that can be achieved by the SUT; this provides the sustainable downlink capacity of the mesh system as seen by TCP applications running on the subscriber stations.
SUT Feature(s) Tested	Maximum per-hop mesh data forwarding capacity, mesh TCP performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and

	Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Per-Hop Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and TCP traffic type 8. Select Mesh Gateway to Mesh Hops (downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve a downstream throughput per hop that is at least 75% of the theoretical maximum for the channel: >= 22.5 Mbps for 1518 byte frames >= 18.8 Mbps for 1024 byte frames >= 12 Mbps for 512 byte frames

	>= 7.4 Mbps for 256 byte frames >= 4.1 Mbps for 128 byte frames >= 2.9 Mbps for 88 byte frames

PBTC 046 Bidirectional_TCP_Per-Hop_Throughput

Title	Measure bidirectional TCP mesh throughput per-hop
Purpose	Measure the bidirectional TCP per-hop mesh throughput that can be achieved by the SUT; this gives the sustainable uplink bandwidth per subscriber as seen by TCP applications
SUT Feature(s) Tested	Maximum per-hop mesh data forwarding capacity, mesh routing performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Per-Hop Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and TCP traffic type 8. Select Mesh Hops to Mesh Gateway traffic mapping with bidirectional mode 9. Run the test

	10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve a bidirectional throughput per hop that is at least 50% of the theoretical maximum for the channel: >= 15 Mbps for 1518 byte frames >= 12.5 Mbps for 1024 byte frames >= 8 Mbps for 512 byte frames >= 4.5 Mbps for 256 byte frames >= 2.75 Mbps for 128 byte frames >= 1.9 Mbps for 88 byte frames Note that bidirectional throughput may be lower than downstream throughput due to contention effects.

PBTC 047 Upstream_UDP_Aggregate_Throughput

Title	Measure upstream UDP mesh throughput on an aggregate basis
Purpose	Measure the upstream UDP aggregate mesh throughput that can be achieved by the SUT; this gives the throughput capacity of the entire mesh network SUT
SUT Feature(s) Tested	Total mesh data forwarding capacity, mesh routing performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes

Procedure	1. Launch the WaveApps application 2. Select the Mesh Aggregate Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Mesh Hops to Mesh Gateway (upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve a upstream UDP throughput that is at least 50% of the theoretical maximum for all of the uplink channels put together: >= 15 Mbps for 1518 byte frames >= 12.5 Mbps for 1024 byte frames >= 8 Mbps for 512 byte frames >= 4.5 Mbps for 256 byte frames >= 2.75 Mbps for 128 byte frames >= 1.9 Mbps for 88 byte frames If the number of subscriber access channels is less than the number of uplink channels, then use that number instead.

PBTC 048 Downstream_UDP_Aggregate_Throughput

Title	Measure downstream UDP mesh throughput on an aggregate basis
Purpose	Measure the downstream UDP aggregate mesh throughput that can be achieved by the SUT; this gives the throughput capacity of the entire mesh network SUT
SUT Feature(s) Tested	Total mesh data forwarding capacity, mesh routing performance

Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Aggregate Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Mesh Gateway to Mesh Hops (downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve a downstream UDP throughput that is at least 75% of the theoretical maximum for all of the uplink channels put together:

	>= 22.5 Mbps for 1518 byte frames >= 18.8 Mbps for 1024 byte frames >= 12 Mbps for 512 byte frames >= 7.4 Mbps for 256 byte frames >= 4.1 Mbps for 128 byte frames >= 2.9 Mbps for 88 byte frames If the number of subscriber access channels is less than the number of uplink channels, then use that number instead.

PBTC 049 Bidirectional_UDP_Aggregate_Throughput

Title	Measure bidirectional UDP mesh throughput on an aggregate basis
Purpose	Measure the bidirectional UDP aggregate mesh throughput that can be achieved by the SUT; this gives the throughput capacity of the entire mesh network SUT
SUT Feature(s) Tested	Total mesh data forwarding capacity, mesh routing performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Aggregate Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518

	bytes and UDP traffic type 8. Select Mesh Hops to Mesh Gateway traffic mapping with bidirectional mode 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve a bidirectional UDP throughput that is at least 50% of the theoretical maximum for all of the uplink channels put together: >= 15 Mbps for 1518 byte frames >= 12.5 Mbps for 1024 byte frames >= 8 Mbps for 512 byte frames >= 4.5 Mbps for 256 byte frames >= 2.75 Mbps for 128 byte frames >= 1.9 Mbps for 88 byte frames Note that bidirectional throughput may be lower than downstream throughput due to contention effects. If the number of subscriber access channels is less than the number of uplink channels, then use that number instead.

PBTC 050 Upstream_TCP_Aggregate_Throughput

Title	Measure upstream TCP mesh throughput on an aggregate basis
Purpose	Measure the upstream TCP aggregate mesh throughput that can be achieved by the SUT; this gives the throughput capacity of the entire mesh network SUT as seen by TCP applications.
SUT Feature(s) Tested	Total mesh data forwarding capacity, mesh TCP performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or

	6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Aggregate Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and TCP traffic type 8. Select Mesh Hops to Mesh Gateway (upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve a upstream TCP throughput that is at least 50% of the theoretical maximum for all of the uplink channels put together: >= 15 Mbps for 1518 byte frames >= 12.5 Mbps for 1024 byte frames >= 8 Mbps for 512 byte frames >= 4.5 Mbps for 256 byte frames >= 2.75 Mbps for 128 byte frames >= 1.9 Mbps for 88 byte frames If the number of subscriber access channels is less than the number of uplink channels, then use that number instead.

PBTC 051 Downstream_TCP_Aggregate_Throughput

Title	Measure downstream TCP mesh throughput on an aggregate

	basis
Purpose	Measure the downstream TCP aggregate mesh throughput that can be achieved by the SUT; this gives the throughput capacity of the entire mesh network SUT as seen by TCP applications.
SUT Feature(s) Tested	Total mesh data forwarding capacity, mesh TCP performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Aggregate Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and TCP traffic type 8. Select Mesh Gateway to Mesh Hops (downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs

Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve a downstream TCP throughput that is at least 75% of the theoretical maximum for all of the uplink channels put together: >= 22.5 Mbps for 1518 byte frames >= 18.8 Mbps for 1024 byte frames >= 12 Mbps for 512 byte frames >= 7.4 Mbps for 256 byte frames >= 4.1 Mbps for 128 byte frames >= 2.9 Mbps for 88 byte frames If the number of subscriber access channels is less than the number of uplink channels, then use that number instead.

PBTC 052 Bidirectional_TCP_Aggregate_Throughput

Title	Measure bidirectional TCP mesh throughput on an aggregate basis
Purpose	Measure the bidirectional TCP aggregate mesh throughput that can be achieved by the SUT; this gives the throughput capacity of the entire mesh network SUT as seen by TCP applications.
SUT Feature(s) Tested	Total mesh data forwarding capacity, mesh TCP performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support TCP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Aggregate Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP

	5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and TCP traffic type 8. Select Mesh Hops to Mesh Gateway traffic mapping with bidirectional mode 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade mesh SUT should achieve a bidirectional TCP throughput that is at least 50% of the theoretical maximum for all of the uplink channels put together: >= 15 Mbps * number of channels for 1518 byte frames >= 12.5 Mbps for 1024 byte frames >= 8 Mbps for 512 byte frames >= 4.5 Mbps for 256 byte frames >= 2.75 Mbps for 128 byte frames >= 1.9 Mbps for 88 byte frames Note that bidirectional throughput may be lower than downstream throughput due to contention effects. If the number of subscriber access channels is less than the number of uplink channels, then use that number instead.

Mesh Per-Hop and Aggregate Packet Latency

The following mesh latency tests measure the delay required for packets to be forwarded through the SUT, both on a per-hop basis (i.e., individually for each mesh AP) and an aggregate basis (i.e., collectively for all mesh APs taken as a whole), under increasing client load. Delay-sensitive services such as streaming video and VoIP require low latency for a high-quality user experience. The latency tests present the SUT with an intended load for each frame size and measures the time it takes for each packet to travel from the source port to the destination port through the SUT.

Also see the section dealing with tests on interference effects. Note that interference effects are not applied to the tests in this section.

The intended load is divided equally between SUT ports, and should be adjusted to be just below the SUT throughput (i.e., the value measured using a previous throughput test). The latency tests are conducted with a variety of frame sizes, numbers of clients, security modes, and directions (i.e., upstream and downstream). Only UDP traffic is used for these latency tests.

Note that the test cases must be performed in the appropriate band used for client and subscriber access to the SUT. In many cases, this is the 802.11b/g channel set (2.4 GHz).

PBTC 053 Upstream_UDP_Per-Hop_Latency

Title	Measure upstream UDP mesh latency per-hop
Purpose	Measure the upstream UDP per-hop mesh latency that can be achieved through the SUT; this gives the latency seen by individual subscribers.
SUT Feature(s) Tested	Mesh per-hop buffering and forwarding efficiency and delays, mesh routing efficacy
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Per-Hop Latency Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1

	7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Mesh Hops to Mesh Gateway (upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade SUT should not impose a packet latency of more than 50 milliseconds from any hop to the portal under the specified loading, in order to support delay-sensitive voice and multimedia traffic.

PBTC 054 Downstream_UDP_Per-Hop_Latency

Title	Measure downstream UDP mesh latency per-hop
Purpose	Measure the downstream UDP per-hop mesh latency that can be achieved through the SUT; this gives the latency seen by individual subscribers.
SUT Feature(s) Tested	Mesh per-hop buffering and forwarding efficiency and delays, mesh routing efficacy
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application

	2. Select the Mesh Per-Hop Latency Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Mesh Gateway to Mesh Hops (downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade SUT should not impose a packet latency of more than 50 milliseconds from the portal to any hop under the specified loading, in order to support delay-sensitive voice and multimedia traffic.

PBTC 055 Upstream_UDP_Aggregate_Latency

Title	Measure upstream UDP mesh latency on an aggregate basis
Purpose	Measure the aggregate minimum, maximum and average upstream UDP latency that can be achieved through the entire mesh SUT; this gives the latency for the whole network.
SUT Feature(s) Tested	Mesh forwarding efficiency and delays, mesh routing performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points

	- Configure the SUT with open authentication - Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) - Set client PHY rate to 54 Mb/s - Run test with no cipher and open authentication - Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Aggregate Latency Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Mesh Hops to Mesh Gateway (upstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade SUT should not impose a maximum packet latency of more than 50 milliseconds under the specified loading, in order to support delay-sensitive voice and multimedia traffic.

PBTC 056 Downstream_UDP_Aggregate_Latency

Title	Measure downstream UDP mesh latency on an aggregate basis
Purpose	Measure the aggregate minimum, maximum and average downstream UDP latency that can be achieved through the entire mesh SUT; this gives the latency for the whole network.

SUT Feature(s) Tested	Mesh forwarding efficiency and delays, mesh routing performance
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT in mesh configuration with at least two access points • Configure the SUT with open authentication • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client PHY rate to 54 Mb/s • Run test with no cipher and open authentication • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes
Procedure	1. Launch the WaveApps application 2. Select the Mesh Aggregate Latency Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the test and configure into 802.11g or 802.11a mode as required 4. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 6. Set the initial number of Wi-Fi clients to 1 7. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 8. Select Mesh Gateway to Mesh Hops (downstream) mapping 9. Run the test 10. Wait until test completes 11. Collect report and results data 12. Repeat steps 5 to 11 with 10, 20, 100 and 500 clients configured on both Ethernet and Wi-Fi sides (one-to-one) 13. Repeat steps 5 to 12 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory for Mesh SUTs
Test Type	Performance
Pass/Fail Criteria	A Carrier Grade SUT should not impose a maximum packet latency of more than 50 milliseconds under the specified loading, in order to support delay-sensitive voice and multimedia traffic.

Quality of Service

The following Quality of Service (QoS) tests measure the low-level QoS performance of the SUT, in terms of the ability of the SUT to distinguish between low-QoS flows and high-QoS flows, to isolate the high-QoS flows from the low-QoS flows, and to support large numbers of roaming VoIP handsets.

A high degree of isolation is essential in enterprise-class networks in order to insure that low-priority best-efforts traffic will not adversely impact critical voice and/or video streams. Failure to support QoS differentiation with high performance leads to dropped calls, poor call quality, and jerky or unusable video.

Modern enterprise WLAN infrastructures are often called upon to support VoIP handsets. An essential component of the VoIP user experience is mobility; handsets are expected to roam seamlessly between APs during use to ensure that users can maintain their phone conversations as they move about within a building or campus. It is therefore necessary to verify that mobility is supported without impacting call quality or causing call drops.

The QoS tests are conducted with a variety of numbers of clients and security modes; the service differentiation tests test different frame sizes, while the roaming tests configure different roaming rates. Only UDP traffic is used, as most delay-sensitive traffic is UDP. These tests are only applicable to SUTs that support WMM/802.11e QoS functions.

PBTC 059 VoIP_SLA_Assurance

Title	Measure voice SLA assurance under high data load conditions
Purpose	Determine the degree to which a specified service level agreement (SLA) is met by the SUT for a predetermined number of voice calls when the SUT is simultaneously loaded with high levels of best efforts data traffic. The SLA is expressed in terms of an objective voice quality measure (R-value).
SUT Feature(s) Tested	Voice/data prioritization, QoS implementation efficacy, forwarding datapath capabilities
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support 2 (or more) QoS levels and UDP traffic with static IP addresses
Test Setup	• Configure the SUT with open authentication • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g APs, if present) or 6Mbps, 12Mbps and 24Mbps (802.11a APs, if present)

	• Enable WMM/802.11e and 802.1Q prioritization on the SUT with the number of QoS classes being at least 2 (Best Efforts and Voice); each WMM/802.11e AC should correspond to a different SSID configured on the SUT • Set the SLA for the test as: minimum R-value of 78 • Run test with no encryption, TKIP and AES-CCMP • Run test with 1, 10 and 50 clients per AP • Run test with Best Efforts TCP traffic frame sizes: 88, 128, 256, 512, 1024 and 1518 bytes • Run test with 1 and 10 voice calls per AP • Run test with G.711, G.723 and G.729 voice codec types
Procedure	1. Launch the WaveApps application 2. Select the Service Assurance Test under the VoIP QoS test suite 3. Select the test port(s) (i.e., APs) to use for the test 4. Select SSID and configure WLAN clients to obtain IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the number of Ethernet clients set to 1 6. Set the voice call traffic to use WLAN QoS with user priority 6 and the background traffic to use WLAN QoS with user priority 0 7. Set the other traffic QoS settings (TOS, DSCP, port numbers) to match the SUT requirements 8. Set the initial Wi-Fi security mode to open (no security) 9. Set the initial number of Wi-Fi clients to 1 per AP 10. Select the initial background traffic frame size as 88 bytes, and TCP traffic type 11. Set the initial codec type to G.711 12. Set the initial number of calls per AP to 1 13. Run the test 14. Wait until test completes 15. Collect report and results data 16. Repeat steps 13 to 15 with 10 voice calls per AP 17. Repeat steps 12 to 16 with G.723 and G.729 codec types 18. Repeat steps 11 to 17 with frame sizes 128, 256, 512, 1024 and 1518 bytes 19. Repeat steps 10 to 18 with 10 and 100 Wi-Fi clients per AP 20. Repeat steps 9 to 19 with WPA-PSK (TKIP) and WPA2-PSK (AES-CCMP) security modes

Test Priority	High
Test Type	Voice Capacity
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should not allow the R-value of the voice traffic (whether 1 or 10 calls/AP) to go below 78 Mb/s regardless of the level of data traffic offered at the same time. (It should drop the data traffic in preference to affecting voice quality.) In addition, the SUT should support at least 5 Mb/s of sustained data traffic when carrying 10 voice calls per AP at the specified minimum R-value of 78.

PBTC 060 VoIP_Roaming_80211g

Title	Determine impact of roaming on call quality in 802.11g mode
Purpose	Measures the call quality impact and call drops when handsets actively engaged in voice calls are made to roam between the APs present in the SUT. The SUT is configured in 802.11g mode, and stressed with different numbers of clients and other parameters.
SUT Feature(s) Tested	Roaming impact on VoIP handsets, QoS support by SUT, interaction of mobility and roaming, SUT datapaths
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support 2 (or more) QoS levels and UDP traffic with static IP addresses • 2 or more 802.11g APs in SUT • RADIUS server supporting PEAP/MSCHAPv2 and EAP/FAST
Test Setup	• Configure the SUT with security modes to: Open, WPA-PSK, WPA2-PSK, WPA-PEAP-MSCHAPv2, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g mode • Set call duration to 1 minute and call drop delay threshold to 50 msec • Run test with WLAN client counts of: 10, 50, 100 and 500 • Run test with roaming rates of: 0.5, 1, and 5 roams/second • Run test with G.711, G.723 and G.729 voice codec types
Procedure	1. Launch the WaveApps application 2. Select the Roaming Service Quality Test under the VoIP QoS test suite 3. Select the test ports (i.e., APs) to use for the test (a minimum

	of 2 ports is required) 4. Set the initial number of clients to 10 5. Select SSID and initially configure the clients for Open (no security) 6. For username/password based EAP types, configure a matching username and password (note: these EAP types typically require the RADIUS server to be present). 7. Create an Ethernet client group on the correct port 8. Set the roam sequence to roam all clients uniformly across all test ports 9. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams) 10. Set the initial codec type to G.711, and configure the TOS or DSCP values for the voice traffic according to the DUT setup 11. Run the test 12. Wait until test completes 13. Collect reports and results data 14. Repeat steps 11 to 13 with codec types of G.723 and G.729 15. Repeat steps 10 to 14 with 50, 100 and 500 clients 16. Repeat steps 9 to 15 with 1 and 5 roams/second 17. Repeat steps 6 to 16 with WPA-PSK, WPA2-PSK, WPA-PEAP-MSCHAPv2, WPA2-PEAP-MSCHAPv2, and WPA2-EAP-FAST security modes
Test Priority	High
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should complete this test with zero dropped calls, zero failed roams and a voice call quality of at least 78 (R-value) regardless of the number of clients configured.

PBTC 061 VoIP_Roaming_80211a

Title	Determine impact of roaming on call quality in 802.11a mode
Purpose	Measures the call quality impact and call drops when handsets actively engaged in voice calls are made to roam between the APs present in the SUT. The SUT is configured in 802.11a mode, and stressed with different numbers of clients and other parameters.
SUT Feature(s) Tested	Roaming impact on VoIP handsets, QoS support by SUT, interaction of mobility and roaming, SUT datapaths
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and

	Ethernet Waveblade(s) • SUT set up to support 2 (or more) QoS levels and UDP traffic with static IP addresses • 2 or more 802.11a APs in SUT • RADIUS server supporting PEAP/MSCHAPv2 and EAP/FAST
Test Setup	• Configure the SUT with security modes to: Open, WPA-PSK, WPA2-PSK, WPA-PEAP-MSCHAPv2, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT APs to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Set call duration to 1 minute and call drop delay threshold to 50 msec • Run test with WLAN client counts of: 10, 50, 100 and 500 • Run test with roaming rates of: 0.5, 1, and 5 roams/second • Run test with G.711, G.723 and G.729 voice codec types
Procedure	1. Launch the WaveApps application 2. Select the Roaming Service Quality Test under the VoIP QoS test suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Set the initial number of clients to 10 5. Select SSID and initially configure the clients for Open (no security) 6. For username/password based EAP types, configure a matching username and password (note: these EAP types typically require the RADIUS server to be present). 7. Create an Ethernet client group on the correct port 8. Set the roam sequence to roam all clients uniformly across all test ports 9. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams) 10. Set the initial codec type to G.711, and configure the TOS or DSCP values for the voice traffic according to the DUT setup 11. Run the test 12. Wait until test completes 13. Collect reports and results data 14. Repeat steps 11 to 13 with codec types of G.723 and G.729 15. Repeat steps 10 to 14 with 50, 100 and 500 clients 16. Repeat steps 9 to 15 with 1 and 5 roams/second 17. Repeat steps 6 to 16 with WPA-PSK, WPA2-PSK, WPA-PEAP-

	MSCHAPv2, WPA2-PEAP-MSCHAPv2, and WPA2-EAP-FAST security modes
Test Priority	High
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT should complete this test with zero dropped calls, zero failed roams and a voice call quality of at least 78 (R-value) regardless of the number of clients configured.

PBTC 062 VoIP_Roaming_80211g_Accel

Title	Determine impact of roaming on call quality in 802.11g mode with various security modes using different speedup mechanisms
Purpose	Measures the call quality impact and call drops when handsets actively engaged in voice calls are made to roam between the APs present in the SUT. The SUT is configured in 802.11g mode, and stressed with different numbers of clients and other parameters. Different acceleration strategies such as proactive key caching (PKC), preauthentication and PMKID caching are enabled to permit roaming delays to be reduced considerably.
SUT Feature(s) Tested	Roaming impact on VoIP handsets, QoS support by SUT, interaction of mobility and roaming, SUT datapaths, performance improvements gained from roaming accelerations
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support 2 (or more) QoS levels and UDP traffic with static IP addresses • 2 or more 802.11g APs in SUT • RADIUS server supporting PEAP/MSCHAPv2, EAP/TLS and EAP/TTLS
Test Setup	• Configure the SUT with security modes to: WPA-PSK, WPA2-PSK, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-TTLS • Configure static IP subnets in the SUT and related network • Configure one or more of the SUT speedup mechanisms such as proactive key caching, preauthentication and PMKID caching • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11g mode • Set call duration to 1 minute and call drop delay threshold to 50 msec • Run test with WLAN client counts of: 10, 50, 100 and 500

	• Run test with roaming rates of: 0.5, 1, and 5 roams/second • Run test with G.711, G.723 and G.729 voice codec types • Run test with proactive key caching, preauthentication and PMKID caching (during different trials)
Procedure	1. Launch the WaveApps application 2. Select the Roaming Service Quality Test under the VoIP QoS test suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Set the initial number of clients to 10 5. Select SSID and initially configure the clients for Open (no security) 6. For TLS or TTLS EAP types, configure certificates on tester and SUT to match; for username/password types, configure a matching username and password. 7. Create an Ethernet client group on the correct port 8. Set the roam sequence to roam all clients uniformly across all test ports 9. Enable proactive key caching for the clients 10. Set the roam sequence to roam all clients uniformly across all test ports 11. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams) 12. Set the initial codec type to G.711, and configure the TOS or DSCP values for the voice traffic according to the DUT setup 13. Run the test 14. Wait until test completes 15. Collect reports and results data 16. Repeat steps 11 to 13 with codec types of G.723 and G.729 17. Repeat steps 10 to 14 with 50, 100 and 500 clients 18. Repeat steps 9 to 15 with 1 and 5 roams/second 19. Repeat steps 6 to 16 with WPA2-PSK, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-TTLS security modes 20. Disable proactive key caching, enable preauthentication, and repeat steps 4 to 19 21. Disable preauthentication, enable PMKID caching, and repeat steps 4 to 19
Test Priority	Medium
Test Type	QoS

Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT must implement at least one accelerated roaming mode in order to successfully complete this test with zero dropped calls, zero failed roams and a voice call quality of at least 78 (R-value).

PBTC 063 VoIP_Roaming_80211a_Accel

Title	Determine impact of roaming on call quality in 802.11a mode with various security modes using different speedup mechanisms
Purpose	Measures the call quality impact and call drops when handsets actively engaged in voice calls are made to roam between the APs present in the SUT. The SUT is configured in 802.11a mode, and stressed with different numbers of clients and other parameters. Different acceleration strategies such as proactive key caching (PKC), preauthentication and PMKID caching are enabled to permit roaming delays to be reduced considerably.
SUT Feature(s) Tested	Roaming impact on VoIP handsets, QoS support by SUT, interaction of mobility and roaming, SUT datapaths, performance improvements gained from roaming accelerations
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support 2 (or more) QoS levels and UDP traffic with static IP addresses • 2 or more 802.11a APs in SUT • RADIUS server supporting PEAP/MSCHAPv2, EAP/TLS and EAP/TTLS
Test Setup	• Configure the SUT with security modes to: WPA-PSK, WPA2-PSK, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-TTLS • Configure static IP subnets in the SUT and related network • Configure one or more of the SUT speedup mechanisms such as proactive key caching, preauthentication and PMKID caching • Set Basic Rate Set on SUT APs to 6Mbps, 12Mbps, 24Mbps • Set client PHY rate to 54 Mb/s in 802.11a mode • Set call duration to 1 minute and call drop delay threshold to 50 msec • Run test with WLAN client counts of: 10, 50, 100 and 500 • Run test with roaming rates of: 0.5, 1, and 5 roams/second • Run test with G.711, G.723 and G.729 voice codec types • Run test with proactive key caching, preauthentication and PMKID caching (during different trials)
Procedure	1. Launch the WaveApps application

	2. Select the Roaming Service Quality Test under the VoIP QoS test suite 3. Select the test ports (i.e., APs) to use for the test (a minimum of 2 ports is required) 4. Set the initial number of clients to 10 5. Select SSID and initially configure the clients for Open (no security) 6. For TLS or TTLS EAP types, configure certificates on tester and SUT to match; for username/password types, configure a matching username and password. 7. Create an Ethernet client group on the correct port 8. Set the roam sequence to roam all clients uniformly across all test ports 9. Enable proactive key caching for the clients 10. Set the roam sequence to roam all clients uniformly across all test ports 11. Set the initial roaming rate to 0.5 roams/second (for the entire SUT) and the test duration to 300 seconds (i.e., 150 roams) 12. Set the initial codec type to G.711, and configure the TOS or DSCP values for the voice traffic according to the DUT setup 13. Run the test 14. Wait until test completes 15. Collect reports and results data 16. Repeat steps 11 to 13 with codec types of G.723 and G.729 17. Repeat steps 10 to 14 with 50, 100 and 500 clients 18. Repeat steps 9 to 15 with 1 and 5 roams/second 19. Repeat steps 6 to 16 with WPA2-PSK, WPA2-EAP-TLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-TTLS security modes 20. Disable proactive key caching, enable preauthentication, and repeat steps 4 to 19 21. Disable preauthentication, enable PMKID caching, and repeat steps 4 to 19
Test Priority	Medium
Test Type	QoS
Pass/Fail Criteria	An Enterprise Class / Carrier Grade SUT must implement at least one accelerated roaming mode in order to successfully complete this test with zero dropped calls, zero failed roams and a voice call quality of at least 78 (R-value).

Client Association Rate

The client association rate tests determine how well the SUT can support large numbers of concurrently associating clients (i.e., many clients trying to connect to APs in the SUT at the same time). Most WLAN tests assume a steady-state level of client load, and connect all the clients before starting the test. However, a real-life network can be subjected to bursts of client connection attempts – for example, if an AP supporting a number of clients goes down, then all clients connected to the failed AP will simultaneously try to switch to a nearby or secondary AP, causing a burst load on the system. As another example, a power glitch can cause all client connections to be dropped, and every client will then attempt to reconnect before TCP or application layer protocol timers expire. Inability of the system to respond well to bursts of client connections results in lost user sessions and dropped handset calls.

The client association rate test is conducted iteratively until the maximum capacity of the SUT is reached, defined as the rate beyond which the SUT fails to successfully connect one or more clients. The test is performed with different numbers of clients and security modes, as well as with DHCP on and off. In the latter case, this also tests the capacity of the SUT and DHCP server to interwork well.

PBTC 066 Max_Client_Association_Rate

Title	Measure maximum client association rate with static IP addresses
Purpose	Measure the maximum rate at which WLAN clients can successfully associate with the SUT under various security settings but with DHCP not being used. The client pool is continuously associated and re-associated with the SUT during the entire duration of each trial in order to assure a steady-state measurement unaffected by artificial factors such as the amount of buffering in the SUT.
SUT Feature(s) Tested	Sustained client connection rate, security state update rate
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP disabled (static IP addressing)
Test Setup	• Configure the SUT with security modes to: Open, WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST • Configure static IP subnets in the SUT and related network • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode APs) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode APs)

	• Set client PHY rate to 54 Mb/s • Run test with no cipher, WEP-128, TKIP (WPA) and AES-CCMP (WPA2) encryption • Run test with 50, 100, and 500 clients
Procedure	1. Launch the WaveApps application 2. Select the AAA Authentication Rate test 3. Select the test port(s) (i.e., APs) to use for the test and configure each port into 802.11g or 802.11a mode as required 4. Select the SSID(s) for the clients and configure the clients to open authentication with no encryption and using static IP 5. Create an Ethernet client group on the correct port(s) with the number of Ethernet clients set to 1 6. Set the initial security mode of the Wi-Fi clients to Open (no security) 7. Set the initial number of Wi-Fi clients to 50 8. Set the starting Authentication Rate (rate at which the test offers clients to the SUT) to 10 per second and the trial duration to 30 seconds 9. Run the test and wait until it completes, then examine the results 10. If all clients have authenticated successfully and there were no authentication failures, then increase the Authentication Rate; otherwise, if authentication failures were observed, decrease the Authentication rate 11. Repeat steps 9 and 10 until the maximum Authentication Rate without failures is found 12. Collect report and results data for the maximum Authentication Rate 13. Repeat steps 8 to 12 with 100 and 500 clients configured on the Wi-Fi side 14. Repeat steps 7 to 13 with WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST security modes (note: For TLS or TTLS security types, configure certificates on tester and SUT to match; for username/password types, configure a matching username and password)
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Grade / Carrier Grade SUT should support an association rate with static IP addresses of at least 50 clients/second, in order to assure network availability during burst load or network recovery periods.

PBTC 067 Max_Client_Association_Rate_DHCP

Title	Measure maximum client association rate with DHCP active
Purpose	Measure the maximum rate at which WLAN clients can successfully associate with the SUT under various security settings and with DHCP being used. The client pool is continuously associated and re-associated with the SUT during the entire duration of each trial in order to assure a steady-state measurement unaffected by artificial factors such as the amount of buffering in the SUT.
SUT Feature(s) Tested	Sustained client connection rate, security state update rate, DHCP transaction completion rate and efficiency
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled
Test Setup	• Configure the SUT with security modes to: Open, WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST • Configure DHCP addressing in the SUT and related network (i.e., DHCP server) • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode APs) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode APs) • Set client PHY rate to 54 Mb/s • Run test with no cipher, TKIP (WPA) and AES-CCMP (WPA2) encryption • Run test with 50, 100, and 500 clients
Procedure	1. Launch the WaveApps application 2. Select the AAA Authentication Rate test 3. Select the test port(s) (i.e., APs) to use for the test and configure each port into 802.11g or 802.11a mode as required 4. Select the SSID(s) for the clients and configure the clients to open authentication with no encryption, and to obtain their IP addresses via DHCP 5. Create an Ethernet client group on the correct port(s) with the number of Ethernet clients set to 1 6. Set the initial security mode of the Wi-Fi clients to Open (no security) 7. Set the initial number of Wi-Fi clients to 50 8. Set the starting Authentication Rate (rate at which the test offers clients to the SUT) to 10 per second and the trial

	duration to 30 seconds 9. Run the test and wait until it completes, then examine the results 10. If all clients have authenticated successfully and there were no authentication failures, then increase the Authentication Rate; otherwise, if authentication failures were observed, decrease the Authentication rate 11. Repeat steps 9 and 10 until the maximum Authentication Rate without failures is found 12. Collect report and results data for the maximum Authentication Rate 13. Repeat steps 8 to 12 with 100 and 500 clients configured on the Wi-Fi side 14. Repeat steps 7 to 13 with WEP-128, WPA-PSK, WPA2-PSK, LEAP-WEP, WPA-EAP-TLS, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS, WPA2-PEAP-MSCHAPv2, WPA2-EAP-FAST security modes (note: For TLS or TTLS security types, configure certificates on tester and SUT to match; for username/password types, configure a matching username and password)
Test Priority	Mandatory
Test Type	Performance
Pass/Fail Criteria	An Enterprise Grade / Carrier Grade SUT should support an association rate with DHCP-assigned addresses of at least 20 clients/second, in order to assure network availability during burst load or network recovery periods.

System Testing

This section covers test cases conducted on a fully integrated system with all operational components ready so as to evaluate the system’s compliance with specific system-level requirements. Test cases seek to detect defects both within the inter-component interfaces and also within the system as a whole. The results either indicate if the SUT passes or fails to meet specific conditions. A passing test result indicates that SUT is capable of operating effectively under those deployment conditions.

Traffic Variation

It is expected that the SUT will continue to provide high performance in spite of continuously changing network load conditions. Examples of such load conditions are data overloads and high-load roaming situations. An enterprise SUT is expected to continue to provide adequate service to clients in one portion of the network while overloads and stresses are occurring in another portion.

These tests are only applicable to SUTs having 4 or more APs attached to one or more WLAN controllers.

TVTC 001 Data_Load_Isolation

Title	Test ability of SUT to isolate data traffic overloads
Purpose	Determine whether the SUT can prevent traffic overloads and congestion situations occurring on one portion of the SUT from affecting normal traffic flowing through another portion of the SUT.
SUT Feature(s) Tested	Reliability, service and traffic isolation, QoS
Requirement(s)	• VeriWave WaveApps running on host PC (two instances) • WT-90 or WT-20 chassis with at least 10 Wi-Fi WaveBlades and 2 Ethernet WaveBlades SUT with at least 10 APs set up to support UDP traffic and static IP addresses
Test Setup	• Configure the SUT with open-system authentication mode • Set Basic Rate Set on SUT AP to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client data PHY rate to 54 Mb/s and management PHY rate to 6 Mb/s • Set overload traffic to UDP, 256 bytes, and ILOAD of 10000 frames/second per AP • Run test with UDP test traffic frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with: 10, 50, 100, and 200 clients per AP Run test with SUT security modes of: Open, WPA-PSK (TKIP), WPA2-PSK (AES-CCMP)
Procedure	1. Measure the downstream UDP throughput of the SUT for each of the test traffic frame sizes (i.e., 88, 128, 256, 512, 1024, 1280 and 1518 bytes) using the WaveApps throughput test, and record these values 2. Launch the first instance of the WaveApps application, to serve as the test traffic generator and analysis function 3. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 4. Select a subset of the test ports (i.e., APs) to use for the test traffic; one of the Ethernet ports, and at least 40% and no more than 60% of the available APs in the SUT should be devoted to carrying test traffic 5. Select the SSID to use, and configure the Wi-Fi clients to open authentication with no encryption and static IP addressing 6. Set the initial number of Wi-Fi clients to 10 (and the corresponding number of Ethernet clients)

	7. Select the initial frame size as 88 bytes, UDP traffic type, the ILOAD of the test traffic to 90% of the measured aggregate throughput at the configured frame size, and the trial duration to 30 seconds 8. Select Ethernet to Wireless (one-to-one, downstream) mapping 9. Launch the second instance of the WaveApps application (on the same or a different host PC), to serve as the overload traffic generator 10. Select the Packet Loss Test 11. Select the remaining APs in the SUT to serve as test ports, along with a second Ethernet port 12. Select the SSID and configure the Wi-Fi clients to open authentication with no encryption and static IP addressing 13. Set the number of Wi-Fi clients to 1 (with the corresponding number of Ethernet clients 14. Set the frame size to 256 bytes, UDP traffic type, the ILOAD to 10000 frames/second per overloaded AP in SUT, the trial duration to 10 seconds, the number of trials to 30, and the settling time between trials to 5 seconds 15. Select Ethernet to Wireless (downstream) mapping 16. Start the overload traffic (i.e., the second instance of the WaveApps application) 17. After 10 seconds, start the test traffic (i.e., the first instance of the WaveApps application) 18. Wait until both instances complete 19. Collect the report and results data for the test traffic 20. Repeat steps 7 to 19 with 50, 100, and 200 clients per AP configured on both Ethernet and Wi-Fi sides (one-to-one) in the test traffic application 21. Repeat steps 6 to 20 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Mandatory
Test Type	System
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should show zero packet loss experienced by the test traffic, regardless of the level of overload being experienced by the other APs in the SUT.

TVTC 002 Roaming_Isolation_Network

Title	Test ability of SUT to isolate roaming loads between different physical parts of the WLAN

Purpose	Determine whether the SUT can prevent roaming overload situations occurring on one portion of the SUT from affecting normal roaming clients on another portion of the SUT.
SUT Feature(s) Tested	Reliability, service and roaming isolation, QoS
Requirement(s)	• VeriWave WaveApps running on host PC (two instances) • WT-90 or WT-20 chassis with at least 10 Wi-Fi WaveBlades and 2 Ethernet WaveBlades • SUT with at least 10 APs set up to support UDP traffic • DHCP server • RADIUS server supporting EAP/TLS and PEAP/MSCHAPv2
Test Setup	• Configure the SUT with open-system authentication mode and supporting both DHCP and static IP addressing • Set Basic Rate Set on SUT AP to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client data PHY rate to 54 Mb/s and management PHY rate to 6 Mb/s • Configure 100 overload roaming clients roaming at a rate of 30 roams/second • Run test with: 10, 50, 100 and 500 test roaming clients (for the SUT) roaming at a rate of 0.5 roams/second • Run test with SUT security modes of: Open (no security), WPA2-PSK, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS
Procedure	1. Measure the roaming delay and failed roams of the SUT for each of the counts of roaming clients (i.e., 10, 50, 100 and 500) at a roaming rate of 0.5 roams/second using the WaveApps Roaming Benchmark test, and record these values 2. Launch the first instance of the WaveApps application, to serve as the test roaming generator and analysis function 3. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 4. Select a subset of the test ports (i.e., APs) to use for the test roaming generator; one of the Ethernet ports, and at least 40% and no more than 60% of the available APs in the SUT should be devoted to supporting test roaming clients 5. Select the SSID to use, configure the Wi-Fi clients to Open security with DHCP, and create an Ethernet client group on the correct port 6. Set the initial number of test roaming clients to 10 7. If TLS or TTLS security types are set per above, configure certificates on tester and SUT to match; for username/ password types, configure a matching username and password.

	8. Set the roam sequence to roam all clients uniformly across all the port subset, with a uniform initial client distribution, set the initial roaming rate to 0.5 roams/second (for the entire SUT), and set the test duration to 300 seconds 9. Set the data traffic flow to a frame size of 256 bytes and a flow rate of 100 pps (per client) 10. Launch the second instance of the WaveApps application (on the same or a different host PC), to serve as the overload roaming generator 11. Select the Roaming Benchmark Test under the WLAN Roaming Test Suite 12. Select the remaining APs in the SUT to serve as overload roaming ports, along with a second Ethernet port for traffic injection 13. Select the SSID to use, configure the Wi-Fi clients to WPA2-PSK security with static IP addressing, and set the number of overload roaming clients to 10; set the data traffic flow to a frame size of 256 bytes and a flow rate of 100 pps (per client) 14. Set the roam sequence to roam all clients uniformly across all the port subset at a rate of 30 roams/second, and set the test duration to 240 seconds 15. Start the test roaming traffic (i.e., the first instance of the WaveApps application) 16. After 10 seconds, start the overload roaming traffic (i.e., the second instance of the WaveApps application) 17. Wait until both instances complete 18. Collect the report and results data for the test roaming clients 19. Repeat steps 7 to 19 with 50, 100, 200 and 500 total clients configured for the test roaming traffic application 20. Repeat steps 6 to 19 with WPA2-PSK, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS security modes for the test roaming traffic clients
Test Priority	High
Test Type	System
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should show no change in roaming delays or failures experienced by the test roaming traffic, regardless of the level of roaming overload being experienced by the other APs in the SUT.

TVTC 003 Roaming_Isolation_SSID

Title	Test ability of SUT to isolate roaming loads between different logical WLANs (i.e., SSIDs)

Purpose	Determine whether the SUT can maintain roaming load isolation between logically distinct portions of the SUT – i.e., prevent a high roaming load on one SSID from affecting roaming traffic on a different SSID on the same set of APs.
SUT Feature(s) Tested	Reliability, service and roaming isolation, QoS
Requirement(s)	• VeriWave WaveApps running on host PC • WT-90 or WT-20 chassis with at least 10 Wi-Fi WaveBlades and 2 Ethernet WaveBlades • SUT with at least 10 APs set up to support UDP traffic • DHCP server • RADIUS server supporting EAP/TLS and PEAP/MSCHAPv2
Test Setup	• Configure the SUT with open-system authentication mode and supporting two SSIDs (configured similarly), supporting both DHCP and static IP addressing • Set Basic Rate Set on SUT AP to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set client data PHY rate to 54 Mb/s and management PHY rate to 6 Mb/s • Configure 100 overload roaming clients roaming on one SSID at a rate of 20 roams/second • Run test with: 10, 50, 100 and 400 test roaming clients roaming on a different SSID at a rate of 0.5 roams/second • Run test with SUT security modes of: Open (no security), WPA2-PSK, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS
Procedure	1. Measure the roaming delay and failed roams of the SUT for each of the counts of roaming clients (i.e., 10, 50, 100 and 500) at a roaming rate of 0.5 roams/second using the WaveApps Roaming Benchmark test, and record these values 2. Launch the WaveApps application and select the Roaming Delay Test under the WLAN Roaming Test Suite 3. Configure one group of clients to serve as the test roaming clients; assign these clients to the SUT SSID created for this purpose, configure the Wi-Fi clients to Open security with DHCP 4. Set the initial number of test roaming clients to 10 5. If TLS or TTLS security types are set per above, configure certificates on tester and SUT to match; for username/ password types, configure a matching username and password. 6. Set the roam sequence to roam all clients uniformly across all the port subset, with a uniform initial client distribution, and set the initial roaming dwell time to 20 seconds (i.e., roaming rate of 0.5 roams/second)

	7. Set the data traffic flow to a frame size of 256 bytes and a flow rate of 100 pps (per client) 8. Configure a second group of 100 clients to serve as the overload roaming clients; assign these clients to the SUT SSID created for this purpose, configure the clients to WPA2-PSK security with static IP addressing 9. Set the data traffic flow to a frame size of 256 bytes and a flow rate of 10 pps (per client) 10. Set the roam sequence to roam the overload roaming clients at uniform times, but all starting from the same AP, with a dwell time of 5 seconds (i.e., roaming rate of 20 roams/second, with a successive-overload profile) 11. Set the test duration to 300 seconds 12. Start the test and wait it completes 13. Collect the report and results data for the test roaming clients 14. Repeat steps 5 to 13 with 50, 100, and 400 test roaming clients 15. Repeat steps 4 to 14 with WPA2-PSK, WPA-PEAP-MSCHAPv2, WPA2-EAP-TLS, WPA2-EAP-TTLS security modes for the test roaming traffic clients
Test Priority	High
Test Type	System
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should show no change in roaming delays or failures experienced by the test roaming traffic on one SSID, regardless of the level of roaming overload being experienced by the other SSIDs in the SUT.

WiMix Tests

The WiMix traffic tests verify operation of the SUT under real-world traffic loading scenarios.

WMTC 001 WiMix_Hospital_Environment

Title	Demonstrate support level of the SUT for hospital environments
Purpose	Assess the ability of the SUT to support typical hospital WLAN traffic using the WiMix Hospital traffic profile. The SUT is subjected to traffic mixes found in various sizes of hospital environments and different application-specific metrics (packet loss, latency, R-values, etc.) are measured to determine the level of support.
SUT Feature(s) Tested	Efficient traffic mix handling, hospital environment support
Requirement(s)	• WiMix application running on host PC • WT-90 or WT-20 chassis with 10 or more Wi-Fi Waveblades

	and 1 or more Ethernet Waveblade(s) • SUT with 10 or more APs set up to support UDP, TCP, voice and video traffic • DHCP server • RADIUS server supporting different EAP types
Test Setup	• Connect the Wi-Fi WaveBlades to the SUT APs • Configure at least 2 SSIDs on the SUT (one for voice, the other for data/video) with appropriate VLANs on the Ethernet side; 3 SSIDs are preferred, so that data, voice and video may be properly separated • Configure the voice SSID to use WPA2-PSK security mode • Configure desired QoS parameters for data, voice and video on the SUT • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g AP(s), if present) or 6Mbps, 12Mbps and 24Mbps (802.11a AP(s), if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Run test with 100, 500, 1000 and 2000 clients for the SUT • Run test with data/video security modes of WPA2-PSK, WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS
Procedure	1. Inspect and record the SUT CPU and memory status prior to running the test. 2. Launch the WiMix application 3. Select the test ports (i.e., APs in SUT and Ethernet ports) to use for the test and set the channel(s) appropriately 4. Select SSIDs for the client groups and configure the clients with the appropriate security types, and also set them to obtain IP addresses via DHCP 5. Select the Hospital WiMix profile, and use the client-based setup view 6. Set the total number of clients in the generated environment to 100 (per SUT) 7. Set the test duration to 1800 seconds 8. Leave the QoS thresholds and client/traffic parameters configured at their defaults 9. Run the test and wait until it completes 10. Collect and examine the generated report 11. Repeat steps 7 to 10 with 500, 1000 and 2000 clients for the SUT 12. Repeat steps 4 to 11 with data/video security modes of WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS

	13. Inspect the SUT CPU and memory status after all the trials have been completed and compare to the initial status.
Test Priority	Mandatory
Test Type	System
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should be able to support the different client and traffic loads in a Hospital environment without loss of stability or progressive degradation in system capacity (e.g., due to memory leaks or CPU overload). Further, all of the clients and traffic flows should have satisfied their required QoS levels.

WMTC 002 WiMix_Enterprise_Environment

Title	Demonstrate support level of the SUT for enterprise environments
Purpose	Assess the ability of the SUT to support typical corporate enterprise WLAN traffic using the WiMix Enterprise traffic profile. The SUT is subjected to traffic mixes found in various sizes of enterprise environments and different application-specific metrics (packet loss, latency, R-values, etc.) are measured to determine the level of support.
SUT Feature(s) Tested	Efficient traffic mix handling, hospital environment support
Requirement(s)	• WiMix application running on host PC • WT-90 or WT-20 chassis with 10 or more Wi-Fi Waveblades and 1 or more Ethernet Waveblade(s) • SUT with 10 or more APs set up to support UDP, TCP, voice and video traffic • DHCP server • RADIUS server supporting different EAP types
Test Setup	• Connect the Wi-Fi WaveBlades to the SUT APs • Configure at least 2 SSIDs on the SUT (one for voice, the other for data/video) with appropriate VLANs on the Ethernet side; 3 SSIDs are preferred, so that data, voice and video may be properly separated • Configure the voice SSID to use WPA2-PSK security mode • Configure desired QoS parameters for data, voice and video on the SUT • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g AP(s), if present) or 6Mbps, 12Mbps and 24Mbps (802.11a AP(s), if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Run test with 100, 500, 1000 and 2000 clients for the SUT

	- Run test with data/video security modes of WPA2-PSK, WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS
Procedure	1. Inspect and record the SUT CPU and memory status prior to running the test. 2. Launch the WiMix application 3. Select the test ports (i.e., APs in SUT and Ethernet ports) to use for the test and set the channel(s) appropriately 4. Select SSIDs for the client groups and configure the clients with the appropriate security types, and also set them to obtain IP addresses via DHCP 5. Select the Enterprise WiMix profile, and use the client-based setup view 6. Set the total number of clients in the generated environment to 100 (per SUT) 7. Set the test duration to 1800 seconds 8. Leave the QoS thresholds and client/traffic parameters configured at their defaults 9. Run the test and wait until it completes 10. Collect and examine the generated report 11. Repeat steps 7 to 10 with 500, 1000 and 2000 clients for the SUT 12. Repeat steps 4 to 11 with data/video security modes of WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS 13. Inspect the SUT CPU and memory status after all the trials have been completed and compare to the initial status.
Test Priority	Mandatory
Test Type	System
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should be able to support the different client and traffic loads in an Enterprise environment without loss of stability or progressive degradation in system capacity (e.g., due to memory leaks or CPU overload). Further, all of the clients and traffic flows should have satisfied their required QoS levels.

WMTC 003 WiMix_University_Environment

Title	Demonstrate support level of the SUT for university environments
Purpose	Assess the ability of the SUT to support typical university WLAN traffic using the WiMix University traffic profile. The SUT is subjected to traffic mixes found in various sizes of university environments and different application-specific metrics (packet loss, latency, R-values, etc.) are measured to determine the level of

	support.
SUT Feature(s) Tested	Efficient traffic mix handling, university environment support
Requirement(s)	• WiMix application running on host PC • WT-90 or WT-20 chassis with 10 or more Wi-Fi Waveblades and 1 or more Ethernet Waveblade(s) • SUT with 10 or more APs set up to support UDP, TCP, voice and video traffic • DHCP server • RADIUS server supporting different EAP types
Test Setup	• Connect the Wi-Fi WaveBlades to the SUT APs • Configure at least 2 SSIDs on the SUT (one for voice, the other for data/video) with appropriate VLANs on the Ethernet side; 3 SSIDs are preferred, so that data, voice and video may be properly separated • Configure the voice SSID to use WPA2-PSK security mode • Configure desired QoS parameters for data, voice and video on the SUT • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g AP(s), if present) or 6Mbps, 12Mbps and 24Mbps (802.11a AP(s), if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Run test with 100, 500, 1000 and 2000 clients for the SUT • Run test with data/video security modes of WPA2-PSK, WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS
Procedure	1. Inspect and record the SUT CPU and memory status prior to running the test. 2. Launch the WiMix application 3. Select the test ports (i.e., APs in SUT and Ethernet ports) to use for the test and set the channel(s) appropriately 4. Select SSIDs for the client groups and configure the clients with the appropriate security types, and also set them to obtain IP addresses via DHCP 5. Select the University WiMix profile, and use the client-based setup view 6. Set the total number of clients in the generated environment to 100 (per SUT) 7. Set the test duration to 1800 seconds 8. Leave the QoS thresholds and client/traffic parameters configured at their defaults 9. Run the test and wait until it completes 10. Collect and examine the generated report

	11. Repeat steps 7 to 10 with 500, 1000 and 2000 clients for the SUT 12. Repeat steps 4 to 11 with data/video security modes of WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS 13. Inspect the SUT CPU and memory status after all the trials have been completed and compare to the initial status.
Test Priority	Mandatory
Test Type	System
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should be able to support the different client and traffic loads in a University environment without loss of stability or progressive degradation in system capacity (e.g., due to memory leaks or CPU overload). Further, all of the clients and traffic flows should have satisfied their required QoS levels.

WMTC 004 WiMix_Retail_Environment

Title	Demonstrate support level of the SUT for retail environments
Purpose	Assess the ability of the SUT to support typical retail application WLAN traffic using the WiMix Retail traffic profile. The SUT is subjected to traffic mixes found in various sizes of retail environments and different application-specific metrics (packet loss, latency, R-values, bar-code reader support, etc.) are measured to determine the level of support.
SUT Feature(s) Tested	Efficient traffic mix handling, retail environment support
Requirement(s)	• WiMix application running on host PC • WT-90 or WT-20 chassis with 10 or more Wi-Fi Waveblades and 1 or more Ethernet Waveblade(s) • SUT with 10 or more APs set up to support UDP, TCP, voice and video traffic • DHCP server • RADIUS server supporting different EAP types
Test Setup	• Connect the Wi-Fi WaveBlades to the SUT APs • Configure at least 3 SSIDs on the SUT (one for voice, another for special-purpose devices such as RFID readers, and the third for standard data/video) with appropriate VLANs on the Ethernet side; 3 SSIDs are preferred, so that data, voice and video may be properly separated • Configure the voice SSID to use WPA2-PSK security mode • Configure the special-purpose device SSID to use WEP-128 security mode • Configure desired QoS parameters for data, voice and video on the SUT

	• Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g AP(s), if present) or 6Mbps, 12Mbps and 24Mbps (802.11a AP(s), if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Run test with 100, 500, 1000 and 2000 total clients for the SUT • Run test with data/video security modes of WPA2-PSK, WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS
Procedure	1. Inspect and record the SUT CPU and memory status prior to running the test. 2. Launch the WiMix application 3. Select the test ports (i.e., APs in SUT and Ethernet ports) to use for the test and set the channel(s) appropriately 4. Select SSIDs for the client groups and configure the clients with the appropriate security types, and also set them to obtain IP addresses via DHCP 5. Select the Retail WiMix profile, and use the client-based setup view 6. Set the total number of clients in the generated environment to 100 (per SUT) 7. Set the test duration to 1800 seconds 8. Leave the QoS thresholds and client/traffic parameters configured at their defaults 9. Run the test and wait until it completes 10. Collect and examine the generated report 11. Repeat steps 7 to 10 with 500, 1000 and 2000 clients for the SUT 12. Repeat steps 4 to 11 with data/video security modes of WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS 13. Inspect the SUT CPU and memory status after all the trials have been completed and compare to the initial status.
Test Priority	High
Test Type	System
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should be able to support the different client and traffic loads in a Retail environment without loss of stability or progressive degradation in system capacity (e.g., due to memory leaks or CPU overload). Further, all of the clients and traffic flows should have satisfied their required QoS levels.

WMTC 005 WiMix_Triple_Play_Unicast

Title	Demonstrate support level of the SUT for mixed voice, unicast video and data traffic streams
Purpose	Assess the ability of the SUT to support triple-play traffic mixes (voice, unicast video and data) using a customized WiMix traffic profile. Such traffic mixes are commonly found in service provider, consumer wireless access, and enterprise multimedia situations. The SUT is subjected to these traffic mixes and different application-specific metrics (loss/latency for data, R-values for voice, and MDI scores for video) are measured to determine the support level of the SUT.
SUT Feature(s) Tested	QoS maintenance, triple-play traffic, voice, unicast video
Requirement(s)	• WiMix application running on host PC • WT-90 or WT-20 chassis with 10 or more Wi-Fi Waveblades and 1 or more Ethernet Waveblade(s) • SUT with 10 or more APs set up to support UDP, TCP, voice and video traffic • DHCP server • RADIUS server supporting different EAP types
Test Setup	• Connect the Wi-Fi WaveBlades to the SUT APs • Configure at least 2 SSIDs on the SUT (one for voice, the other for data/video) with appropriate VLANs on the Ethernet side; 3 SSIDs are preferred, so that data, voice and video may be properly separated • Configure the voice SSID to use WPA2-PSK security mode • Configure the video SSID (if present) to use WPA-PEAP-MSCHAPv2 security mode • Configure desired QoS parameters for data, voice and video on the SUT • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g AP(s), if present) or 6Mbps, 12Mbps and 24Mbps (802.11a AP(s), if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Run test with 100, 500, 1000 and 2000 total clients for the SUT • Run test with different triple-play mixes as follows: o 50% HTTP data clients, 20% FTP data clients, 20% voice clients, 10% video clients o 40% HTTP data clients, 10% FTP data clients, 30% voice clients, 20% video clients o 30% HTTP data clients, 4% FTP data clients, 33% voice clients, 33% video clients • Run test with data security modes of WPA2-PSK, WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS

Procedure	1. Inspect and record the SUT CPU and memory status prior to running the test. 2. Launch the WiMix application 3. Select the test ports (i.e., APs in SUT and Ethernet ports) to use for the test and set the channel(s) appropriately 4. Select SSIDs for the client groups and configure the clients with the appropriate security types, and also set them to obtain IP addresses via DHCP; set the data client security mode to WPA2-PSK 5. Select the Custom WiMix profile, and use the client-based setup view 6. Set the total number of clients in the generated environment to 100 (per SUT) 7. Set the client ratio to: 50% HTTP data clients, 20% FTP data clients, 20% voice clients, 10% video clients 8. Set the test duration to 600 seconds 9. Leave the QoS thresholds and client/traffic parameters configured at their defaults 10. Run the test and wait until it completes 11. Collect and examine the generated report 12. Repeat steps 9 to 12 with client ratios of: 40% HTTP data clients, 10% FTP data clients, 30% voice clients, 20% video clients; and 30% HTTP data clients, 4% FTP data clients, 33% voice clients, 33% video clients 13. Repeat steps 8 to 13 with 500, 1000 and 2000 clients for the SUT 14. Repeat steps 6 to 14 with data security modes of WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS 15. Inspect the SUT CPU and memory status after all the trials have been completed and compare to the initial status
Test Priority	Medium
Test Type	System
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should be able to support the different client and traffic loads in a Triple-Play situation without loss of stability or progressive degradation in system capacity (e.g., due to memory leaks or CPU overload). Further, all of the voice/video clients and traffic flows should have satisfied their required QoS levels. The latency levels for the data clients should remain under 50 msec.

WMTC 006 WiMix_Triple_Play_Multicast

Title	Demonstrate support level of the SUT for mixed voice, unicast video and data traffic streams
Purpose	Assess the ability of the SUT to support triple-play traffic mixes (voice, multicast video and data) using a customized WiMix traffic profile. Such traffic mixes are commonly found in service provider, consumer wireless access, and enterprise multimedia situations. The SUT is subjected to these traffic mixes and different application-specific metrics (loss/latency for data, R-values for voice, and MDI scores for video) are measured to determine the support level of the SUT.
SUT Feature(s) Tested	QoS maintenance, triple-play traffic, voice, multicast video
Requirement(s)	• WiMix application running on host PC • WT-90 or WT-20 chassis with 10 or more Wi-Fi Waveblades and 1 or more Ethernet Waveblade(s) • SUT with 10 or more APs set up to support UDP, TCP, voice and video traffic • DHCP server • RADIUS server supporting different EAP types
Test Setup	• Connect the Wi-Fi WaveBlades to the SUT APs • Configure at least 2 SSIDs on the SUT (one for voice, the other for data/video) with appropriate VLANs on the Ethernet side; 3 SSIDs are preferred, so that data, voice and video may be properly separated • Configure the voice SSID to use WPA2-PSK security mode • Configure the video SSID (if present) to use WPA-PEAP-MSCHAPv2 security mode • Configure a Class D multicast address of 250.0.0.10 to be used as the multicast video target • Configure desired QoS parameters for data, voice and video on the SUT • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g AP(s), if present) or 6Mbps, 12Mbps and 24Mbps (802.11a AP(s), if present) • Set client flow PHY rate to 54 Mb/s and management (i.e., connection) PHY rate to 6 Mb/s • Run test with 100, 500, 1000 and 2000 total clients for the SUT • Run test with different triple-play mixes as follows: o 50% HTTP data clients, 20% FTP data clients, 20% voice clients, 10% video clients o 40% HTTP data clients, 10% FTP data clients, 30% voice clients, 20% video clients o 30% HTTP data clients, 4% FTP data clients, 33% voice clients, 33% video clients

	• Run test with data security modes of WPA2-PSK, WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS
Procedure	1. Inspect and record the SUT CPU and memory status prior to running the test. 2. Launch the WiMix application 3. Select the test ports (i.e., APs in SUT and Ethernet ports) to use for the test and set the channel(s) appropriately 4. Select SSIDs for the client groups and configure the clients with the appropriate security types, and also set them to obtain IP addresses via DHCP; set the data client security mode to WPA2-PSK 5. Select the Custom WiMix profile, and use the client-based setup view 6. Set the total number of clients in the generated environment to 100 (per SUT) 7. Set the client ratio to: 50% HTTP data clients, 20% FTP data clients, 20% voice clients, 10% video clients 8. Configure the multicast video target IP address to 250.0.0.10 (and a corresponding multicast MAC address), and configure the appropriate multicast video server in the WiMix application 9. Set the test duration to 600 seconds 10. Leave the QoS thresholds and client/traffic parameters configured at their defaults 11. Run the test and wait until it completes 12. Collect and examine the generated report 13. Repeat steps 9 to 13 with client ratios of: 40% HTTP data clients, 10% FTP data clients, 30% voice clients, 20% video clients; and 30% HTTP data clients, 4% FTP data clients, 33% voice clients, 33% video clients 14. Repeat steps 8 to 14 with 500, 1000 and 2000 clients for the SUT 15. Repeat steps 6 to 15 with data security modes of WPA-PEAP-MSCHAPv2 and WPA2-EAP-TLS 16. Inspect the SUT CPU and memory status after all the trials have been completed and compare to the initial status
Test Priority	Medium
Test Type	System
Pass/Fail Criteria	An Enterprise Class/Carrier Grade SUT should be able to support the different client and traffic loads in a Triple-Play situation without loss of stability or progressive degradation in system capacity (e.g., due to memory leaks or CPU overload). Further, all

	of the voice/video clients and traffic flows should have satisfied their required QoS levels. The latency levels for the data clients should remain under 50 msec.

Mesh Interference Effects

It is expected that mesh SUTs will handle interference and continue to maintain availability and performance to sections of the mesh that are not directly impacted by the interference. For example, if interference brings down one link, then the mesh routing algorithms are expected to discover a path around the interference and restore service to the affected portions.

IETC 001 Mesh_UDP_Throughput_Interference_Impact

Title	Assess impact on UDP traffic throughput during high-interference events
Purpose	Measure the degradation of client UDP data throughput in a WLAN mesh SUT as the interference level is progressively increased on a backhaul link.
SUT Feature(s) Tested	Mesh routing adaptability, interference handling, mesh stability
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • Mesh SUT set up to support UDP traffic • DHCP server
Test Setup	• Configure the SUT in mesh configuration with at least four access points, set up to provide primary and backup backhaul paths • Configure the SUT with open authentication and DHCP enabled • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set BLOG interference parameters to: all frame sizes from 64 bytes to 1518 bytes, begin time of 0% of trial duration, end time of 100% of trial duration • Set client PHY rate to 54 Mb/s, and set clients to use DHCP to obtain IP addresses • Set trial duration to 60 seconds • Run the Mesh Throughput per Hop test with 1, 10, 20, and 100 clients per mesh AP • Run test with no cipher, WPA-TKIP and WPA2-AES • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with BLOG interference levels of: 10%, 20%, 30%,

	40%, 50%, 60%, 70%, and 80%
Procedure	1. Launch the WaveApps application 2. Select the Mesh Per-Hop Throughput Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the data traffic and configure into 802.11g or 802.11a mode as required 4. Select the test port to use as a Backhaul Load and Obstruction Generator (BLOG) and configure as above 5. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 6. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 per mesh AP 7. Set the initial number of Wi-Fi clients to 1 per AP 8. Set the initial BLOG interference level to 10% 9. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type 10. Select Mesh Hops to Mesh Gateway traffic mapping with bidirectional mode 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 9 to 13 with BLOG interference levels of: 20%, 30%, 40%, 50%, 60%, 70%, and 80% 15. Repeat steps 8 to 14 with 10, 20, and 100 clients configured on both Ethernet and Wi-Fi sides (one-to-one) per mesh AP 16. Repeat steps 6 to 15 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Medium
Test Type	System
Pass/Fail Criteria	A robust Carrier Grade SUT should show a graceful degradation of UDP throughput (i.e., a linear decrease with no sharp peaks or troughs) with progressively increasing levels of interference. Ideally, the SUT should also utilize alternate paths to carry data traffic as the level of interference exceeds 50%, in order to ensure that a carrier can use a standard 50% provisioning model to cope with interference impact.

IETC 002 Mesh_Latency_Interference_Impact

Title	Assess impact on UDP traffic latency during high-interference events

Purpose	Measure degradation of latency experienced by client UDP traffic traversing a WLAN mesh SUT as the interference level is progressively increased on a specific backhaul link.
SUT Feature(s) Tested	Mesh routing adaptability, interference handling, mesh stability
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • Mesh SUT set up to support UDP traffic • DHCP server
Test Setup	• Configure the SUT in mesh configuration with at least four access points, set up to provide primary and backup backhaul paths • Configure the SUT with open authentication and DHCP enabled • Set Basic Rate Set on SUT to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode) or 6Mbps, 12Mbps and 24Mbps (802.11a mode) • Set BLOG interference parameters to: all frame sizes from 64 bytes to 1518 bytes, begin time of 0% of trial duration, end time of 100% of trial duration • Set client PHY rate to 54 Mb/s, and set clients to use DHCP to obtain IP addresses • Set intended load (ILOAD) for each frame size to 90% of the throughput of the SUT as obtained from the mesh per-hop throughput tests (if the SUT throughput is unknown, use theoretical values) • Set trial duration to 60 seconds • Run test with 1, 10, 20, and 100 clients per mesh AP • Run test with no cipher, WPA-TKIP and WPA2-AES • Run test with frame sizes: 88, 128, 256, 512, 1024, 1280 and 1518 bytes • Run test with BLOG interference levels of: 10%, 20%, 30%, 40%, 50%, 60%, 70%, and 80%
Procedure	1. Launch the WaveApps application 2. Select the Mesh Per-Hop Latency Test under the Wireless Mesh Test Suite 3. Select the test port(s) (i.e., APs) to use for the data traffic and configure into 802.11g or 802.11a mode as required 4. Select the test port to use as a Backhaul Load and Obstruction Generator (BLOG) and configure as above 5. Select SSID and configure the clients to open authentication with no encryption and obtain IP addresses via DHCP 6. Create an Ethernet client group on the correct port(s) with the initial number of Ethernet clients set to 1 per AP

	7. Set the initial number of Wi-Fi clients to 1 per AP 8. Set the initial BLOG interference level to 10% 9. Select frame sizes of 88, 128, 256, 512, 1024, 1280 and 1518 bytes and UDP traffic type; adjust the intended load (ILOAD) table to target traffic load as per test setup details above 10. Select Mesh Hops to Mesh Gateway (upstream) traffic mapping 11. Run the test 12. Wait until test completes 13. Collect report and results data 14. Repeat steps 9 to 13 with BLOG interference levels of: 20%, 30%, 40%, 50%, 60%, 70%, and 80% 15. Repeat steps 8 to 14 with 10, 20, and 100 clients configured on both Ethernet and Wi-Fi sides (one-to-one) per mesh AP 16. Repeat steps 6 to 15 with WPA-TKIP and WPA2-AES encryption modes
Test Priority	Medium
Test Type	System
Pass/Fail Criteria	A robust Carrier Grade SUT should show a graceful degradation of UDP latency (i.e., a linear increase with no sharp peaks or troughs) with progressively increasing levels of interference. Ideally, the SUT should also utilize alternate paths to carry data traffic as the latency level exceeds 100 msec, in order to ensure that voice traffic will not suffer adverse latency impact due to mesh interference.

Stress Testing

Stress testing determines the long-term stability of the SUT under various extremes of operational conditions, such as large numbers of clients attempting to connect or roam for very long periods of time. It involves testing beyond normal operational capacity and often to a breaking point, in order to observe whether the SUT behaves predictably and reliably, and recovers fully after the stress is removed. Performing stress testing is essential to ensure reliability under busy enterprise or service provider deployment scenarios, where the WLAN equipment must function reliably and consistently for months or years without observable crashes or resets.

Stress test results are expressed as pass/fail criteria. A passing test result indicates that SUT is capable of withstanding the specific operational stresses applied during the test, and can recover to the level of performance and capability observed prior to the application of the stress. A failing result is cause for serious concern, as it indicates a potential field deployment issue caused by internal bugs.

In all cases, it is highly recommended that the largest feasible configuration of the SUT be tested. This maximizes the stress on the internal SUT functions and ensures the highest probability of finding functional issues.

Note that if the SUT has to be reset, rebooted or power-cycled during or after any of these stress tests, it must automatically be considered to have failed that test. These stress tests should preferably be run back-to-back without SUT resets in between, to ensure the maximum level of long-term traffic loading.

Traffic Stress

Any enterprise SUT must be able to sustain high levels of traffic for very long periods of time without experiencing performance issues due to internal problems such as memory leaks or data structure corruption. The traffic stress test therefore subjects the SUT to a realistic enterprise traffic scenario for long periods of time. Throughput and latency measurements are made before and after the traffic stress, in order to verify that permanent degradation in SUT performance has not occurred as a consequence of the traffic stress.

TSTC 001 Traffic_Stress

Title	Verify ability of SUT to withstand high levels of mixed data traffic
Purpose	Stresses the SUT with a typical enterprise traffic mix (using the WiMix Enterprise profile) for a long duration, to determine if performance changes occur due to internal issues. SUT performance is verified before and after the stress period using standard throughput and latency tests.
SUT Feature(s) Tested	Datapath robustness, buffer management, queue management, scheduling functions
Requirement(s)	• WaveApps application running on host PC • WT-90 or WT-20 chassis with Wi-Fi Waveblade(s) and Ethernet Waveblade(s) • SUT set up to support WiMix traffic • DHCP enabled with internal or external DHCP server • RADIUS server with support for EAP types used
Test Setup	• Configure the SUT with security modes on different SSIDs to: Open, WPA-PSK, and WPA2-EAP-TLS (Note: if the SUT supports only one active SSID, use only WPA2-EAP-TLS security mode and a single SSID) • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode APs) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode APs) • Set client PHY rate to 54 Mb/s • Set client security types to match those in the SUT

	• Run test with 50 clients per AP in the SUT
Procedure	1. Configure the SUT as indicated above 2. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT, and record the results 3. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT, and record the results 4. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT, and record the results 5. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT, and record the results 6. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT, and record the results 7. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT, and record the results 8. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT, and record the results 9. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT, and record the results 10. Launch the WaveVCE application 11. Select the WiMix test and select the Enterprise profile within the WiMix test 12. Select the test ports (i.e., APs) to use for the WiMix test and configure each port into 802.11g or 802.11a mode as required 13. Create client groups to support (50 x *N*) clients, where *N* is the number of APs in the SUT; select the SSIDs for the clients and configure the clients to the appropriate security modes for the SSIDs, and assign IP addresses using DHCP 14. Create an Ethernet client group on the correct ports with the number of Ethernet clients set to 1 15. Set traffic parameters consistent with the Enterprise traffic mix and the trial duration to 72 hours 16. Run the test and wait until it completes 17. Verify that at the end of 72 hours the test is still running and no clients have been disconnected for any reason 18. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT again, and record the results 19. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT again, and record the results 20. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT again, and record the results 21. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT again, and record the results

	22. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT again, and record the results 23. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT again, and record the results 24. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT again, and record the results 25. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT again, and record the results
Test Priority	Mandatory
Test Type	Stress
Pass/Fail Criteria	The throughput and latency measurements performed before and after the 72-hour WiMix traffic load stress must be within 5% of each other. Further, no client disconnections or traffic flow stoppages should be observed at the end of the 72-hour traffic load stress period. If either of these two conditions is not satisfied, the test must be considered to have failed.

Roaming Stress

It is critical for the SUT to able to maintain good performance over very long periods of time even in the face of continuous internal state changes caused as connected clients move about in the WLAN. The roaming stress tests therefore subject the SUT to various types of dense mobile client environments for long periods of time, and verify that essential SUT performance parameters such as throughput, latency and QoS support are not affected.

RSTC 001 Data_Roaming_Stress

Title	Verify ability of SUT to withstand long-duration roaming stress from many data clients
Purpose	Stress SUT with large numbers of mobile laptop/PDA clients exchanging data traffic for a long time, and verify that performance is unaffected. Verify SUT health before and after the test period using standard throughput and latency tests.
SUT Feature(s) Tested	Control plane robustness, client context management, long-term stability, AP/controller context interchange robustness
Requirement(s)	• WaveApps application running on host PC • WT-90 chassis with Wi-Fi Waveblades and Ethernet Waveblade(s) • SUT set up to support UDP traffic • DHCP enabled with internal or external DHCP server • RADIUS server with support for EAP types used
Test Setup	• Configure the SUT with security modes on different SSIDs to:

	Open, WPA-PSK, and WPA2-EAP-TLS (Note: if the SUT supports only one active SSID, use only WPA2-EAP-TLS security mode and a single SSID) • Set the Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode APs) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode APs) • Set client data PHY rate to 54 Mb/s and management PHY rate to 6 Mb/s • Set client security types to match those in the SUT • Run test with 500 roaming clients total
Procedure	1. Configure the SUT as indicated above 2. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT as a group, and record the results 3. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT as a group, and record the results 4. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT as a group, and record the results 5. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT as a group, and record the results 6. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT as a group, and record the results 7. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT as a group, and record the results 8. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT as a group, and record the results 9. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT as a group, and record the results 10. Launch the WaveApps application 11. Select the Roaming Delay test 12. Select the test ports (i.e., APs) to use for the Roaming Delay test and configure each port into 802.11g or 802.11a mode as required 13. Create client groups to support 500 roaming clients; select the SSIDs for the clients and configure the clients to the appropriate security modes for the SSIDs, and assign IP addresses using DHCP 14. Create an Ethernet client group on the correct ports with the number of Ethernet clients set to 1 15. Create a roam sequence wherein all clients in all groups roam over all APs in the SUT in a uniform manner 16. Set the dwell time to 1000 seconds, select a uniform

	distribution of clients and roams, and set the total roaming duration to 72 hours 17. Run the test and wait until it completes 18. Verify that at the end of 72 hours clients are continuing to roam 19. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT as a group again, and record the results 20. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT as a group again, and record the results 21. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT as a group again, and record the results 22. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT as a group again, and record the results 23. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT as a group again, and record the results 24. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT as a group again, and record the results 25. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT as a group again, and record the results 26. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT as a group again, and record the results
Test Priority	Mandatory
Test Type	Stress
Pass/Fail Criteria	The throughput and latency measurements performed before and after the 72-hour roaming stress test must be within 5% of each other. Further, the aggregate number of roam failures must be less than 10% of the total number of roams performed. If either of these two conditions is not satisfied, the test must be considered to have failed.

RSTC 002 VoIP_Roaming_Stress

Title	Verify ability of SUT to withstand long-duration roaming stress from many handset (VoIP) clients
Purpose	Stress SUT with large numbers of roaming VoIP handset clients performing voice calls for a long time, and verify that performance

	is unaffected. Verify SUT health before and after using standard throughput and latency tests.
SUT Feature(s) Tested	Control plane robustness, client context management, QoS robustness, AP/controller context interchange robustness, long-term stability
Requirement(s)	• WaveApps application running on host PC • WT-90 chassis with Wi-Fi Waveblades and Ethernet Waveblade(s) • SUT set up to support VoIP traffic with QoS functions enabled • DHCP enabled with internal or external DHCP server • RADIUS server with support for EAP types used
Test Setup	• Configure the SUT with security modes on different SSIDs to: Open, WPA-PSK, and WPA2-EAP-TLS (Note: if the SUT supports only one active SSID, use only WPA2-EAP-TLS security mode and a single SSID) • Set the Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode APs) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode APs) • Set the handset codec to G.711 and the baseline call duration to 5 minutes • Set handset security types to match those in the SUT • Run test with 500 roaming handsets total
Procedure	1. Configure the SUT as indicated above 2. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT as a group, and record the results 3. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT as a group, and record the results 4. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT as a group, and record the results 5. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT as a group, and record the results 6. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT as a group, and record the results 7. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT as a group, and record the results 8. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT as a group, and record the results 9. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT as a group, and record the results 10. Launch the WaveApps application 11. Select the Roaming Service Quality test

	12. Select the test ports (i.e., APs) to use for the Roaming Service Quality test and configure each port into 802.11g or 802.11a mode as required 13. Create client groups to support 500 roaming handsets; select the SSIDs for the handsets and configure them to the appropriate security modes for the SSIDs; assign IP addresses using DHCP 14. Create an Ethernet client group on the correct ports with the number of Ethernet clients set to 1 15. Place all handsets into the roam sequence 16. Set the roam rate to 30 roams/minute and set the total roaming duration to 72 hours 17. Set the codec type to G.711 and the baseline call duration to 5 minutes 18. Run the test and wait until it completes 19. Verify that at the end of 72 hours clients are continuing to roam 20. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT as a group again, and record the results 21. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT as a group again, and record the results 22. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT as a group again, and record the results 23. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT as a group again, and record the results 24. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT as a group again, and record the results 25. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT as a group again, and record the results 26. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT as a group again, and record the results 27. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT as a group again, and record the results
Test Priority	High
Test Type	Stress

Pass/Fail Criteria	The throughput and latency measurements performed before and after the 72-hour VoIP roaming stress test must be within 5% of each other. Further, the aggregate number of roam failures must be less than 10% of the total number of roams performed, and the VoIP QoS during the test must not drop below an R-value of 70. If any of these conditions is unsatisfied, the test must be considered to have failed.

Connection Stress

The SUT must be able to maintain good performance over very long periods of time, even though clients may be constantly connecting and disconnecting from the network, while concurrently attempting to transfer high rates of traffic with multiple traffic types. The following stress tests therefore subject the SUT to extended periods of connection and disconnection, with a background traffic load in order to stress the data plane of the system, and verify that the SUT recovers properly and does not experience progressive degradation in capabilities.

CSTC 001 Client_Connection_Stress

Title	Verify ability of SUT to withstand high levels of connection stress with mixed data background traffic
Purpose	Stresses the SUT with a mix of long periods of rapid connections and disconnections (AAA Authentication Load Test) plus high data traffic load of multiple traffic types (WiMix Test). SUT data plane and control plane performance is verified before and after the test period using standard throughput, latency, and client capacity measurements.
SUT Feature(s) Tested	Control path robustness, client context management, control path and data path interaction, long-term stability
Requirement(s)	• WaveApps and WiMix applications running on one or more host PCs • WT-90 chassis with Wi-Fi Waveblades and Ethernet Waveblades • SUT set up to support RADIUS security and multiple SSIDs • DHCP enabled with internal or external DHCP server • RADIUS server with support for EAP types used
Test Setup	• Configure the SUT with security modes on different SSIDs to: Open, WPA-PSK, and WPA2-EAP-TLS (Note: if the SUT supports only one active SSID, use only WPA2-EAP-TLS security mode and a single SSID) • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode APs) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode APs) • Set client PHY rate to 54 Mb/s

	• Set client security types to match those in the SUT • Set client authentication load to 10 connections per second • Set number of clients to 50 WiMix clients per AP, or 100 Authentication Load Test clients per AP
Procedure	1. Configure the SUT as indicated above 2. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT, and record the results 3. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT, and record the results 4. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT, and record the results 5. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT, and record the results 6. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT, and record the results 7. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT, and record the results 8. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT, and record the results 9. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT, and record the results 10. Perform CBTC 002, Max_Client_Capacity_DHCP, on all APs in the SUT and record the results 11. Launch the WiMix application 12. Select the WiMix test and select the Enterprise profile within the WiMix test 13. Select the test ports (i.e., APs) to use for the WiMix test and configure each port into 802.11g or 802.11a mode as required; 50% of the SUT test ports should be selected to sustain WiMix traffic 14. Create client groups to support (50 x *N*) WiMix clients, where *N* is the number of APs in the SUT used for the WiMix test; select the SSIDs for the clients and configure the clients to the appropriate security modes for the SSIDs, and assign IP addresses using DHCP 15. Create an Ethernet client group on the correct ports with the number of Ethernet clients set to 1 16. Set traffic parameters consistent with the Enterprise traffic mix and the trial duration to 72 hours 17. Now launch the WaveApps application, on the same or a different host PC 18. Select the AAA Authentication Load test under the Security Test Suite

	19. Select the test ports (i.e., APs) to use for the AAA Authentication Load test and configure each port into 802.11g or 802.11a mode as required; those SUT test ports that are not selected for WiMix traffic should be used for the AAA Authentication Load test 20. Create client groups to support (100 x *M*) AAA Authentication Load clients, where *M* is the number of APs in the SUT assigned for the AAA Authentication Load test; select the SSIDs for the clients and configure the clients to the appropriate security modes for the SSIDs, and assign IP addresses using DHCP 21. Create an Ethernet client group on the correct ports with the number of Ethernet clients set to 1 22. Set the client connection rate to 10 per second, the timeout to 1 second, the iteration duration to 1000 seconds, and the settle time between iterations to 5 seconds; set the trial duration to 72 hours 23. Start both the WiMix and the AAA Authentication Load tests within 30 seconds of each other, and wait until both tests complete 24. Verify that at the end of 72 hours both tests are still running and no error messages have been reported to the respective consoles 25. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT again, and record the results 26. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT again, and record the results 27. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT again, and record the results 28. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT again, and record the results 29. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT again, and record the results 30. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT again, and record the results 31. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT again, and record the results 32. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT again, and record the results 33. Perform CBTC 002, Max_Client_Capacity_DHCP, on all APs in the SUT and record the results
Test Priority	Mandatory
Test Type	System

Pass/Fail Criteria	The throughput and latency measurements performed before and after the 72-hour stress test must be within 5% of each other. Further, the client capacity measurements before and after the stress test must be equal. If either of these two conditions is not satisfied, the test must be considered to have failed.

CSTC 002 Client_Connection_Data_Overload_Stress

Title	Verify ability of SUT to withstand high levels of connection stress in the presence of UDP data traffic overloads
Purpose	Stresses the SUT with a mix of rapid connections and disconnections (AAA Authentication Rate Test) plus a steady-state downstream UDP data overload (packet loss test with ILOAD higher than theoretical maximum). SUT data plane performance is verified before and after the test period using standard throughput and latency measurements.
SUT Feature(s) Tested	Control path robustness, client context management, control stability under data overload, long-term stability
Requirement(s)	• WaveApps running on one or more host PCs • WT-90 chassis string with Wi-Fi Waveblades and at least 3 Ethernet Waveblades • SUT with at least 10 APs set up to support RADIUS security and multiple SSIDs • DHCP enabled with internal or external DHCP server • RADIUS server with support for EAP types used
Test Setup	• Configure the SUT with security modes on different SSIDs to: Open, WPA-PSK, and WPA2-EAP-TLS (Note: if the SUT supports only one active SSID, use only WPA2-EAP-TLS security mode and a single SSID) • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode APs) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode APs) • Set client PHY rate to 54 Mb/s • Set client security types to match those in the SUT • Set client authentication load to 20 connections per second • Set the downstream UDP intended load applied per Ethernet port to 512 byte packets and 100% of the theoretical maximum rate • Set number of clients to 50 Packet Loss Test clients per AP, or 100 Authentication Load Test clients per AP
Procedure	1. Configure the SUT as indicated above 2. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT, and record the results 3. Perform PBTC 002, Downstream_UDP_80211g_Throughput,

	on all 802.11g APs in the SUT, and record the results 4. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT, and record the results 5. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT, and record the results 6. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT, and record the results 7. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT, and record the results 8. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT, and record the results 9. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT, and record the results 10. Launch the WaveApps application 11. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 12. Select the test ports (i.e., APs) to use for the UDP data traffic overload (i.e., the Packet Loss Test) and configure each port into 802.11g or 802.11a mode as required; 50% of the SUT Wi-Fi test ports should be selected to sustain the data traffic 13. Create client groups to support (50 x *N*) Packet Loss Test clients, where *N* is the number of APs in the SUT selected in step 12 above; select the SSIDs for the clients and configure the clients to the appropriate security modes for the SSIDs, and assign IP addresses using DHCP 14. Create Ethernet client group(s) on the correct Ethernet test ports with the total number of Ethernet clients set equal to the number of Wi-Fi clients; select all but one of the Ethernet WaveBlades to support these Ethernet clients 15. Select UDP traffic type, set the frame size to 512 bytes, and set the ILOAD to (235,000 * *E*) frames/second, where *E* is the number of Ethernet ports assigned for the Packet Loss Test 16. Set the trial duration to 72 hours 17. Now launch a second instance of WaveApps application, on the same or a different host PC 18. Select the AAA Authentication Load test under the Security Test Suite 19. Select the test ports (i.e., APs) to use for the AAA Authentication Load test and configure each port into 802.11g or 802.11a mode as required; those SUT test ports that are not selected for WiMix traffic should be used for the AAA Authentication Load test 20. Create client groups to support (100 x *M*) AAA Authentication Load clients, where *M* is the number of APs in the SUT assigned for the AAA Authentication Load test; select the

	SSIDs for the clients and configure the clients to the appropriate security modes for the SSIDs, and assign IP addresses using DHCP 21. Create an Ethernet client group on the correct ports with the number of Ethernet clients set to 1 22. Set the client connection rate to 20 per second, the timeout to 1 second, the iteration duration to 1000 seconds, and the settle time between iterations to 5 seconds; set the trial duration to 72 hours 23. Start both the Packet Loss and AAA Authentication Load tests within 30 seconds of each other, and wait until both tests complete 24. Verify that at the end of 72 hours both tests are still running, no error messages have been reported to the respective consoles, and all of the clients in the Packet Loss test are still connected 25. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT again, and record the results 26. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT again, and record the results 27. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT again, and record the results 28. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT again, and record the results 29. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT again, and record the results 30. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT again, and record the results 31. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT again, and record the results 32. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT again, and record the results
Test Priority	High
Test Type	System
Pass/Fail Criteria	The throughput and latency measurements performed before and after the 72-hour stress test must be within 5% of each other. Otherwise, the test must be considered to have failed.

Overload Recovery

The SUT must be able to withstand temporary overloads (in terms of both data and client connections) and recover after the overload is removed to the original state. Failure to recover to the original state indicates issues such as memory leaks or internal data corruption.

ORTC 001 Data_Overload_Recovery

Title	Verify ability of SUT to recover from a high degree of data traffic overload without adverse effects
Purpose	Determine whether the SUT can return to its original capabilities after a predetermined time period during which it is subjected to a high degree of data overload. A UDP packet loss test is used to provide the data traffic overload, and the measurement of SUT capabilities before and after is done using throughput, latency and VoIP roaming tests.
SUT Feature(s) Tested	Data path robustness, stability under data overload, recovery from overload
Requirement(s)	• WaveApps running on a host PC • WT-90 chassis string with at least 25 Wi-Fi Waveblades and at least 5 Ethernet Waveblades • SUT with at least 25 APs set up to support RADIUS security and multiple SSIDs • DHCP enabled with internal or external DHCP server • RADIUS server with support for EAP types used
Test Setup	• Configure the SUT with security modes on different SSIDs to: Open, WPA-PSK, and WPA2-EAP-TLS (Note: if the SUT supports only one active SSID, use only WPA2-EAP-TLS security mode and a single SSID) • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode APs) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode APs) • Set client PHY rate to 54 Mb/s • Set client security types to match those in the SUT • Set the downstream UDP intended load applied per Ethernet port to 512 byte packets and 100% of the theoretical maximum rate • Set the number of clients to 50 per AP
Procedure	1. Configure the SUT as indicated above 2. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT, and record the results 3. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT, and record the results 4. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT, and record the results 5. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT, and record the results 6. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT, and record the results 7. Perform PBTC 021, Downstream_80211g_Packet_Latency, on

	all 802.11g APs in the SUT, and record the results 8. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT, and record the results 9. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT, and record the results 10. Perform PBTC 063, VoIP_Roaming_80211g, on all 802.11g APs in the SUT, and record the results 11. Perform PBTC 064, VoIP_Roaming_80211a, on all 802.11a APs in the SUT, and record the results 12. Wait 60 seconds after performing the above tests for the SUT to settle 13. Launch the WaveApps application 14. Select the Packet Loss Test under the IEEE 802.11.2 Benchmark Test Suite 15. Select the test ports (i.e., APs) to use for the UDP data traffic overload (i.e., the Packet Loss Test) and configure each port into 802.11g or 802.11a mode as required 16. Create client groups to support (50 x *N*) Packet Loss Test clients, where *N* is the number of APs in the SUT used in the test; select the SSIDs for the clients and configure the clients to the appropriate security modes for the SSIDs, and assign IP addresses using DHCP 17. Create Ethernet client group(s) on the correct Ethernet test ports with the total number of Ethernet clients set equal to the number of Wi-Fi clients 18. Select UDP traffic type, set the frame size to 512 bytes, and set the ILOAD to (235,000 * *E*) frames/second, where *E* is the number of Ethernet ports used in the test 19. Set the trial duration to 72 hours 20. Run the Packet Loss Test and wait until it completes 21. Verify that at the end of 72 hours the test is still running, no error messages have been reported to the console, and all of the clients are still connected 22. Wait at least 300 seconds after the above test has completed to allow the SUT to settle and recover if necessary 23. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT again, and record the results 24. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT again, and record the results 25. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT again, and record the results 26. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT again, and record the results

	27. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT again, and record the results 28. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT again, and record the results 29. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT again, and record the results 30. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT again, and record the results 31. Perform PBTC 063, VoIP_Roaming_80211g, on all 802.11g APs in the SUT, and record the results 32. Perform PBTC 064, VoIP_Roaming_80211a, on all 802.11a APs in the SUT, and record the results
Test Priority	Mandatory
Test Type	System
Pass/Fail Criteria	The throughput and latency measurements performed before and after the 72-hour stress test must be within 5% of each other. Further, the VoIP roaming time and voice quality measurements before and after the stress test must be within 10% of each other. If either of these two conditions is not satisfied, the test must be considered to have failed.

ORTC 002 Connection_Overload_Recovery

Title	Show function
Purpose	Determine whether the SUT can return to its original capabilities after a predetermined time period during which it is subjected to a high degree of client connection overload. An AAA authentication load test is used to provide the connection overload, and the measurement of SUT capabilities before and after is done using throughput, latency and VoIP roaming tests.
SUT Feature(s) Tested	Control path robustness, stability under control plane overload, recovery from overload
Requirement(s)	• WaveApps application running on one host PC • WT-90 chassis string with at least 25 Wi-Fi Waveblades and one Ethernet Waveblade • SUT with at least 25 APs set up to support RADIUS security and multiple SSIDs, and static IP addressing • RADIUS server with support for EAP types used
Test Setup	• Configure the SUT with security modes on different SSIDs to: Open, WPA-PSK, and WPA2-EAP-TLS (Note: if the SUT supports only one active SSID, use only WPA2-EAP-TLS security mode and a single SSID) • Set Basic Rate Set on SUT APs to 1Mbps, 2Mbps, 5.5Mbps,

	6Mbps, 11Mbps, 12Mbps and 24Mbps (802.11g mode APs) and/or 6Mbps, 12Mbps and 24Mbps (802.11a mode APs) • Set client PHY rate to 54 Mb/s • Set client security types to match those in the SUT • Set the number of Authentication Load Test clients to 100 per AP, and the client authentication load to 30 connections per second
Procedure	1. Configure the SUT as indicated above 2. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT, and record the results 3. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT, and record the results 4. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT, and record the results 5. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT, and record the results 6. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT, and record the results 7. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT, and record the results 8. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT, and record the results 9. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT, and record the results 10. Perform PBTC 063, VoIP_Roaming_80211g, on all 802.11g APs in the SUT, and record the results 11. Perform PBTC 064, VoIP_Roaming_80211a, on all 802.11a APs in the SUT, and record the results 12. Wait 60 seconds after performing the above tests for the SUT to settle 13. Select the AAA Authentication Load test under the Security Test Suite 14. Select the test ports (i.e., APs) to use for the UDP data traffic overload (i.e., the Packet Loss Test) and configure each port into 802.11g or 802.11a mode as required 15. Create client groups to support (100 x M) AAA Authentication Load clients, where M is the number of APs in the SUT assigned for the AAA Authentication Load test 16. Select the SSIDs for the test clients and configure the clients to the appropriate security modes for the SSIDs, and assign IP addresses statically 17. Create an Ethernet client group on the Ethernet test port with the number of Ethernet clients set to 1

	18. Set the client connection rate to 30 per second, the timeout to 1 second, the iteration duration to 1000 seconds, and the settle time between iterations to 5 seconds 19. Set the trial duration to 72 hours 20. Run the AAA Authentication Load Test and wait until it completes 21. Verify that at the end of 72 hours that no error messages have been reported to the console 22. Wait at least 300 seconds after the above test has completed to allow the SUT to settle and recover if necessary 23. Perform PBTC 001, Upstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT again, and record the results 24. Perform PBTC 002, Downstream_UDP_80211g_Throughput, on all 802.11g APs in the SUT again, and record the results 25. Perform PBTC 004, Upstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT again, and record the results 26. Perform PBTC 005, Downstream_UDP_80211a_Throughput, on all 802.11a APs in the SUT again, and record the results 27. Perform PBTC 020, Upstream_80211g_Packet_Latency, on all 802.11g APs in the SUT again, and record the results 28. Perform PBTC 021, Downstream_80211g_Packet_Latency, on all 802.11g APs in the SUT again, and record the results 29. Perform PBTC 022, Upstream_80211a_Packet_Latency, on all 802.11a APs in the SUT again, and record the results 30. Perform PBTC 023, Downstream_80211a_Packet_Latency, on all 802.11a APs in the SUT again, and record the results 31. Perform PBTC 063, VoIP_Roaming_80211g, on all 802.11g APs in the SUT, and record the results 32. Perform PBTC 064, VoIP_Roaming_80211a, on all 802.11a APs in the SUT, and record the results
Test Priority	High
Test Type	System
Pass/Fail Criteria	The throughput and latency measurements performed before and after the 72-hour stress test must be within 5% of each other. Further, the VoIP roaming time and voice quality measurements before and after the stress test must be within 10% of each other. If either of these two conditions is not satisfied, the test must be considered to have failed.