WHITE PAPER

802.11n Access Point Performance Goals

Table of Contents

Introduction 4
MIMO Performance 5
Basic Aggregation Testing 6
Looking for Aggregation Performance Killers 7
Forward Rate Limits 8
Encryption Performance 9
Dual Radio AP Performance 10
Mixed Mode Clients and Protection 11
QoS and All the Rest 12
Conclusion 12

Introduction

As the volume of 802.11n access points (APs) continues to grow, it remains critical that the end-user experience be a primary focus throughout development. Ixia has witnessed the potential performance issues and capabilities of 802.11n APs first hand, along with the issues associated with their chipsets.

As a result, this document describes a series of tests for use in analyzing critical aspects of 802.11n access point performance:

- MIMO Performance
- Basic Aggregation (AMPDU)
- Forwarding Rate Limits
- Encryption Performance
- Dual Radio AP Performance
- Mixed Mode Client and Protection
- QoS

MIMO Performance

The Issue: Determining whether problems occur when an 802.11n access point encounters a MIMO situation including more than one spatial stream. When testing 802.11n access points, findings show that each spatial streams must be within specifications regarding EVM, phase noise, and frequency errors.

MIMO decoders require the performance of each stream to be within these specifications in order to be decoded consistently. For example, if a radio is outside specifications on one of the spatial streams and the stream cannot be properly decoded, poor throughput or forwarding rates will occur with the MIMO streams.

Test Procedure: Run the IxVeriWave Downstream Packet Loss test at 50% theoretical maximum with a single-stream MCS index of 0-7 and a multi-stream MCS index of 8-15. Pay close attention to the FCS error rates.

Analysis of Results: If a significant increase in FCS errors occurs with a multi-stream encoding (MCS index of 8-15), this indicates an existing MIMO problem that will not be solved through tweaking of the attenuation or other system parameters. Additional performance testing will not fall into place until this specific issue is addressed; therefore, it is essential to make sure you have proper MIMO operation handled upfront.

Basic Aggregation Testing

The Issue: 802.11n access point performance relies heavily on the amount of MPDUs per AMPDU that the DUT is capable of delivering and forwarding. If an AP can only aggregate half of what is needed to get to the highest rate of performance, a severely degraded end-user experience may result.

Test Procedure: Run the IxVeriWave Downstream Packet Loss test with a frame size of 1518 bytes, MCS=15, and a frame rate equal to the theoretical maximum.

Analysis of Results: An 802.11n access point should be capable of producing 42 MPDUs per AMPDU under these conditions. Therefore, if the AP is only aggregating at say 16 MPDUs per AMPDU, performance will be limited to about 232Mbs instead of the 267Mbs achievable with full aggregation.

Test Procedure: Next, run the IxVeriWave Downstream Packet Loss test with a small frame size of 88 bytes, MCS=15, and a frame rate equal to the theoretical maximum.

Analysis of Results: An 802.11n access point should theoretically be producing 64 MPDUs per AMPDU. The effect on performance due to lack of aggregation is even more pronounced when forwarding small frame sizes. Theoretically the AP should be able to forward 121Mbs in this test condition. However, if the AP is only capable of aggregating 32 MPDUs the forwarding rate drops to just 82Mbs.

Test Procedure: Run the IxVeriWave Upstream Packet Loss test in a clean environment achieved by using a bypass channel model and cabled environment. This will test the ability of the 802.11n AP to forward full-size AMPDUs as high as 64 MPDUs on an 88 byte frame, or the full 42 MPDUs on a larger frame size.

Analysis of Results: Poor Block ACK formation can be seen if there are frames that were received by the AP with FCS errors, which then must be retried. The Block ACK bitmap string indicates which frames in the block of 64 frames have or have not been received.

Incorrect management of the BLK ACK will result in useless retries, or dropped frames. Therefore, if there is performance degradation in the upstream, it may be due to a faulty chipset that is not properly relaying which packets it has and hasn't received.

Another possible performance problem will be Radio Rx drift, where the radio receiver is actually the cause of the problem. Radio Rx drift usually occurs more on these large aggregates than on singletons due to the extended amount of time the radio has to stay locked onto the signal in order to achieve the full throughput.

Looking for Aggregation Performance Killers

Aggregation performance killers refer to the actual AMPDUs that the 802.11n access point is generating or seeing. The first performance killer is what is known as turnaround time.

Turnaround time can be seen in the IFG or Inter-frame Gap, which is the time between when the Block ACK is received and the next AMPDU is sent. By specification the IFG should be between 40 – 160 microseconds (usecs) based on the standard backoff algorithms.

There are two possible causes for slow turnaround times. The first is that long IFG in downstream forwarding may be due to a processing limitation in the AP. By providing a sustained large offered load to the AP's Ethernet port, it will be required to form AMPDUs to keep up its forwarding rate. If the processor in the AP cannot keep up in forming the AMPDUs, it can be evidenced by the longer IFG.

Conversely, short IFG is a way to actually obtain very high downstream performance. By not adhering to the normal timing requirements (e.g. shorting backoff timers) an AP can greatly improve performance. However, this will cause severe degradation in bi-directional performance since the client devices will not be allowed equal access for upstream traffic.

Timely re-transmission comes into play when the AP must resend one or more MPDUs that were sent as an AMPDU but were not received by the client. The 802.11n specification says that when an AMPDU is received by a station any MPDU inside that aggregated transmission that was not properly received will not be acknowledged in the Block ACK.

The specification requires that sending station include the missing MPDUs in the very next AMPDU that it sends. However, many current data engines basically have to pre-configure or pre-load the next AMPDU in order to get it out in any reasonable amount of time. So we don't usually see those error frames in the next AMPDU, rather they will come out in some subsequent one. That's acceptable to an extent depending on the duration of the delay. Long delays will have an effect on TCP performance as it measures the response time of the system.

Forward Rate Limits

The Issue: An 802.11n access point should be able to forward every 802.11 frame that it acknowledges without any frame loss.

Test Procedure: Run the IxVeriWave Upstream Packet Loss test with the maximum possible offered load into the 802.11n access point.

Analysis of Results: Since the 802.11n access point is only going to acknowledge good frames that it actually has received, there should be no frame loss as it is expected that the AP can forward all frames in the upstream direction.

Test Procedure: Run the IxVeriWave downstream throughput test at the three standard frame sizes (1518, 512 and 88 bytes). It is recommended to run the test using the largest frame size first because the rates at which packets are forwarded is lesser with larger frame sizes.

With smaller frame sizes, the rates at which frames must be forwarded is much greater. Loading some APs with these extreme rates had been known to cause an AP crash.

Analysis of Results: Most 802.11n access points are rate limited in terms of frames per second. Essentially, the big frames will go through whatever rates they have and by the time the frame size gets down to 512 bytes the 802.11n AP has most likely already encountered an issue where it can't forward frames in the downstream direction at the theoretical limits (100,000 frames/second).

The limits on small frame forwarding rate will in turn impact TCP performance. If there are several TCP sessions in progress and the 802.11n AP is unable to forward several small frames in this mixed traffic mode the AP's performance will be impacted severely.

Encryption Performance

The Issue: Can an access point keep up with line rate AES encryption? Enterprise class 802.11n APs are not going to be running in the real-world environment without encryption turned on; therefore these devices should reach near theoretical max throughput with encryption.

Test Procedure: Run the IxVeriWave throughput test with WPA2 security turned on.

Analysis of Results: When running the IxVeriWave throughput test with WPA2 security, it appears that some 802.11n access points are capable of handling this in regards to performance, while first generation 802.11n APs don't have the capability to handle line rate encryption. This will cause a significant drop off in throughput performance and reveal limitations in buffer design.

Key management problems also occur when this throughput test begins to scale. For example, when the number of clients go from 1 to 20 the AP must properly manage the keying operations for all client sessions. One evidence of encryption key problems is ARP failures. If ARP failures occur for no reason other than the turn on of encryption there may be a mismatch in the keys, which is revealed if an ARP frame is sent and doesn't seem to go anywhere.

Dual Radio AP Performance

The Issue: An 802.11n access point consists of two radios as a solution for an endpoint. This is intended to be able to increase the capacity on the 802.11n AP by using both radios simultaneously, usually one radio for legacy traffic and the other 11n clients.

The issue is: can AP actually handle traffic on both radios simultaneously?

Test Procedure: Run the IxVeriWave throughput test using both radios simultaneously, while connecting 10 clients per radio. This test can be run even if the radios are set with different capabilities (20 MHz on g, 40 MHz on a). This is so because a comparison of single radio results vs. dual radio results will reveal if there is a forwarding rate problem. For instance, the second test using two radios should be 2x of what was obtained in the previous test using one radio.

Analysis of Results: Because the dual radios typically share the same data processing engine, forwarding rate limits often occur. The CPU is also being shared between both these radios causing capacity to be far less than theoretical estimates.

Mixed Mode Clients and Protection

The Issue: Can 802.11n access points provide proper aggregation for 11n clients while servicing legacy clients?

Test Procedure: Run the IxVeriWave Throughput Test using a mixture of clients (for example, 4 clients and 16 n-clients), in order to determine whether the 802.11n device is capable of gaining access to a significant portion of the medium capacity. IxVeriWave's WaveApps benchmarks are designed to equitably distribute the load between client types by calculating the required bandwidth for each client.

Analysis of Results: CTS-to-self Protection is the standard mechanism implemented in most 802.11n access points and is evident when packets are being forwarded downstream using mixed-mode clients. The CTS-to-self protection takes up some of the bandwidth causing the throughput numbers in the downstream mode to decrease accordingly, while upstream throughput is dependent upon the client settings.

In some cases the 802.11n AP may choose to stop aggregation, because the system fails to allow for aggregation in mixed modes. This will therefore cause the n-clients to be unable to use the amount of bandwidth they would have otherwise, dramatically decreasing the overall throughput in the system.

802.11n access points may also go into RTS/CTS as a result of default behavior. However, RTS/CTS cause frames to forward extremely slow, once again resulting in low throughput rates.

QoS and All the Rest

The Issue: Is the 802.11n access point able to correctly forward real-world traffic with prioritization.

Test Procedure: Run the IxVeriWave WaveQoE test using one of the pre-configured deployment models (enterprise, hospital, etc.). Set the QoS for voice and video traffic as appropriate for the Device Under Test (DUT).

Determine the highest achievable load using the IxVeriWave linear search mechanism. This will provide insight into what the traffic actually looks like.

Analysis of Results: An 802.11n AP should drop background and best effort traffic while maintaining forwarding rates for prioritized traffic. However, in many cases the AP will inappropriately use aggregation of video traffic leading to jitter. In other words, the AP is unable to recognize for a particular priority how often it needs to provide transmission opportunities, or what it must do to avoid delay.

The WaveQoE test will create congestion, showing the effects of forwarding problems that were seen in previous tests. This occurs because of the large amount of packets that are involved and their various sizes.

Conclusion

By breaking down the testing of 802.11n APs as outlined here, basic problems with design and implementation can be revealed. Resolving basic forwarding problems using simple UDP traffic will ultimately help in the forwarding of real-world application traffic running over UDP or TCP.

Solving forwarding and latency problems prior to running prioritized QoS traffic will ensure that any problems revealed during these more sophisticated tests are actually related to the QoS mechanism itself.

Any AP that can reasonably pass these tests should have no problem dealing with the most stressful real-world deployment.

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(Fax) 818.871.1805
www.ixiacom.com

Other Ixia Contacts
Info: info@ixiacom.com
Investors: ir@ixiacom.com
Public Relations: pr@ixiacom.com
Renewals: renewals@ixiacom.com
Sales: sales@ixiacom.com
Support: support@ixiacom.com
Training: training@ixiacom.com

For more information see http://www.ixiacom.com/