it^{+46}

Link Performance Parameters in IEEE 802.11

– How to increase the throughput of a wireless long distance link

IT+46

Louise Berthilson

Alberto Escudero-Pascual

www.it46.se

April 2007

v0.6

Table of Contents

1.   Introduction

This document is a general guide for advanced link performance parameters for wireless (IEEE 802.11 based) networks. It targets a set of features that with correct usage can improve the throughput of the wireless link. Most of this parameters are not part of the IEEE 802.11 standard and they need to be implemented carefully. The parameters discussed in this document modify the behaviour of IEEE 802.11 MAC. Other optimizations in the IP or transport layer are out of the scope of this document.

To make the document as simple as possible we have described all features following a common template: functionality, default values, valid range and instruction on when and how to best use the feature.

Although the guide can be applied with many wireless access points, we have used the smartBridges serie AirPoint/AirClient NEXUS PRO TOTAL as a reference. Notice that many of these parameters can have different names depending on the vendor.

Link Performance Parameters in IEEE 802.11   April 2007
Louise Berthilson   Version 0.6
Alberto Escudero Pascual

2.   Fragment length

Default[1]: 2346
Range: 256 – 2346
Unit: Bytes
IEEE 802.11 standard: Yes

Functionality:
The IEEE 802.11 standard includes an optional feature that allows radio based NICs and access points to fragment data frames into smaller pieces to improve performance in presence of interference of poorly covered areas.

By sending smaller frames, the risk of collision with other frames are less likely. This results in increased reliability of frame transmission to the cost of a higher overhead.

The fragmentation effect will take place when the access point of the wireless nodes tries to send a frame with greater size than the fragmentation threshold.
Before setting the fragment length, you should first monitor the network and estimate the amount of retransmissions caused by collisions. If the level is high, then consider to change the fragmentation threshold.
In the case of less than 5% collisions, do not use the fragmentation option since the overhead of the fragmentation frames would introduce more overhead than the non-existing collisions would reduce.

When to use it:
To improve performance in presence of interference of poorly covered areas.

How to use it:
Set the fragmentation threshold to a lower value (than default) and gradually decrease it until you get better results. Since larger packets have a higher probability of collisions on the network, by decreasing the length of each packet through setting the fragmentation threshold, the probability of interference during packet transmission can be reduced.

3.   RSSI threshold

Default: - 90
Range: - 100 to – 20
Unit: dbm
IEEE 802.11 standard: No (but will not affect interoperability)

Functionality:
The RSSI (Received Signal Strength Indication) Threshold can be set to limit what RSSI is

---

1 Default value in sB access points. The default value can be different from one vendor to another.

acceptable for processing. The RSSI threshold limits the association of clients with poor signal as the packets are discarded. The RSSI threshold operates in all packets and the wireless unit will ignore any signal below the level. Changing the threshold can allow you to filter undesired signals in a noisy environment. During a site survey, the threshold can be set to the noise level (aprox. -100 dBm) to ensure that association takes place even the signal is very weak.

When to use it:
To improve performance in noisy areas. During a site survey.

How to use it:
It is recommended to set this value to be above the current noise floor to ensure optimal performance and device reliability. For example, if the average noise floor level is -88 dBm, offset it by a few dB by setting the RSSI Threshold to -85 dBm so that any signal below -85dbm will be ignored by the device.

4. Frame bursting

Default: Off
Values: On/Off
IEEE 802.11 standard: Yes, IEEE 802.11e

Functionality:
Frame bursting (aka Packet bursting) is a transmission technique supported by the draft 802.11e QoS specification. It is an approach to increase the throughput of and 802.11a,b or g based wireless networks by ignoring the DIFS and back off time.
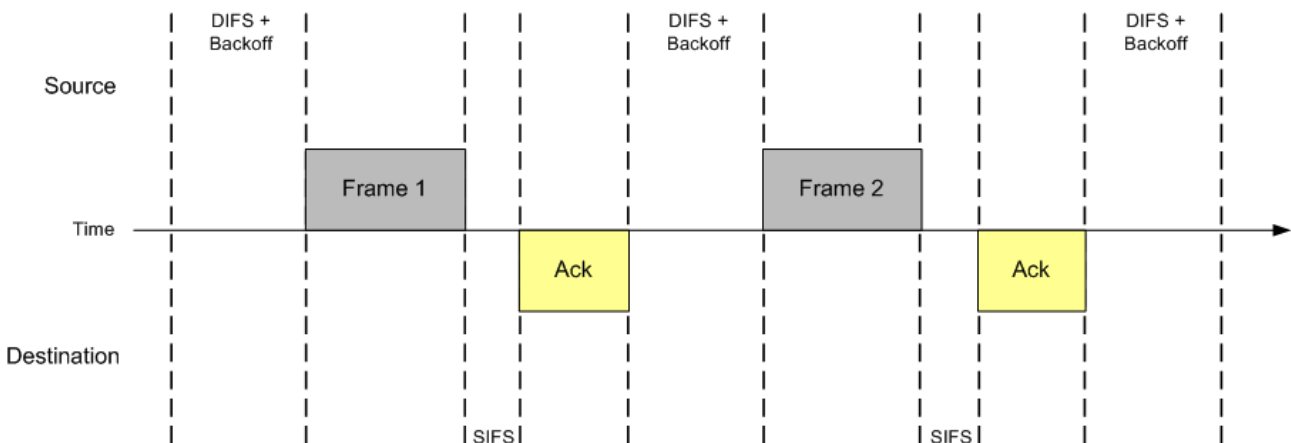

Image 1: The normal process of transmitting two frames in IEEE 802.11

[Image 1] shows the process of transmitting two frames from Source to Destination (Y axis) in time (X axis) in a normal scenario. As only one source can transmit data at a time, each node should contend for airtime during DIFS (Distributed InterFrame Space). If no other node is transmitting, the airtime is free and a frame can be transmitted. After a frame is transmitted, the transmitter

waits for a confirmation on a successful delivery from the destination, a so called Acknowledgement. The acknowledgement (ack) is sent by the receiver immediately after SIFS - Short InterFrame Space. If no ack is received by the sender, it will assume that the packet never was received and will resend it. After receiving an acknowledgement, the sender must again wait for DIFS and only then (if the air is still free) start sending the next frame.

The DIFS take up a considerable part of wireless throughput.

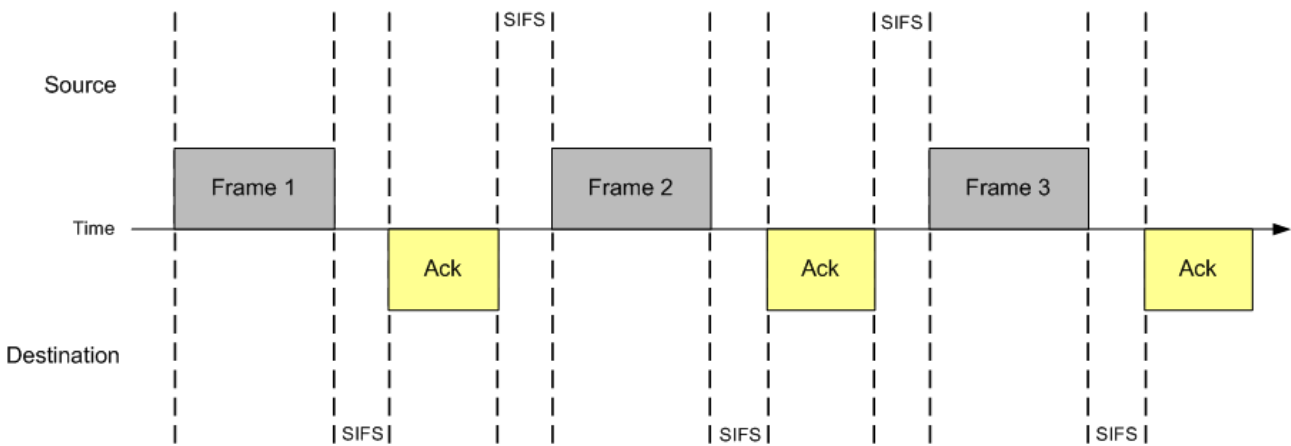In the case of using Frame Bursting the transfer of 3 frames looks like the following [Image 2]:

Image 2: Sending three frames with Frame bursting.

With Frame bursting, the source and the destination *capture the channel* in turns for their transmissions. After the first frame is transmitted and the acknowledgement is received, the transmitter does not wait the required DIFS. The sender waits only SIFS and then transmits the second data frame, etc. In this way, the sender does not give an opportunity for other nodes to start transmissions. They have to wait for the end of this frame burst transmission.

The total transmission time with frame busting is of course limited. Otherwise, large transmissions would paralyse other nodes in the network. Eliminating DIFS allows a larger chunk of data transmitted over the same period of time, thus saving the channel throughput with is increasing the total transmission performance.

Frame Bursting is a subcomponent of the IEEE 802.11e, Wireless Multimedia (WMM) and hence interoperable with other WMM implementations.

When to use it:
To improve throughput for time-sensitive services such as VoIP and multimedia streaming.

How to use it:
Frame Bursting is recommenced for *point-to-point* links to optimize the throughput by not waiting for a wireless acknowledgement frame for each transmitted frame.
It is advised to keep Frame Bursting OFF in a *point-to-multipoint* network.

5. Piggy back

Default: Off
Value: On/Off
IEEE 802.11 standard: Yes

Functionality:
Piggy back is a feature which increases the effective transmission speed.
Piggy back in wireless communication takes advantage of the fact that IEEE 802.11 MAC traffic is bidirectional. For each data frame sent, an acknowledgement must be returned. Piggy backing[2] in a wireless network consist of including the ACK in a data frame instead of sending two separate packets. This feature is part of the IEEE 802.11 standard but it is not implemented by many vendors. In Piggy Back mode, the ACK are always included in a data frame, if there is not a constant and bidirectional traffic flow the ACK will not have a chance to be transmitted and the timeout will occur. The sender will not received the ACK in time and re-transmission is required.

When to use it:
To reduce re-transmissions and collisions.

How to use it:
Piggyback is recommended ONLY for point-to-point links with a very low payload per frame and with consistent transmission at a high packet rate in a bi-directional fashion. Only in a balanced bi-directional traffic pattern, so the piggybacked ACK will not experience time out. This is because the ACKs require a data frame available to travel. If the receiver does not send data frames consistently ACKs timeout.

Piggyback is NOT recommended in a point-to-multipoint environment.

6. Throughput optimizer

Default: 6
Value: 0 – 10
Unit: -
IEEE 802.11 standard: No

Functionality:
The Throughput Optimizer is used to optimize the radio link speed and performance by adjusting its modulation technique according to the link quality. The throughput optimizer is only applicable when the data rate's "Auto Fallback" option is enabled.

Setting a higher value will cause the radio to attempt to establish at the highest possible data rate in

---

2 Radio Piggy Back should not confused with TCP Piggybacking, TCP also has a native scheme that reduces the overhead of the TCP ack transmissions when it is carrying a bidirectional traffic.

an aggressive way. A lower value implies a more stable link but with a lower throughput. The fall over between speeds takes place when the error rate is more than 30%, the throughput optimizer sets the length of the time before reducing the transmission speed (modulation). A value of "10" sets the smallest time, while a value of "0" it forces to keep the speed for the longest time.

When to use it:
To optimize the modulation technique (the speed of the link).

How to use it:
A low Throughput Optimizer value is recommended for a consistent throughput link, e.g. a low-interference point-to-point link.
For a more heavily interfered point-to-multipoint link, which may be experiencing different link qualities for different CPEs, it is recommended to have the Throughput Optimizer set to a high value.

7. RTS/CTS length (Request To Send / Clear To Send)

Default: 2346
Range: 256 – 2346
Unit: bytes
IEEE 802.11 standard: Yes

Functionality:
RTS/CTS is a method used by IEEE 802.11 wireless networks to reduce collisions caused by "hidden nodes". In brief, that is a method to grant access to use the medium which involves a handshaking process between an access point and a wireless node.
RTS/CTS introduces Collision Avoidance in CSMA/CA and hence, makes the access method more robust. At the same time, it adds unavoidable overhead to the network.

The RTS/CTS works as following: A node that wants to send data initiate the handshake with the access point by sending a RTS frame. The access point receive the RTS and responds with a CTS frame if the medium is idle. When the node received the CTS, it starts to send its data. As all nodes must be able to listen to the access point, the CTS frame will reach all nodes connected to it. CTS frame includes a time value that the other nodes must wait until they send any RTS frame. A completed RTS/CTS handshake will ensure that the node can send its data until they send any RTS frame. A completed RTS/CTS handshake will ensure that the node can send its data without being corrupted by frames sent by other nodes.

When to use it:
When hidden nodes are present, typically in point-to-multipoint networks, it is advisable to use the RTS/CTS. If there is only a few clients in the wireless network and all of them can "see" each other, the RTS/CTS option should be switched OFF.

As RTS/CTS introduces overhead in terms of RTS/CTS frames, but also reduces the overhead by reduces retransmissions of data frames, you must find out which factor is the larger one.

To find out, you need to measure the packet loss rate (on TCP level) for both options.

All SmartBridges Nexus radios have support for RTS/CTS but the default value will not trigger any RTS/CTS handshake. Setting RTS/CTS to 2346 bytes means that no packet will require RTS/CTS handshake.

How to use it:

Start by investigating whether a hidden node is present in your network. If you lower the RTS/CTS to 256, 512 or 1024, and you see the throughput increase from the baseline, then it means that there is a hidden node present. By avoiding corrupted frames due to a hidden node at the AP and reducing the retransmissions from CPE, RTS/CTS will actually increase the traffic flow on the network.

8. Preamble settings

Default: Long
Range: long, short or dynamic
IEEE 802.11 standard: Yes

Functionality:

The radio preamble is a section of data at the head of a packet that contains information for wireless devices for sending and receiving packets. The original preamble that is backwards compatible with old DSSS devices uses 144 bits.

New devices use a 72 bits preamble (known as short-preamble) The preamble includes a sequence of 56 bits having alternating 1 and 0 values that are used for synchronization. They serve to give components in the network time to detect the presence of a signal, and being reading the signal before the frame data arrives.

When to use it:

If all remote clients are short preamble enabled, the throughput can be increased by lowering the preamble sequence.

How to use it:

Long: A long preamble provides a stable link and ensures compatibility with most clients.

Short: A short preamble improves throughput performance but it only allows short preamble capable client devices to be associated.

Dynamic: A dynamic preamble allows mixing of short and long preambles

9. Concatenation (Packet aggregation, Fast Frames)

Default: Off
Values: On/Off
IEEE 802.11 standard: No

Functionality:
Concatenation is the process of joining two or more items together. It is used to combine the payload of smaller frames and send bigger frames across the wireless media to reduce overhead.

Concatenation merges data from several packets into one (packet size - up to 4000 bytes). This feature is also known as G+[3]

When to use it:
To improve throughput in stable point-to-point links.

How to use it:
Concatenation can only function in a *point-to-point* environment with a *high quality link* operating in high data rate (48 or 54 Mbps). The quality of the link must be high since any lost or erroneous concatenated frame will result in a re-transmission of *all the sub-frames* in a concatenated frame which will increase the wireless overhead.
It is NOT advisable to enable concatenation in *point-to-multipoint* environment.

10. Distance

Default: 93 miles (150 km)
Value: 1- 93 miles (1-150 km)
IEEE 802.11 standard: No

Functionality:
Distance is the equivalent ACK window value for the radio to wait for a wireless acknowledgement before a time-out occurs and a re-transmission is triggered.

All wireless devices use ACKs timeout also known a SIFS intervals that are part of the IEEE 802 standard. To ensure a good data rate, the 802.11b vendors set a SIFS that has a typical value of half of the slot time (10 microseconds).

As ACKs needs to be received within the SIFs duration. Having a SIFs of 10 microsecond means that ACK timeouts in links longer than 1.5 Kms[4].

---

3   A good reference http://www.digit-life.com/articles2/comm/tech-80211g-super.html
4   http://www.air-stream.org/ACK_Timeouts

When to use it:
If a point-to-point link is experiencing interference the distance (hence, the ACK window value) should be increased to avoid time-outs.

How to use it:
It is recommended to keep this value at the default value unless a link is experiencing interference. For a point-to-point link experiencing interference, set the distance to a value not less than the physical range of the point-to-point link.

For a point-to-multipoint network, set the distance to a value not less than the longest physical range to its furthest CPE.

11. Summary

The table below summarized the nine performance parameters that has been discussed. For each parameter, the following data is given:

- The **purpose** of using the specific parameter

- Whether the parameters is a part of the **IEEE 802.11 standard** or not.

- If the usage of the parameter will ensure **interoperability** with other 802.11 products.

- What type of **network topology** the parameter is aimed for.

Parameter	Purpose	802.11	Interoperability	Topology
Fragment length	Avoid collisions in presence of interference or poor coverage.	Yes	Yes	Any
RSSI threshold	Improve performance in noisy areas	No	Yes	Any
Frame bursting	Improve throughput.	Yes (802.11e)	802.11e: Yes 802.11a/b/g: No	PtP (not PtMP)
Piggy back	Increase transport speed	Yes	Yes?	PtP (not PtMP)
Throughput optimizer	Optimize throughput by changing modulation technique.	No	Yes	Any
RTS/CTS	Reduce collisions caused by hidden nodes.	Yes	Yes	PtMP
Preamble	Improve throughput	No?	No/Yes[5]	Any
Concatenation	Improve throughput in PtP links	No	No	PtP (not PtMP)
Distance	Avoid time-out caused by interference.	No	No?	Any

---

5 All new devices should support short preamble

12. Future work

Other performance techniques that can be of use in wireless network are;

Compression
- Increased data throughput using pre compressed frames
- Real-time hardware data compression
- Lempel Ziv compression algorithm (like in gzip, pkzip, winzip)

Dynamic Turbo
- Similar to trunking techniques used in Fast Ethernet networks
- Utilizes dual channels to "double" transmission rates
- Analyses environment and adjusts bandwidth utilization accordingly