**Beacon Interval**

The default value is 100ms and the allowed range is 1-65,535ms. This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the router to synchronize the wireless network. Please note decreasing beacon interval will improve wireless network roaming process and retain wireless connection better but slow down network throughput. For your testing in this case, you can set it to **75 or 50** and check the result later.

**RTS Threshold**

Default value is 2347 bytes and the allowed range is 0-2347 bytes, only minor change is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be activated. The wireless router sends Request to Send (RTS) frames to a particular receiving computer and negotiates the sending of a data frame. After receiving an RTS, the computer responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

This feature will prevent packet collisions on wireless network but it slows down network throughput too if used incorrectly. If you have many wireless users located far apart and also far from wireless router/access point, you can then test to decrease this threshold to **2304** bytes and check the result.

**Fragmentation Threshold**

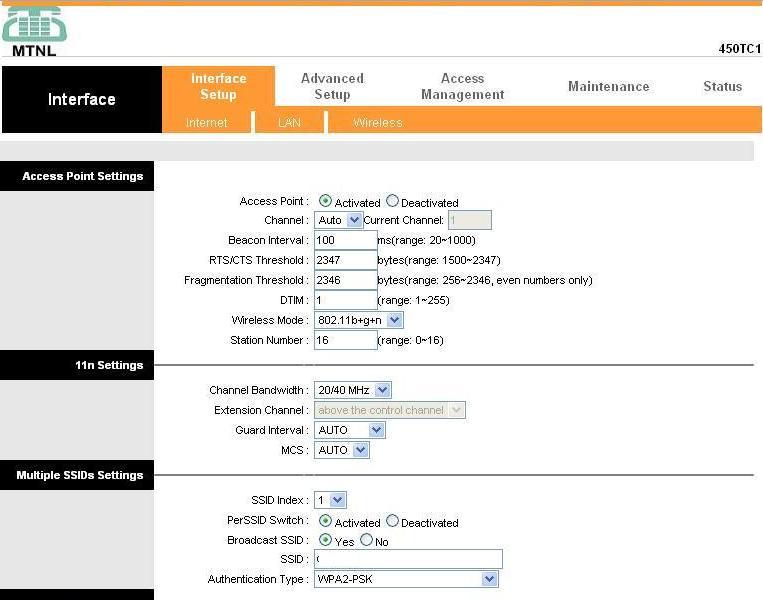
Default setting is 2346 bytes and the allowed range is 256-2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. Same as how RTS threshold works, if you notice frequent collisions on wireless network, then can consider to lower the threshold value. Please note that too low or misuse of fragmentation threshold may result in poor network performance too, so only minor change of this value is recommended. For your testing, you can set this threshold to **2304** bytes and then check the result.

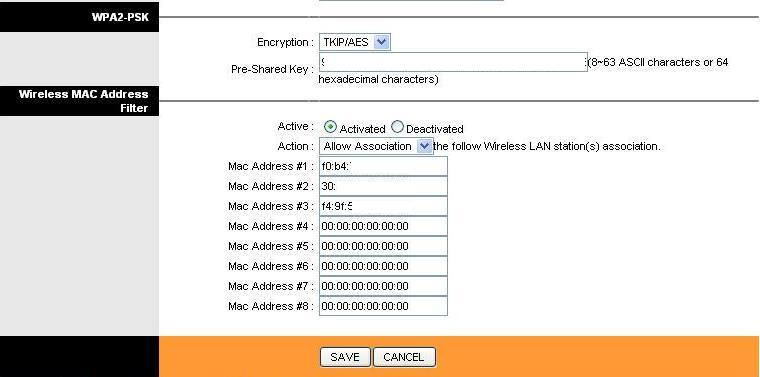
Overall, you are advised to perform the above tunings one by one and finally all together, so that you can identify the result for each change you made and make further tuning better. Hope that the above tips can help you to improve wireless network performance.

**DTIM interval**   
DTIM stands for Delivery traffic indication map or message. It is basically an additional message added after the normal beacon broadcast by your router or access point.

Depending on the timing set for your router, the router “buffers” broadcast and multicast data and let your mobile devices or clients know when to “wake up” to receive those data.

The more often that DTIM is transmitted, the more often that your mobile devices wake up, and the more battery that it uses (due to the lack of “sleep”). By setting a low value of DTIM and beacon interval, you can effectively keep your devices awake indefinitely so they never go into sleep mode when idling. In some cases the “no sleep” setup can use up to 10~20% additional power consumption.





WLAN Authentication Methods

It is important to understand that there is a distinction between being authenticated onto a wireless network and then having the traffic passed be encrypted. It is possible to be authenticated onto a network and pass open unencrypted traffic; this section looks at the commonly used methods of authentication.

There are three main methods of authentication that are used on today's wireless LANs:

* open authentication
* shared authentication
* EAP (Extensible Authentication Protocol) authentication

The **open authentication** method is the simplest of the methods used and only requires that the end device be aware of the Service-Set Identifier (SSID) used on the network, as long as the SSID is known then the device will be allowed onto the network. The problem with this method is that the SSID is typically broadcast and if it is not, it can be easy to figure out with passive capturing techniques.

The **shared authentication** method is commonly used on individual and small business wireless LAN implementations; this method uses a shared key (Pre-Shared Key – PSK) that is given to both sides of the connection; if they match then the device is allowed onto the network.

The third method uses the **Extensible Authentication Protocol (EAP)**and is the most common method used by enterprises. The EAP method utilizes an authentication server that is queried for authentication using a variety of credential options.

WLAN Encryption Methods

Along with the method used for authentication, the choice of encryption method is a very important part of deploying a wireless LAN. Many of the encryption methods that were implemented in earlier wireless LAN standards have been proven insecure and have been depreciated by more modern methods. As time goes on, this is sure to happen with all encryption techniques as they are used more commonly (thus becoming a target for exploitation) and as processing power continues to increase.

Here are the WLAN encryption methods we'll review today:

* Wired Equivalent Privacy (WEP)
* Wi-Fi Protected Access (WPA)
* Wi-Fi Protected Access 2 (WPA2)

The first widely used standard for wireless LANs was 802.11 (prime); this included the **Wired Equivalent Privacy (WEP)** algorithm which was used for security. WEP utilizes RC4 for encryption and has been depreciated because of vulnerabilities that can be used to find the security keys.

In response to the vulnerabilities found in WEP,**Wi-Fi Protected Access (WPA)** was defined. WPA utilizes the Temporal Key Integrity Protocol (TKIP) which utilizes dynamic keys that were not supported with WEP and RC4 for encryption. The TKIP method used with WPA was utilized until vulnerabilities were found in TKIP. These vulnerabilities center on the fact that TKIP uses some of the same mechanisms that WEP does which allow similar attacks.

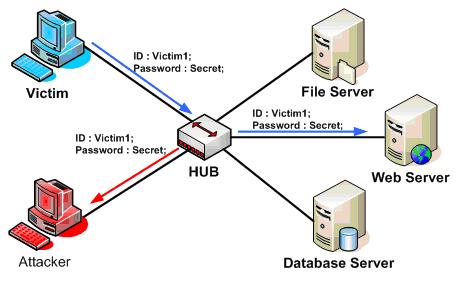
In response to the vulnerabilities in WPA/TKIP, the IEEE 802.11i standard was defined and implemented; the IEEE 802.11i standard is also referred to as WPA2. **WPA2** replaced TKIP with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which is based on Advanced Encryption Standard (AES); it is common for the WPA2 encryption method to be referred to as AES. As of this writing, there are no easy methods that have been found to break AES.

Summary

How secure a wireless LAN is, greatly depends on a number of different configuration parameters that must be entered correctly. The problem with many existing wireless LANs is that the people that are implementing them simply do not have the security knowledge required to maintain a secure wireless network.

All existing and future wireless LAN implementers should make the effort to learn about the most secure methods provided by the chosen equipment (and quite possibly be part of the equipment selection process). The advantage that most modern equipment has is that the WPA2 standard is supported and not that hard to implement.

### What is Eavesdropping?



Eavesdropping is an unauthorized and illegal interception of a private communication. It refers to listening to the private conversions of two or more parties secretly. When an attacker listens to private communication is also referred to sniffing or snooping.

Unexpectedly still major online communications take place in unsecured manner, which allows an attacker to gain access to network traffic by listening or interpreting the travelling information.