



Morse Micro
reaching farther™

Thin LMAC

APPNOTE-20

Copyright © 2024

Table of Contents

1 Scope	3
2 Theory of Operation	4
3 How to Configure	5
Installing Thin LMAC	5
Enabling Thin LMAC	5
Considerations	5
Reduce incidental traffic	5
Reduce keep-alive message frequency	5
Disable IPv6 traffic	6
Use static IP addresses	6
Increase ARP table entry timeout	6
Reduce IPv4 garbage collection frequency	6
Disable unnecessary ARP responses	7
Disable Anti-clogging	7
Other	8
Scaling measures	8
Local IPv4 port range	8
Enable CAC	8
Reduce association retry time	8
4 How to Verify	10
5 Revision History	11

1 Scope

Thin LMAC mode allows a Morse Micro 802.11ah Access Point (AP) to associate with more stations than is possible in the standard SoftMAC mode (which could be called 'Fat LMAC'). The trade-off is that more processing must be performed on the host CPU. No changes are required on the stations; only the AP needs to be set up to use Thin LMAC mode.

The standard SoftMAC mode allows the AP to associate with up to 200 stations. Using Thin LMAC will allow the AP to associate with up to 2,007 stations.

Thin LMAC is supported from Release 1.10.2 onwards (OpenWrt release 2.4.4), but Release 1.14.0 or higher is recommended, because it includes enhancements for reducing the time for a large number of stations to associate.

2 Theory of Operation

Thin LMAC operation is achieved by reducing the per-station memory footprint in the firmware, primarily by moving encryption and decryption of unicast frames from the firmware to the host device.

For that reason, the host device should have a suitable cryptographic processor. Note however, that supporting a large number of simultaneous stations does not intrinsically require more processing power, because it does not impact the total number of packets that can be sent and received per second. In fact, the total achievable throughput will tend to be lower for a large number of stations, due to contention and back-off of over-the-air traffic to/from each station.

3 How to Configure

Installing Thin LMAC

Thin LMAC mode uses a variant of the **mm6108.bin** firmware binary, named **mm6108-tlm.bin**. Make sure this binary image is present in the **/lib/firmware/morse** directory.

mm6108-tlm.bin may be installed already. If not, it must be obtained from Morse Micro and copied into the above location.

Enabling Thin LMAC

 Do not enable Thin LMAC for a device that will be put into Station mode.

Enabling Thin LMAC is documented in the Eval Kit User Guide supplied with the OpenWrt software.

Considerations

Reduce incidental traffic

When deploying a large number of stations, it is important to minimize the amount of incidental traffic. 2,000 stations each sending and receiving a 1kB packet every minute will generate 546 kbps ($2,000 \text{ stations} * 1,024 \text{ bytes} * 2 \text{ directions} * 8 \text{ bits} / 60 \text{ seconds}$) of traffic, or far more in bursts if the traffic is not distributed evenly over time.

Reduce keep-alive message frequency

The default interval for sending a keepalive (empty data) frame to each station is 300 seconds.

Set option “max_inactivity” on the appropriate **wifi-iface**. For example:

```
uci set wireless.default_radio0.max_inactivity=600
```

Disable IPv6 traffic

Using a single network IP protocol (e.g. IPv4) will reduce network traffic, as the devices will not need to negotiate a second time for the additional protocol address. IPv6 also sends regular neighbour discovery packets that are not useful if only IPv4 is required in the network.

Add option `ipv6 '0'` to the config interface `'ahwlan'` section of the `/etc/config/network` file.

MM-IOT-SDK stations

If using the Morse Micro IoT SDK, disable IPv6 with the `LWIP_IPV6=0` build time configuration setting.

Use static IP addresses

If practical, using static IP addresses instead of DHCP will reduce network traffic during association.

Increase ARP table entry timeout

The default ARP entry timeout is 30 (+/-15) seconds. This example increases timeout to 60 (+/-30) minutes. This command requires the Wi-Fi interface to have been brought up, by loading the driver.

```
sysctl -w net.ipv4.neigh.wlan0.base_reachable_time_ms=3600000
```

Reduce IPv4 garbage collection frequency

These settings control the number of entries maintained in the ARP cache. The default values are inadequate for large scale deployments, and will cause ARP entries to constantly be removed, triggering a large number of ARP protocol exchanges between the AP and stations.

gc_thres1: The minimum number of entries to keep in the ARP cache.

gc_thres2: The soft maximum number of entries to keep in the ARP cache. The garbage collector will allow the number of entries to exceed this for a few seconds before collection will be performed.

gc_thres3: The hard maximum number of entries to keep in the ARP cache. The garbage collector will always run if there are more than this number of entries in the cache.

In this example, the above values are set high enough to avoid unnecessary ARP table clean-up for the maximum possible number of stations.

```
sysctl -w net.ipv4.neigh.default.gc_thresh1=2048  
sysctl -w net.ipv4.neigh.default.gc_thresh2=2048  
sysctl -w net.ipv4.neigh.default.gc_thresh3=2048
```

Disable unnecessary ARP responses

These settings minimize responses to ARP requests for IP addresses that are not on the HaLow interface's subnet. They may need adjusting for a given application. Refer to <https://www.kernel.org/doc/Documentation/networking/ip-sysctl.txt> for more information.

```
sysctl -w net.ipv4.conf.all.arp_ignore=1  
sysctl -w net.ipv4.conf.all.arp_announce=2
```

Disable Anti-clogging

Anti-clogging is a hostapd/wpa_supplicant feature that provides minimal protection against DoS by spoofing authentication management frames. When the number of simultaneous association requests exceeds a threshold, hostapd rejects authentication requests and provides a token to the stations. The station must then restart the authentication exchange, supplying the token. This results in at least two extra authentication frames per association, which are significantly larger.

The mechanism provides only superficial DoS support, because it is easily circumvented (by responding to the token requests, but can be detrimental in a large HaLow network. It can be effectively disabled by setting a high threshold in the AP's **hostapd.conf** file. E.g.

```
anti_clogging_threshold=10000
```

CAC (see below) can reduce the number of simultaneous association requests, but must be configured aggressively to completely prevent anti-clogging measures from being triggered.

Other

Check for any other application-generated traffic and consider whether it can be disabled or sent less frequently.

Scaling measures

Local IPv4 port range

The default number of allocated local UDP/TCP ports on the Linux host may not be adequate to handle a high number of simultaneous associations. The range of usable ports can be increased as follows.

```
sysctl -w net.ipv4.ip_local_port_range="32768 65535"
```

Enable CAC

Centralised Authentication Control can reduce the time taken for a large number of stations to associate, by throttling the number of stations that attempt to associate simultaneously, and thereby minimizing contention of time-sensitive association and authentication frame exchanges.

 CAC is described in *MM APPNOTE-24 CAC*.

Reduce association retry time

In very large deployments, or in those with limited bandwidth or duty cycle, some stations may require repeated attempts to associate due to congestion causing timeout of time-sensitive association and authentication frame exchanges.

By default, **wpa_supplicant_s1g** waits for progressively longer intervals between association failures with the same BSS before retrying. The default intervals are 10, 20, 30, 60, 90, and up to 300 seconds for each successive association attempt. These values may be appropriate in more general environments, for example, to avoid thrashing when there is a password mismatch between AP and stations, but can cause significant delays in bringing up a large scale HaLow network.

The following example adds a **backoffs** parameter to **wpa_supplicant_s1g.conf** on the stations, to reduce the backoff interval to a maximum of 32 seconds (plus a random fuzz factor) for the first 12 association attempts. The maximum value of 300 seconds is applied thereafter. These numbers are a tradeoff between having some stations take a

very long time to associate and introducing more congestion because of many stations continually attempting to associate at the same time.

```
...  
network={  
    ssid=<SSID>  
    ...  
    backoffs=8 8 8 16 16 16 24 24 24 32 32 32  
}
```

Because of the large number of variants in any given environment, it's not possible to provide general recommendations regarding the best configuration to use, but the above settings may be helpful if stations are observed to take too long to associate.

4 How to Verify

When Thin LMAC mode has been enabled, more than 200 stations will be able to associate to the device.

Confirm the device is in Thin LMAC mode by using the following command. A value of 1 indicates that Thin LMAC is enabled.

```
# cat /sys/module/morse/parameters/thin_lmac  
1
```

The following message will be logged when the **morse.ko** driver loads if INFO level debugging has been enabled.

```
morse_mac_init: Enabling thin LMAC mode
```

If the firmware is attached to a UART console, the following messages can also be seen during start-up when Thin LMAC is enabled.

```
# cat /var/log/ttyAMA1.log  
Booting from MM6108A1 chip master-2f903a9b0d-NFP 0x56624f24 2024-10-29  
09:38  
Thin LMAC mode
```

5 Revision History

Release Number	Release Date	Release Notes
01	2024-04-19	Initial version
02		Updates
03	2024-11-28	Rework and update for release 1.14.0



Morse Micro Pty. Ltd. Corporate Headquarters

Level 8, 10-14 Waterloo Street, Surry Hills, NSW 2010,
AUSTRALIA

Morse Micro Inc. – USA

40 Waterworks Way
Irvine, CA 92618, UNITED STATES

Morse Micro – China

Floor 7, Room 08-210, Wework office 292 Yan'an Rd,
Shangcheng District, Hangzhou 310003

USA: +1.949.501.7080

Australia: +61.02.905.45922

China: +86.571.229.30277

Email: sales@morsemicro.com

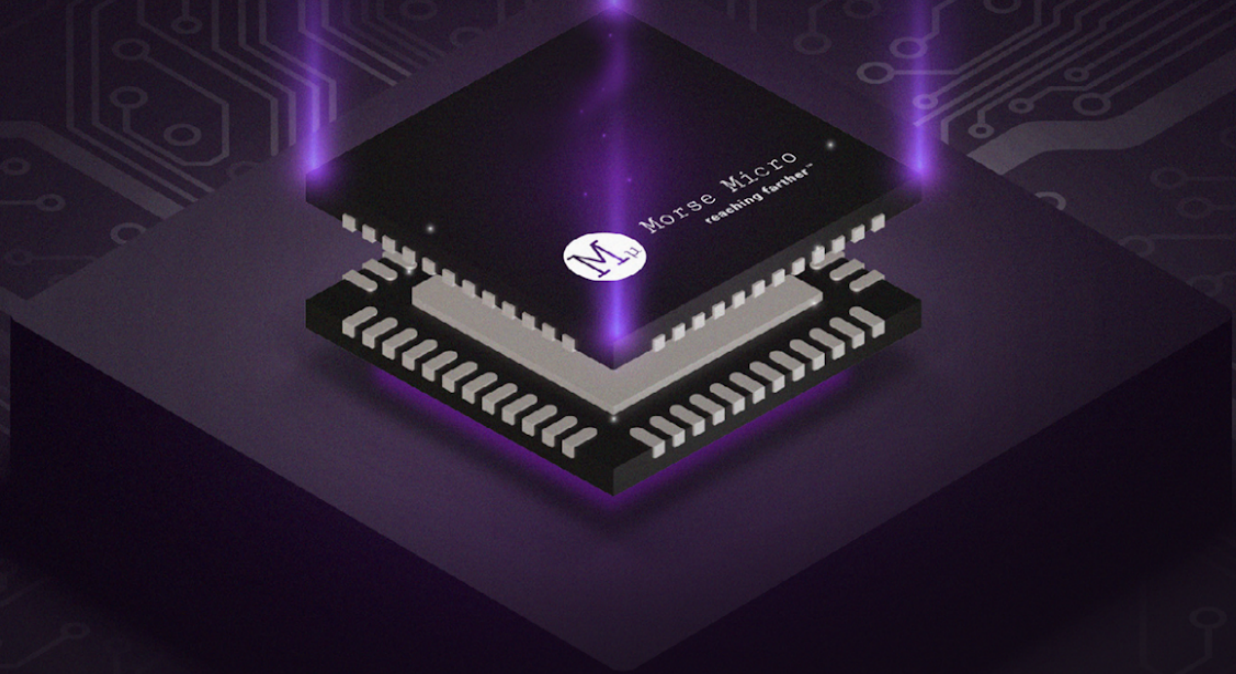
www.morsemicro.com

© 2023 Morse Micro Pty. Ltd.

All rights reserved. Morse Micro and the Morse Micro logo are trademarks of Morse Micro Ltd. All other trademarks and service marks are the property of their respective owners.

About Morse Micro

Morse Micro is producing IEEE 802.11ah / Wi-Fi HaLow solutions for Internet of Things (IoT) - based on a newly certified Wi-Fi standard called HaLow. Morse Micro is a VC-backed Startup headquartered in Sydney, Australia. Learn more at www.morsemicro.com



Morse Micro
reaching farther™