Microchip/ZeroG SDK Errata

Microchip TCP/IP Stack v5.00 and ZeroG Driver 1.4.0

1. Release:

Microchip SDK Version	TCP/IP Stack v5.00
MCUs	PIC18, PIC24, dsPIC, PIC32
Target Boards	PICDEM.net 2, Explorer 16
ZeroG Driver Version	1.4.0
Date	04/27/2009

2. Errata

2.1 No CLI command to define the Listen Interval when ZeroG goes into Sleep Mode (PS-Poll)

The sleep interval is currently a constant value, 4. If the access point's Beacon interval is 100 ms, ZeroG device would wake up every 400 ms to check for unicast frames which may have been buffered by the access point.

Work-around: None.

Disposition: Will be new CLI command Driver v1.6.0 (next full release).

2.2 Not able to handle fragmented frames sent from the access point

Fragmentation Threshold is a configurable parameter on the access point. The default setting is usually 2346 bytes. The range is usually from 256 to 2346 bytes. It specifies the maximum packet size for access point transmission to any station. Packets bigger than the fragmentation threshold are fragmented into multiple packets, and are reassembled by the receiving stations.

This fragmentation and reassembly process is handled at the 802.11 layer, and is independent of other possible fragmentation/reassembly processes performed at higher layers.

Work-around: set access point's fragmentation threshold to 2346-byte.

Disposition: TBD

2.3 Stations may connect while security settings differ on both ends

Once a key type (WEP, WPA) and key is installed onto the ZeroG chip, a secure connection of that type may occur to a supporting access point even if a different key type is programmed.

Work-around: Ensure a hard reset prior to changing security modes.

Disposition: TBD.

2.4 Stations may connect while security settings differ on both ends

ZeroG may connect to an access point with no security setting even though the station is configured with a security setting.

Stations also may also connect in an Adhoc network even though they have different security settings.

Work-around: make sure all nodes are configured with the same security setting.

Disposition: TBD.

2.5 Low TCP throughput in Adhoc mode

You may experience low TCP throughput when connecting ZeroG devices in Adhoc mode. This issue is being investigated by ZeroG.

Work-around: none.

Disposition: TBD.

2.6 Invalid CLI commands may hang the system

Invalid CLI commands, such as “kill”, may cause the system to hang. A hard reset is needed to recover.

Work-around: Do not use invalid CLI commands.

Disposition: TBD

2.7 Iperf client session connecting to the local node causes a system hang

The “-c” option of iperf specifies which remote iperf server to connect to. If you specify the local station as the “remote” iperf server, the system would hang. This is a not-supported procedure.

Work-around: do not perform loop-back testing with iperf.

Disposition: No plan to support.

2.8 Power-save mode displayed as “enabled” in adhoc mode

The CLI command *iwconfig* displays “pwrsave” and “dtim” status. This status has no meaning when the station is in adhoc mode.

Work-around: not needed.

Disposition: No change planned.

2.9 Station does not connect to an access point with hidden SSID

An access point may be configured to not to broadcast its SSID. ZeroG device has problems connecting to some access points configured with this setting. ZeroG is investigating this issue.

Work-around: always enable “wireless SSID broadcast” at the access point.

Disposition: TBD.

2.10 DHCP server may send offers at higher than 2 Mbps data rate

Some access points may have built-in DHCP servers that send DHCP OFFER messages at 5.5 Mbps or higher data rates. ZeroG device can only transmit and receive at either 1 or 2 Mbps. DHCP OFFER transmitted at higher data rates can not be received by ZeroG device. When this happens, a station may get connected to the access point, but fails to acquire a dynamic IP.

Work-around: force the access point to transmit all packets at 1 or 2 Mbps data rate.

Disposition: Fix in DHCP code TBD.