

RoHS Compliant

Protection Zone Application Note

January 20, 2009



Apacer Technology Inc.

9/F, No. 100, Hsin Tai Wu Rd., Hsichih, Taipei Hsien 221, Taiwan

Tel: +886-2-2696-1666 Fax: +886-2-2696-1668

www.apacer.com

Revision History

Revision	Date	Description	Remark
0.1	05/20/2008	Preliminary	
1.0	01/14/2009	Official release	
1.1	01/20/2009	Updated illustrations	

Protection Zone

Introduction

This application note describes in-application user level of protection zone, and it outlines how to configure and how to use this feature on the device. A device can be configured into zones, and each zone is designated by a starting and ending logical sector number. Therefore, within several easy steps, different protection level to different zones can be assigned and protection mechanism can be activated.

Overview

A device can have 3 different types of Zones: Restricted, Read-Only, and Unprotected, and when the product is shipped out of Apacer, all sectors are in Unprotected Zone. A maximum of 4 zones can be configured as either Restricted or Read-Only Zone, which means up to 4 protection zones can be presented concurrently. More than 4 is not allowed and the command will not be executed and will be flagged as command error (refer to Figure 3). The address space outside these 4 zones is automatically in Unprotected Zone (refer to Figure 4). After the zone has been configured, the protection zone can be de-activated or re-activated by either software methods or hardware components. Protection zone configuration is non-volatile and it will be in effect until the next set of configuration overwrites it. A Protection Zone has a starting pointer and an ending pointer. The starting pointer and the ending pointer must be within 0 to N-1, and the starting pointer must be smaller than the ending pointer. No overlapping is allowed between zones (refer to Figure 5). Otherwise, the configuration command will be flagged as a command error.

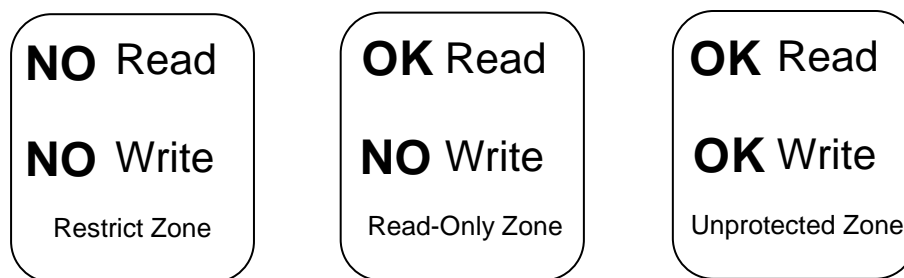


Figure 1 Typical access privilege of users to a protection zone enabled device

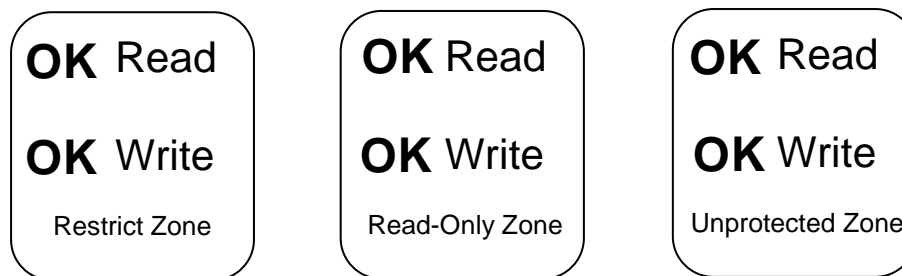


Figure 2 Typical access privilege of users to a protection zone disabled device

Protection zone setup process

1. Create partition

The scheme to create partition varies from partition tools such as FDISK, SPFDISK, DISKEDIT, and etc; nevertheless, all of them fit the same essentiality.

2. Set password

When configuring a brand new device shipped out of Apacer, for the sake of security, setting a new password for the device is necessary. To set the password, the location where the device attaches to and a desired password are required. To change the password, other than the location where the device attaches to, the old password must be provided; otherwise, the password won't be changed.

3. Set protection zone configuration

There are several items to be aware of before engaged in this command. Activation method:

Zone number:

Defines number of zones to be configured as well as indicates how many protect zone data structures are valid. A "0" indicates the whole device will be configured as unprotected zone.

Starting & Ending LBA:

The zone starting point and the zone ending point in 28-bit LBA. Both starting LBA sector and ending LBA sector are included in the protection zone. Starting LBA and ending LBA must not be equal, and starting LBA must be smaller than ending LBA, which be illustrated as the

relationship below.

$$\begin{aligned}
 &0 \leq \text{StartingLBA}[0] < \text{EndingLBA}[0] \\
 &< \text{StartingLBA}[1] < \text{EndingLBA}[1] \\
 &\dots\dots\dots \\
 &< \text{StartingLBA}[\text{ZoneNumbers}] < \text{EndingLBA}[\text{ZoneNumbers}] \leq N
 \end{aligned}$$

where N = total sectors

Protect Level:

Defines whether the protection zone is read-only, restricted with read command rejected, or restricted with read command returns all "0".

4. Activate protection zone

This is the last step to make the protection zone configuration in effective. To activate the protection zone, the location where the device attaches to and the password are required, which is also the prerequisite to retrieve configuration information and to de-activate the protection zone.

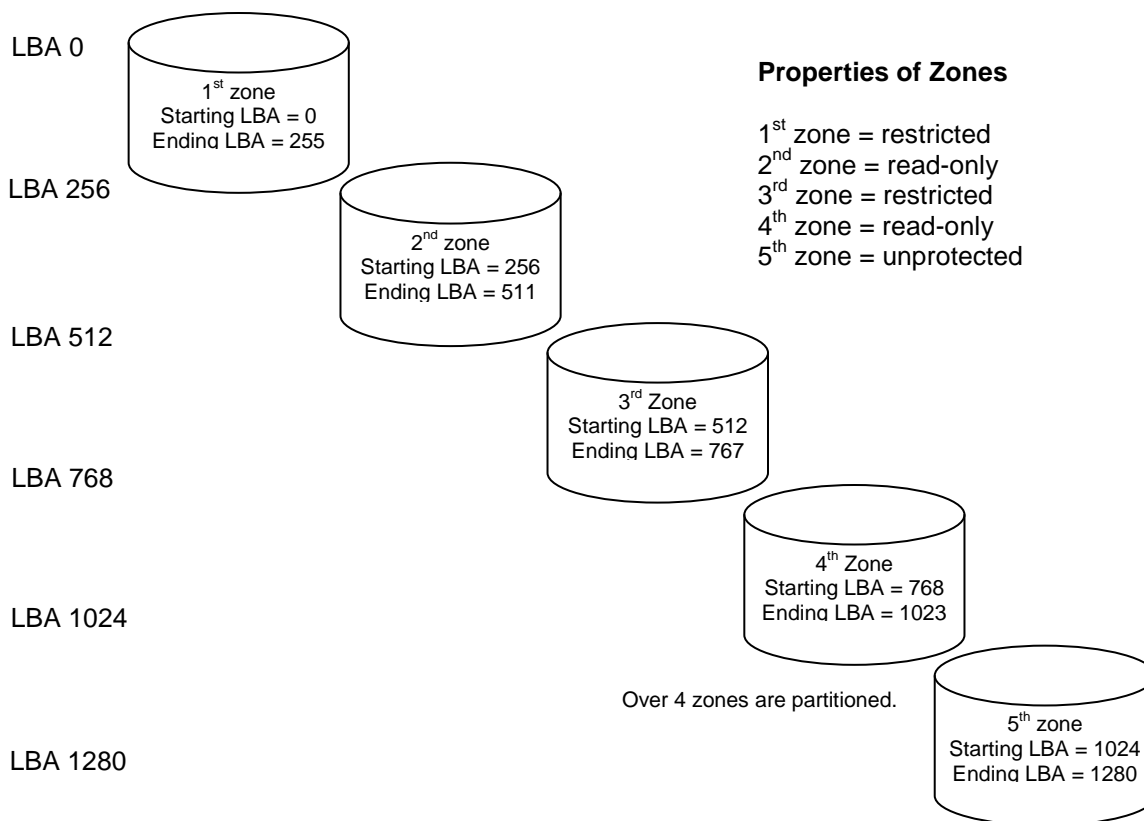


Figure 3 Typical illegal partitioned protection zoned device

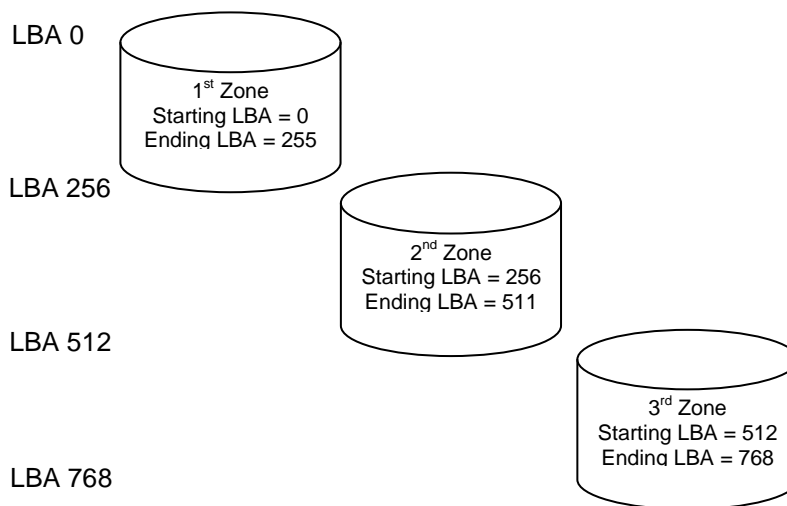


Figure 4 Typical legitimate protection zoned device

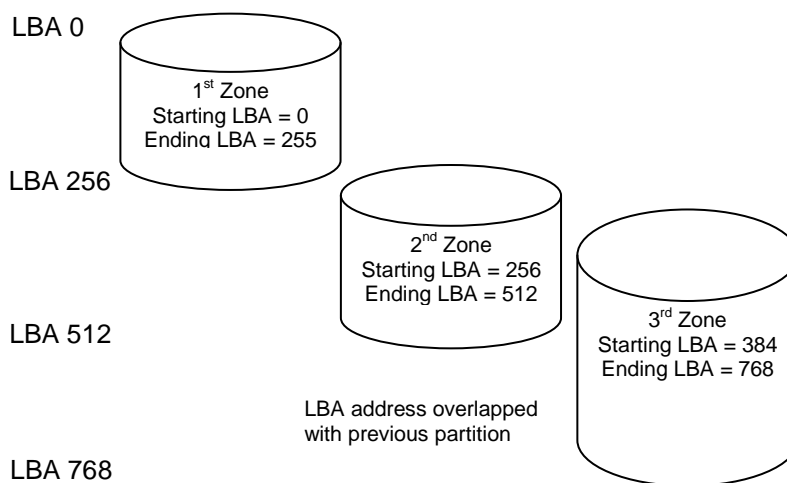


Figure 5 Typical illegal LBA address overlapped protection zoned device

Conclusion

Applying protection zones on the device will definitely elevate the level of securing information on the device. It takes some schemes to work out the configuration, but it pays to prevent from mishaps.

Apacer Technology Inc.

9/F, No. 100, Hsin Tai Wu Rd.
Hsichih, Taipei County 221, Taiwan
Tel: +886-2-2696-1666 Fax: +886-2-2696-1668
www.apacer.com

Copyright © 2009 Apacer Technology Inc. All Rights Reserved.
Information in this document is subject to change without prior notice.
Apacer and the Apacer logo are trademarks or registered trademarks of Apacer Technology Inc.
Other brands, names, trademarks or registered trademarks may be claimed as the property of their
respective owners.