0.1 Asynchronous receive

Sunrise uses both channel program and physical DMA to handle inbound packets.
Upon receiving an inbound packet targeted to Sunrise, Sunrise uses internal decoder to decode if the packet should be handled using channel program or physical DMA according to the following categories:

1. Inbound write request packets that their destination address is in the first 4Gbytes (when using full physical DMA) or pass the security check (when using security table mechanism) are handled using physical DMA (if the physical DMA mechanism for inbound write request is enabled).
2. Inbound read request packets that pass the security table check (when using this mechanism) or their destination address is in the first 4Gbytes (when using full physical DMA) are handled using physical DMA (if the physical DMA mechanism for inbound read request is enabled).
3. Inbound read response packets (for read requests initiated by Sunrise) are handled using physical DMA (if the physical DMA mechanism for inbound read response is enabled).
4. All inbound packets for which there is no Physical DMA are handled using the channel program and directed to the GRU.

If due to some error the GRU sets its dead bit, Sunrise answers with “Busy” acknowledge to all asynchronous inbound packets, no matter whether they should be handled by the GRU or by physical DMA. Asynchronous packets that resides in the GRF (general receive FIFO) are discarded upon such event.

Sunrise writes status information for a packet upon handling completion. If the packet was handled using channel program, status is written to the relevant descriptor field in the GRU channel program. Status for a packet which was handled using physical DMA is written to the PRU conditionally according to rules described in “Physical receive unit (PRU)” on page 11. Status is written to the PRU together with the inbound packet header.

In order to improve system performance, Physical DMA units should be used.

If the PRU is disabled (after a STOP command), all the physical DMA units are disabled. All inbound packets are directed to the GRU.

0.1.1 Security levels for asynchronous transfers

Sunrise implements three levels of security for physical DMA. Security level can range from full security to almost no security. Security levels are used only for handling inbound packets using physical DMA. Packets that are handled using physical DMA can have one of the following types: inbound read request, non broadcast inbound write requests and inbound read response. all other types of inbound packets are handled by the GRU. Since there is a trade off between security and performance, Software is responsible to choose between those levels according to system needs and knowledge.

Security levels are:

1. Full security (no physical DMA) - In this mode all the inbound packets are directed to an intermediate buffer (using the GRU) and software is responsible to handle them. In order to use this mode software should disable all physical DMA units. Use of this mode may result in lack of performance since the CPU is forced to handle every inbound packet.
2. Security table - In this mode a security table is generated and handled by software. The security table resides in system memory. Security table entry format is described in "Security table mechanism" on page 2. Sunrise accesses the table using part of the destination offset as an index. Only destination offsets in the first 4Gbytes of the memory space are checked (other packets are directed immediately to the GRU). If the security check fails, the packet is directed to the GRU and is handled, later, by software. Only packets that pass the security check are handled by Sunrise using physical DMA. To use this mode, software should generate the security table and inform Sunrise about its location in memory (by updating the Security_Table_Ptr register), enable the security window mechanism by setting the Security_table_en bit in the global control register and enable the required physical DMA unit (or units).
3. Full physical DMA - In this mode every enabled physical DMA unit can read or write from the first 4Gbytes of the memory space and no security check is done. Packets that do not reside in the first 4Gbytes are directed to intermediate buffer (by the GRU) and handled by software. To use this mode software should enable the needed physical DMA unit (or units) and clear the Security_table_en bit in the global control register. The destination address in system memory is simply the lower 32 bits of the destination offset fields.

0.1.1.1 Security table mechanism

This clause describes the security table format and Sunrise operation scheme concerning security table mechanism. Sunrise includes a pointer to the table start address in the Security_Table_Ptr register. This pointer should be initialized by software.

0.1.1.2 Security table structure

Security table resides in continues buffer in system memory space. The table start address should be 4Kbytes aligned (page aligned). The number of entries may vary from 512 entries to 8K entries. Each entry is two quadlet wide. Entry format is described in Figure 1 on page 3 and Table 1 on page 3 describes the various fields.

FIGURE 1. Security table entry format

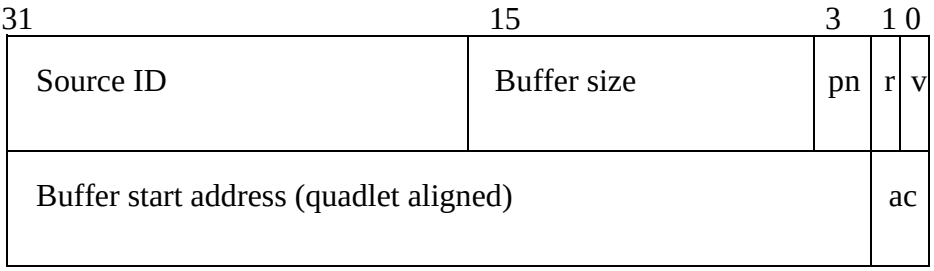


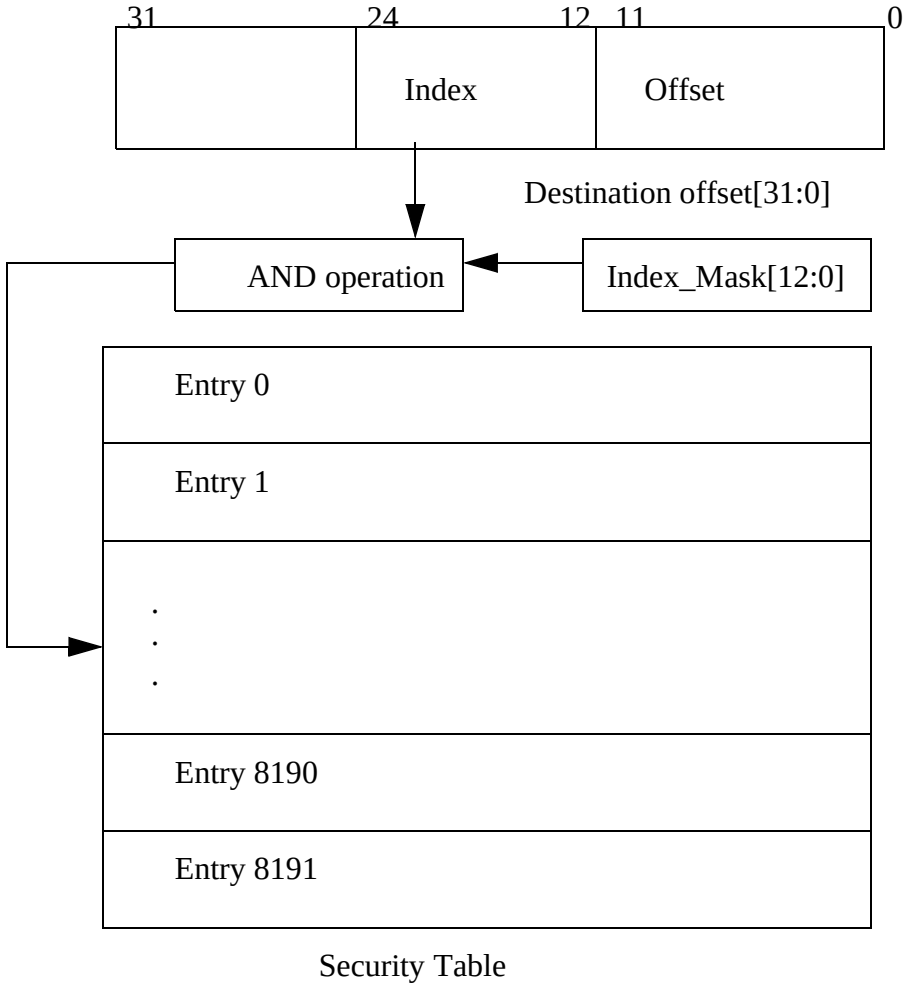
TABLE 1. Security table entry field description

Wide (in bits)	Field name	Description
16	Source ID	Node ID that is allowed to access the data buffer. Value of the bus ID should be equal to Sunrise bus ID. Value of 3Fh in the physical ID indicates that each local node has access permission.
12	Buffer size	Buffer size (in bytes). Allowed values are 0-2048.
2	post notification (pn)	This field indicates Sunrise whether it should update status upon transaction completion. 00b - No status update is needed 01b - Updated status only if the transaction was a read transaction. 10b - Update status only if the transaction was a write transaction. 11b - Update status upon transaction completion.
1	reserved bit (r)	
1	Valid bit (v)	Valid bit for the entry.
30	Buffer start address	Buffer start address (quadlet aligned).
2	Access field (ac)	Access type field. 01b - Read only. 10b - Write only 11b - Read and Write. 00b - Reserved.

0.1.1.3 Accessing the table

Since the table includes 512 to 8K entries, 9-13 bits of index are needed in order to access the security table. Sunrise uses for this purpose 13 bits of the destination offset bits. The lower 12 bits (bits 0 to 11) are used by Sunrise to indicate offset in the buffer and bits 12 to 24 of the destination offset are used as an index to table. Since table may contain less than 8K entries (multiple of 2), mask register is used to indicate the exact number of bits to be used. Figure 2 on page 4 shows the table access mechanism.

FIGURE 2. Access to the security table. (table size is 8K entries)



0.1.1.4 Sunrise operation scheme using the security table.

Sunrise operation scheme using the security table is described in Figure 3.
The security check, performed by Sunrise, consists of the following checks:

1. The entry node ID should be equal to packets Source node ID (with the exception of 3F that indicates that every local node may access this buffer)
2. The packet offset field (destination offset [12:0]) plus packet size should not exceed the buffer size field of the entry.
3. The entry includes valid access type for the relevant packet. E.g for read request packet read access is needed.
4. Valid bit in the entry should be enabled (‘1’).

Only if all of the described checks pass, Sunrise will perform physical DMA. Otherwise the packet is directed to the GRU.

If security check passes, physical address is generated by Sunrise. Sunrise adds destination offset bits 0 to 11 (offset) to buffer start address. The received sum is used as physical start address for the packet.

FIGURE 3. Sunrise operation scheme using the security table.