ICH_HCR_EL2, Interrupt Controller Hyp Control Register

The ICH_HCR_EL2 characteristics are:

Purpose

Controls the environment for VMs.

Configuration

AArch64 System register ICH_HCR_EL2 bits [31:0] are architecturally mapped to AArch32 System register ICH_HCR[31:0].

This register is present only when FEAT_GICv3 is implemented and (EL2 is implemented or EL3 is implemented). Otherwise, direct accesses to ICH_HCR_EL2 are undefined.

If EL2 is not implemented, this register is res0 from EL3.

This register has no effect if EL2 is not enabled in the current Security state.

Attributes

ICH_HCR_EL2 is a 64-bit register.

Field descriptions

63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38
RES0																									
EOIcount																RES0									

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6
RES0																DVIM	TDIR	TSEI	TALL1	TALL0	TC	RES0		vSGIEOICount		VGrp1DIE	VGrp1E

Bits [63:32]

Reserved, res0.

EOIcount, bits [31:27]

This field is incremented whenever a successful write to a virtual EOIR or DIR register would have resulted in a virtual interrupt deactivation. That is either:

- A virtual write to EOIR with a valid interrupt identifier that is not in the LPI range (that is < 8192) when EOI mode is zero and no List Register was found.
- A virtual write to DIR with a valid interrupt identifier that is not in the LPI range (that is < 8192) when EOI mode is one and no List Register was found.

This allows software to manage more active interrupts than there are implemented List Registers.

It is constrained unpredictable whether a virtual write to EOIR that does not clear a bit in the Active Priorities registers (ICH_AP0R<n>_EL2/ICH_AP1R<n>_EL2) increments EOIcount. Permitted behaviors are:

- Increment EOIcount.
- Leave EOIcount unchanged.

The reset behavior of this field is:

- On a Warm reset, this field resets to `0`.

Bits [26:16]

Reserved, res0.

DVIM, bit [15]
When ICH_VTR_EL2.DVIM == 1:

Directly-injected Virtual Interrupt Mask.

DVIM	Meaning
`0b0`	This control has no effect on the signalling of virtual interrupts.
`0b1`	Virtual interrupts received via direct-injection are not presented to the virtual CPU interface and not considered when determining the highest priority pending virtual interrupt.

The reset behavior of this field is:

- On a Warm reset, this field resets to `0`.

Otherwise:

Reserved, res0.

TDIR, bit [14]
When FEAT_GICv3_TDIR is implemented:

Trap EL1 writes to ICC_DIR_EL1 and ICV_DIR_EL1.

TDIR	Meaning
0b0	EL1 writes of ICC_DIR_EL1 and ICV_DIR_EL1 are not trapped to EL2, unless trapped by other mechanisms.
0b1	EL1 writes of ICV_DIR_EL1 are trapped to EL2. It is implementation defined whether writes of ICC_DIR_EL1 are trapped. Not trapping ICC_DIR_EL1 writes is DEPRECATED.

Arm deprecates not including this trap bit.

The reset behavior of this field is:

- On a Warm reset, this field resets to 0.

Otherwise:

Reserved, res0.

TSEI, bit [13]

Trap all locally generated SEIs. This bit allows the hypervisor to intercept locally generated SEIs that would otherwise be taken at EL1.

TSEI	Meaning
0b0	Locally generated SEIs do not cause a trap to EL2.
0b1	Locally generated SEIs trap to EL2.

If ICH_VTR_EL2.SEIS is 0, this bit is res0.

The reset behavior of this field is:

- On a Warm reset, this field resets to 0.

TALL1, bit [12]

Trap all EL1 accesses to ICC_* and ICV_* System registers for Group 1 interrupts to EL2.

TALL1	Meaning
0b0	EL1 accesses to ICC_* and ICV_* registers for Group 1 interrupts proceed as normal.
0b1	EL1 accesses to ICC_* and ICV_* registers for Group 1 interrupts trap to EL2.

The reset behavior of this field is:

- On a Warm reset, this field resets to 0.

TALL0, bit [11]

Trap all EL1 accesses to ICC_* and ICV_* System registers for Group 0 interrupts to EL2.

TALL0	Meaning
0b0	EL1 accesses to ICC_* and ICV_* registers for Group 0 interrupts proceed as normal.
0b1	EL1 accesses to ICC_* and ICV_* registers for Group 0 interrupts trap to EL2.

The reset behavior of this field is:

- On a Warm reset, this field resets to 0.

TC, bit [10]

Trap all EL1 accesses to System registers that are common to Group 0 and Group 1 to EL2.

TC	Meaning
0b0	EL1 accesses to common registers proceed as normal.
0b1	EL1 accesses to common registers trap to EL2.

This affects accesses to ICC_SGI0R_EL1, ICC_SGI1R_EL1, ICC_ASGI1R_EL1, ICC_CTLR_EL1, ICC_DIR_EL1, ICC_PMR_EL1, ICC_RPR_EL1, ICV_CTLR_EL1, ICV_DIR_EL1, ICV_PMR_EL1, and ICV_RPR_EL1.

The reset behavior of this field is:

- On a Warm reset, this field resets to `0`.

Bit [9]

Reserved, res0.

vSGIEOICount, bit [8]
When FEAT_GICv4p1 is implemented:

Controls whether deactivation of virtual SGIs can increment ICH_HCR_EL2.EOIcount

vSGIEOICount	Meaning
`0b0`	Deactivation of virtual SGIs can increment ICH_HCR_EL2.EOIcount.
`0b1`	Deactivation of virtual SGIs does not increment ICH_HCR_EL2.EOIcount.

The reset behavior of this field is:

- On a Warm reset, this field resets to `0`.

Otherwise:

Reserved, res0.

VGrp1DIE, bit [7]

VM Group 1 Disabled Interrupt Enable. Enables the signaling of a maintenance interrupt while signaling of Group 1 interrupts from the virtual CPU interface to the connected vPE is disabled:

VGrp1DIE	Meaning
`0b0`	Maintenance interrupt disabled.
`0b1`	Maintenance interrupt signaled when ICH_VMCR_EL2.VENG1 is 0.

The reset behavior of this field is:

- On a Warm reset, this field resets to `0`.

VGrp1EIE, bit [6]

VM Group 1 Enabled Interrupt Enable. Enables the signaling of a maintenance interrupt while signaling of Group 1 interrupts from the virtual CPU interface to the connected vPE is enabled:

VGrp1EIE	Meaning
0b0	Maintenance interrupt disabled.
0b1	Maintenance interrupt signaled when ICH_VMCR_EL2.VENG1 is 1.

The reset behavior of this field is:

- On a Warm reset, this field resets to 0.

VGrp0DIE, bit [5]

VM Group 0 Disabled Interrupt Enable. Enables the signaling of a maintenance interrupt while signaling of Group 0 interrupts from the virtual CPU interface to the connected vPE is disabled:

VGrp0DIE	Meaning
0b0	Maintenance interrupt disabled.
0b1	Maintenance interrupt signaled when ICH_VMCR_EL2.VENG0 is 0.

The reset behavior of this field is:

- On a Warm reset, this field resets to 0.

VGrp0EIE, bit [4]

VM Group 0 Enabled Interrupt Enable. Enables the signaling of a maintenance interrupt while signaling of Group 0 interrupts from the virtual CPU interface to the connected vPE is enabled:

VGrp0EIE	Meaning
0b0	Maintenance interrupt disabled.
0b1	Maintenance interrupt signaled when ICH_VMCR_EL2.VENG0 is 1.

The reset behavior of this field is:

- On a Warm reset, this field resets to 0.

NPIE, bit [3]

No Pending Interrupt Enable. Enables the signaling of a maintenance interrupt when there are no List registers with the State field set to `0b01` (pending):

NPIE	Meaning
`0b0`	Maintenance interrupt disabled.
`0b1`	Maintenance interrupt signaled while the List registers contain no interrupts in the pending state.

The reset behavior of this field is:

- On a Warm reset, this field resets to `0`.

LRENPIE, bit [2]

List Register Entry Not Present Interrupt Enable. Enables the signaling of a maintenance interrupt while the virtual CPU interface does not have a corresponding valid List register entry for an EOI request:

LRENPIE	Meaning
`0b0`	Maintenance interrupt disabled.
`0b1`	Maintenance interrupt is asserted while the EOIcount field is not 0.

The reset behavior of this field is:

- On a Warm reset, this field resets to `0`.

UIE, bit [1]

Underflow Interrupt Enable. Enables the signaling of a maintenance interrupt when the List registers are empty, or hold only one valid entry:

UIE	Meaning
`0b0`	Maintenance interrupt disabled.
`0b1`	Maintenance interrupt is asserted if none, or only one, of the List register entries is marked as a valid interrupt.

The reset behavior of this field is:

- On a Warm reset, this field resets to `0`.

En, bit [0]

Enable. Global enable bit for the virtual CPU interface:

En	Meaning
0b0	Virtual CPU interface operation disabled.
0b1	Virtual CPU interface operation enabled.

When this field is set to 0:

- The virtual CPU interface does not signal any maintenance interrupts.
- The virtual CPU interface does not signal any virtual interrupts.
- A read of ICV_IAR0_EL1, ICV_IAR1_EL1, GICV_IAR or GICV_AIAR returns a spurious interrupt ID.

Note

This field is res0 when SCR_EL3.{NS,EEL2}=={0,0}

The reset behavior of this field is:

- On a Warm reset, this field resets to 0.

Accessing ICH_HCR_EL2

Accesses to this register use the following encodings in the System register encoding space:

MRS <Xt>, ICH_HCR_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1011	0b000

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.<NV2,NV> == '11' then
        X[t, 64] = NVMem[0x4C0];
    elsif EL2Enabled() && HCR_EL2.NV == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    if ICC_SRE_EL2.SRE == '0' then
```

```
            AArch64.SystemAccessTrap(EL2, 0x18);
        else
            X[t, 64] = ICH_HCR_EL2;
    elsif PSTATE.EL == EL3 then
        if ICC_SRE_EL3.SRE == '0' then
            AArch64.SystemAccessTrap(EL3, 0x18);
        else
            X[t, 64] = ICH_HCR_EL2;
```

MSR ICH_HCR_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b1100	0b1011	0b000

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.<NV2,NV> == '11' then
        NVMem[0x4C0] = X[t, 64];
    elsif EL2Enabled() && HCR_EL2.NV == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    if ICC_SRE_EL2.SRE == '0' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        ICH_HCR_EL2 = X[t, 64];
elsif PSTATE.EL == EL3 then
    if ICC_SRE_EL3.SRE == '0' then
        AArch64.SystemAccessTrap(EL3, 0x18);
    else
        ICH_HCR_EL2 = X[t, 64];
```


28/03/2023 16:01; 72747e43966d6b97dcbd230a1b3f0421d1ea3d94