VTTBR_EL2, Virtualization Translation Table Base Register

The VTTBR_EL2 characteristics are:

Purpose

Holds the base address of the translation table for the initial lookup for stage 2 of an address translation in the EL1&0 translation regime, and other information for this translation regime.

Configuration

AArch64 System register VTTBR_EL2 bits [63:0] are architecturally mapped to AArch32 System register VTTBR[63:0].

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.

VTTBR_EL2 is a 128-bit register that can also be accessed as a 64-bit value. If it is accessed as a 64-bit register, accesses read and write bits [63:0] and do not modify bits [127:64].

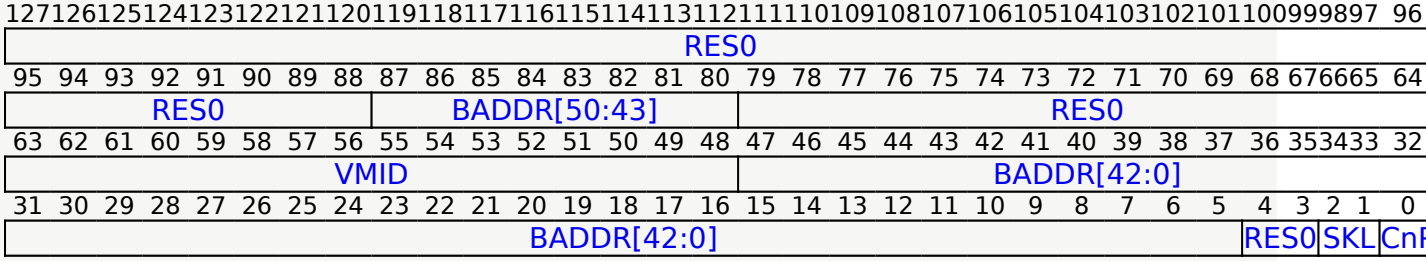
Attributes

VTTBR_EL2 is a:

- 128-bit register when FEAT_D128 is implemented and VTCR_EL2.D128 == 1
- 64-bit register when FEAT_D128 is not implemented or VTCR_EL2.D128 == 0

Field descriptions

When FEAT_D128 is implemented and VTCR_EL2.D128 == 1:



Bits [127:88]

Reserved, res0.

BADDR, bits [87:80, 47:5]

Translation table base address:

- Bits A[55:x] of the stage 2 translation table base address bits are in register bits[87:80, 47:x].
- Bits A[(x-1):0] of the stage 2 translation table base address are zero.

Address bit x is the minimum address bit required to align the translation table to the size of the table. x is calculated based on LOG2(StartTableSize), as described in VMSAv9-128. The smallest permitted value of x is 5.

The BADDR field is split as follows:

- BADDR[50:43] is VTTBR_EL2[87:80].
- BADDR[42:0] is VTTBR_EL2[47:5].

The reset behavior of this field is:

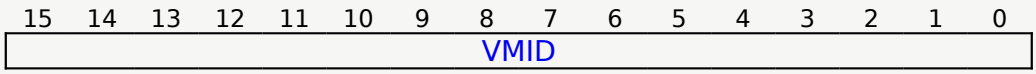
- On a Warm reset, this field resets to an architecturally unknown value.

Bits [79:64]

Reserved, res0.

VMID, bits [63:48]

VMID encoding when FEAT_VMID16 is implemented and VTCR_EL2.VS == 1



VMID, bits [15:0]

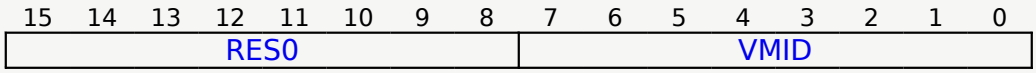
The VMID for the translation table.

If the implementation has an 8-bit VMID, bits [15:8] of this field are res0.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

VMID encoding when FEAT_VMID16 is not implemented or VTCR_EL2.VS == 0



Bits [15:8]

Reserved, res0.

VMID, bits [7:0]

The VMID for the translation table.

The VMID is 8 bits when any of the following are true:

- EL2 is using AArch32.
- VTCR_EL2.VS is 0.
- FEAT_VMID16 is not implemented.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Bits [4:3]

Reserved, res0.

SKL, bits [2:1]

Skip Level. Skip Level determines the number of levels to be skipped from the regular start level of the Non-Secure Stage 2 translation table walk.

SKL	Meaning
0b00	Skip 0 level from the regular start level.
0b01	Skip 1 level from the regular start level.
0b10	Skip 2 levels from the regular start level.
0b11	Skip 3 levels from the regular start level.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

CnP, bit [0]
When FEAT_TTCNP is implemented:

Common not Private. This bit indicates whether each entry that is pointed to by VTTBR_EL2 is a member of a common set that can be used by every PE in the Inner Shareable domain for which the value of VTTBR_EL2.CnP is 1.

CnP	Meaning
0b0	The translation table entries pointed to by VTTBR_EL2 are permitted to differ from the entries for VTTBR_EL2 for other PEs in the Inner Shareable domain. This is not affected by the value of the current VMID.
0b1	The translation table entries pointed to by VTTBR_EL2 are the same as the translation table entries for every other PE in the Inner Shareable domain for which the value of VTTBR_EL2.CnP is 1 and the VMID is the same as the current VMID.

This bit is permitted to be cached in a TLB.

Note

If the value of VTTBR_EL2.CnP bit is 1 on multiple PEs in the same Inner Shareable domain and those VTTBR_EL2s do not point to the same translation table entries when using the current VMID then the results of translations using VTTBR_EL2 are constrained unpredictable, see 'CONSTRAINED UNPREDICTABLE behaviors due to caching of control or data values'.

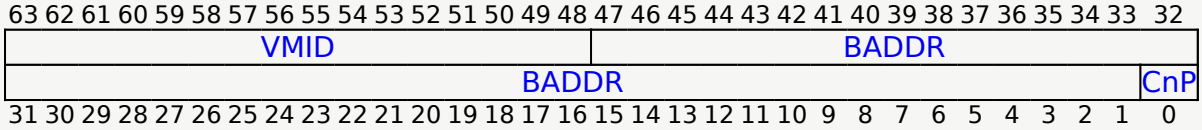
The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

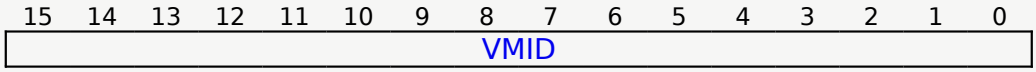
Reserved, res0.

When FEAT_D128 is not implemented or VTCR_EL2.D128 == 0:



VMID, bits [63:48]

VMID encoding when FEAT_VMID16 is implemented and VTCR_EL2.VS == 1



VMID, bits [15:0]

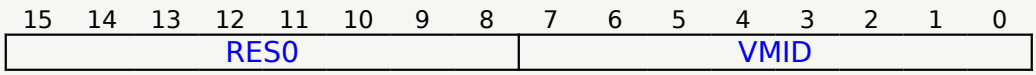
The VMID for the translation table.

If the implementation has an 8-bit VMID, bits [15:8] of this field are res0.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

VMID encoding when FEAT_VMID16 is not implemented or VTCR_EL2.VS == 0



Bits [15:8]

Reserved, res0.

VMID, bits [7:0]

The VMID for the translation table.

The VMID is 8 bits when any of the following are true:

- EL2 is using AArch32.
- VTCR_EL2.VS is 0.
- FEAT_VMID16 is not implemented.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

BADDR, bits [47:1]

Translation table base address, A[47:x] or A[51:x], bits[47:1].

Note

If an OA size of more than 48 bits is in use, and the translation table has fewer than eight entries, the table must be aligned to 64 bytes. Otherwise the translation table must be aligned to the size of the table.

In an implementation that includes FEAT_LPA, if the value of VTCR_EL2.PS is `0b110`, then:

- Register bits[47:z] hold bits[47:z] of the stage 2 translation table base address, where z is determined as follows:
  - If x >= 6 then z=x.
  - Otherwise, z=6.
- Register bits[5:2] hold bits[51:48] of the stage 2 translation table base address.
- When z>x register bits[(z-1):x] are res0, and bits[(z-1):x] of the translation table base address are zero.
- When x>6 register bits[(x-1):6] are res0.
- Register bit[1] is res0.
- Bits[5:2] of the stage 2 translation table base address are zero.
- In an implementation that includes FEAT_TTCNP, bit[0] of the stage 2 translation table base address is zero.

Note

When the value of ID_AA64MMFR0_EL1.PARange indicates that the implementation does not support a 52 bit PA size, if a translation table lookup uses this register when the Effective value of VTCR_EL2.PS is `0b110` and the value of register bits[5:2] is nonzero, an Address size fault is generated. When the value of ID_AA64MMFR0_EL1.PARange indicates that the implementation supports a 56 bit PA size, bits [55:52] of the stage 2 translation table base address are zero.

If the Effective value of VTCR_EL2.PS is not `0b110` then:

- Register bits[47:x] hold bits[47:x] of the stage 2 translation table base address.
- Register bits[(x-1):1] are res0.
- If the implementation supports 52-bit PAs and IPAs then bits[51:48] of the translation table base addresses used in this stage of translation are `0b0000`.

If any VTTBR_EL2[47:0] bit that is defined as res0 has the value 1 when a translation table walk is performed using VTTBR_EL2, then the translation table base address might be misaligned, with effects that are constrained unpredictable, and must be one of the following:

- Bits[x-1:0] of the translation table base address are treated as if all the bits are zero. The value read back from the corresponding register bits is either the value written to the register or zero.
- The result of the calculation of an address for a translation table walk using this register can be corrupted in those bits that are nonzero.

The AArch64 Virtual Memory System Architecture chapter describes how x is calculated based on the value of VTCR_EL2.T0SZ, the stage of translation, and the translation granule size.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

CnP, bit [0]
When FEAT_TTCNP is implemented:

Common not Private. This bit indicates whether each entry that is pointed to by VTTBR_EL2 is a member of a common set that can be used by every PE in the Inner Shareable domain for which the value of VTTBR_EL2.CnP is 1.

CnP	Meaning

0b0	The translation table entries pointed to by VTTBR_EL2 are permitted to differ from the entries for VTTBR_EL2 for other PEs in the Inner Shareable domain. This is not affected by the value of the current VMID.
0b1	The translation table entries pointed to by VTTBR_EL2 are the same as the translation table entries for every other PE in the Inner Shareable domain for which the value of VTTBR_EL2.CnP is 1 and the VMID is the same as the current VMID.

This bit is permitted to be cached in a TLB.

Note

If the value of VTTBR_EL2.CnP bit is 1 on multiple PEs in the same Inner Shareable domain and those VTTBR_EL2s do not point to the same translation table entries when using the current VMID then the results of translations using VTTBR_EL2 are constrained unpredictable, see 'CONSTRAINED UNPREDICTABLE behaviors due to caching of control or data values'.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

Accessing VTTBR_EL2

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

MRS <Xt>, VTTBR_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0001	0b000

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.<NV2,NV> == '11' then
        X[t, 64] = NVMem[0x020];
    elsif EL2Enabled() && HCR_EL2.NV == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = VTTBR_EL2<63:0>;
elsif PSTATE.EL == EL3 then
    X[t, 64] = VTTBR_EL2<63:0>;
```

MSR VTTBR_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0001	0b000

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.<NV2,NV> == '11' then
        NVMem[0x020] = X[t, 64];
    elsif EL2Enabled() && HCR_EL2.NV == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    VTTBR_EL2<63:0> = X[t, 64];
elsif PSTATE.EL == EL3 then
    VTTBR_EL2<63:0> = X[t, 64];
```

When FEAT_D128 is implemented

MRRS <Xt+1>, <Xt>, VTTBR_EL2

op0	op1	CRn	CRm	op2

0b11	0b100	0b0010	0b0001	0b000

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.<NV2,NV> == '11' then
        (X[t + 1, 64], X[t, 64]) = (NVMem[0x028],
NVMem[0x020]);
    elsif EL2Enabled() && HCR_EL2.NV == '1' then
        AArch64.SystemAccessTrap(EL2, 0x14);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    if Halted() && HaveEL(EL3) && EDSCR.SDD == '1'
&& boolean IMPLEMENTATION_DEFINED "EL3 trap priority
when SDD == '1'" && SCR_EL3.D128En == '0' then
        UNDEFINED;
    elsif HaveEL(EL3) && SCR_EL3.D128En == '0' then
        if Halted() && EDSCR.SDD == '1' then
            UNDEFINED;
        else
            AArch64.SystemAccessTrap(EL3, 0x14);
    else
        (X[t + 1, 64], X[t, 64]) =
(VTTBR_EL2<127:64>, VTTBR_EL2<63:0>);
elsif PSTATE.EL == EL3 then
    (X[t + 1, 64], X[t, 64]) = (VTTBR_EL2<127:64>,
VTTBR_EL2<63:0>);
```

When FEAT_D128 is implemented

MSRR VTTBR_EL2, <Xt+1>, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0001	0b000

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.<NV2,NV> == '11' then
        (NVMem[0x028], NVMem[0x020]) = (X[t + 1,
64], X[t, 64]);
    elsif EL2Enabled() && HCR_EL2.NV == '1' then
        AArch64.SystemAccessTrap(EL2, 0x14);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    if Halted() && HaveEL(EL3) && EDSCR.SDD == '1'
&& boolean IMPLEMENTATION_DEFINED "EL3 trap priority
when SDD == '1'" && SCR_EL3.D128En == '0' then
        UNDEFINED;
    elsif HaveEL(EL3) && SCR_EL3.D128En == '0' then
```

```
        if Halted() && EDSCR.SDD == '1' then
            UNDEFINED;
        else
            AArch64.SystemAccessTrap(EL3, 0x14);
    else
        (VTTBR_EL2<127:64>, VTTBR_EL2<63:0>) = (X[t
+ 1, 64], X[t, 64]);
elsif PSTATE.EL == EL3 then
    (VTTBR_EL2<127:64>, VTTBR_EL2<63:0>) = (X[t + 1,
64], X[t, 64]);
```

28/03/2023 16:02; 72747e43966d6b97dcbd230a1b3f0421d1ea3d94