

**Requirements List
of
The RISC-V Instruction Set Manual
Volume II: Privileged Architecture**

Document Version 20211203*

**by
Mehmet Öner**

Version 1.0

*“The RISC-V Instruction Set Manual, Volume II: Privileged Architecture, Document Version 20211203”, Editors Andrew Waterman, Krste Asanović, and John Hauser, RISC-V International, December 2021.
<https://riscv.org/technical/specifications/>
Released under a Creative Commons Attribution 4.0 International License.
<https://creativecommons.org/licenses/by/4.0/>

About

The Document

In systems engineering approach, before doing anything with the design of the system under consideration, *requirements analysis* must be completed as one of the first tasks (if not the very first). Beginning with an itemized, atomic, classified and well defined list of requirements is essential. Because, following activities at various stages of development (like design coverage analysis, testing, verification, validation ...) depend on the requirement specifications stated at the beginning.

RISC-V International provides the ISA (Instruction Set Architecture) and non-ISA requirement specifications for the RISC-V architecture (<https://riscv.org/technical/specifications/>). These documents in general are good written technical plain text documents. However, they lack some aspects of good requirement specification practices:

- Requirements are in free text form and not itemized: Itemized list of requirements enables requirement coverage in design, test, verification and validation phases.
- Text includes comments and information statements along with requirements: Statements must be clearly labeled and categorized.
- Some statements include more than one specifications: Each specification need to be isolated.
- Some specifications such as instruction definitions are distributed throughout the text: The distributed content need to be put together to have a complete the specification.

The aim of this document is providing an edited list of requirements for “The RISC-V Instruction Set Manual, Volume II: Privileged Architecture, Document Version 20211203”, Editors Andrew Waterman, Krste Asanović, and John Hauser, RISC-V International, December 2021. <https://riscv.org/technical/specifications/>. Released under a Creative Commons Attribution 4.0 International License. <https://creativecommons.org/licenses/by/4.0/>

In particular:

- Statements were itemized and given an ID number.
- Each itemized statement was referenced to the original document to provide traceability
- Itemized statements were categorized
- Complex statements were broken into simpler atomic requirement statements when needed.
- Distributed requirement information was put together to form complete specifications.

Special attention was given to preserve original statements, even when dividing complex statements into simpler atomic statements. But occasionally, some statements were re-written as to form a formal requirement statement.

Following table lists which chapters are included or excluded from this document and why.

Chapter	Status	Explanation
Chapter 1 Introduction	Included	This chapter includes introductory materials and some requirements
Chapter 2 Control and Status Registers (CSRs)	Included	Zicsr extension is ratified already.
Chapter 3 Machine-Level ISA	Included	Machine-Level ISA is ratified
Chapter 4 Supervisor-Level ISA	Included	Supervisor-Level ISA is ratified

Chapter	Status	Explanation
Chapter 5 “Svnapot” Standard Extension for NAPOT Translation Contiguity	Included	Svnapot extension is ratified
Chapter 6 “Svpbmt” Standard Extension for Page-Based Memory Types	Included	Svpbmt extension is ratified
Chapter 7 “Svinval” Standard Extension for Fine-Grained Address-Translation Cache Invalidation	Included	Svinval extension is ratified
Chapter 8 Hypervisor Extension	Included	Hypervisor Extension is ratified
Chapter 9 RISC-V Privileged Instruction Set Listings	Excluded	The information in this chapter is already given in respective instruction statements.
Chapter 10 History	Excluded	This chapter is history.

This document is released under a Creative Commons Attribution 4.0 International License. Please use and cite accordingly.

The Editor (or the systems engineer)

After 34 years of my career, I retired from my regular job in 2023. Now, I do part time consulting services to interested parties, while I do work on projects that interest me more than a regular work.

In my career I dealt with very diverse fields of engineering: Academics, C/C++ desktop programming, embedded systems, analog circuit design, DSP algorithms, VLSI/FPGA design, underwater acoustics are to name few.

I've always enjoyed designing controllers and processors with generic HDL for VLSI or FPGA. So, as my personal project to work on, I decided to design RISC-V cores with different capabilities.

Having some defense sector background, I find systems engineering approach very useful. After reading RISC-V specification documents, I decided to take the initiative and edit the documents into customer requirements list format which is a tough, tedious and time consuming work.

In case someone else could find these documents useful, I share them on github:

<https://github.com/vizionerco/RISC-V>

Best regards,

Mehmet Öner, Ph.D.

www.linkedin.com/in/mehmet-oner-00453733/

Table of Contents

About.....	2
The Document.....	2
The Editor (or the systems engineer).....	3
Definitions.....	5
CHAPTER 1 INTRODUCTION.....	8
CHAPTER 2 Control and Status Registers (CSRs).....	11
CHAPTER 3 Machine-Level ISA.....	19
CHAPTER 4 Supervisor-Level ISA.....	56
CHAPTER 5 “Svnapot” Standard Extension for NAPOT Translation Contiguity.....	79
CHAPTER 6 “Svpbmt” Standard Extension for Page-Based Memory Types.....	81
CHAPTER 7 “Svinval” Standard Extension for Fine-Grained Address-Translation Cache Invalidation.....	83
CHAPTER 8 Hypervisor Extension.....	86

Definitions

Table 1: Requirement Types

TYPE	NAME	EXPLANATION
H	Heading	Headings in the original document. Headings are included to provide context to the subsequent requirements
I	Information	These are statements that explain some aspects of the subject, but actually do not specify any requirement. For these types, the statement(s) in the text is given as is.
C	Comment	These statements are original comment statements in the RISC_V documentation which are explained as: "Commentary on our design decisions is formatted as in this paragraph. This non-normative text can be skipped if the reader is only interested in the specification itself." For these types, the statement(s) in the text is given as is.
R	Requirement	These are statements that specify a specific need to be fulfilled. For these types, the statement(s) in the text is given as is where possible. In some cases, information is collected from different tables and figures to form a complete specification. In some cases, context is added in parenthesis to make the requirement self explanatory. In some cases, the statements are broken into single statements requirement statements.
O	Optional Requirement	These are statements that specify a property that is not mandatory to implement. However if it is chosen to fulfill, it should obey this requirement. Inclusion of the text is the same as R/Requirement type.
T	Tentative Requirement	These are requirements but are not frozen yet by the RISC-V committee. Inclusion of the text is the same as R/Requirement type.

Table 2: Abbreviations & Definitions

SHORT	MEANING
ABI	Application binary interface
Accelerator	either a non-programmable fixed-function unit or a core that can operate autonomously but is specialized for certain tasks.
AEE	Application Execution Environment
Bare Metal EEI	Hardware platforms where harts are directly implemented by physical processor threads and instructions have full access to the physical address space. The hardware platform defines an execution environment that begins at power-on reset.
Contained Trap	The trap is visible to, and handled by, software running inside the execution environment. For example, in an EEI providing both supervisor and user mode on harts, an ECALL by a user-mode hart will generally result in a transfer of control to a supervisor mode handler running on the same hart. Similarly, in the same environment, when a hart is interrupted, an interrupt handler will be run in supervisor mode on the hart.
Coprocessor	a unit that is attached to a RISC-V core and is mostly sequenced by a RISC-V instruction stream, but which contains additional architectural state and instruction-set extensions, and possibly some limited autonomy relative to the primary RISC-V instruction stream.
Core	A component is termed a core if it contains an independent instruction fetch unit
CSR	Control and Status Registers
EEI	Execution environment interface

SHORT	MEANING
Emulator EEI	Emulates RISC-V harts on an underlying operating system, and which can provide either a user-level or a supervisor-level execution environment.
Exception	We use the term <i>exception</i> to refer to an unusual condition occurring at run time associated with an instruction in the current RISC-V hart.
Fatal Trap	The trap represents a fatal failure and causes the execution environment to terminate execution. Examples include failing a virtual-memory page-protection check or allowing a watchdog timer to expire. Each EEI should define how execution is terminated and reported to an external environment.
FLEN	We use the term FLEN to describe the width of the floating-point registers in the RISC-V ISA
Foundation	RISC-V Foundation
Hart	Hardware Thread. From the perspective of software running in a given execution environment, a hart is a resource that autonomously fetches and executes RISC-V instructions within that execution environment. In this respect, a hart behaves like a hardware thread resource even if time-multiplexed onto real hardware by the execution environment.
HBI	Hypervisor binary interface
HEE	Hypervisor execution environment
HSXLEN	The effective XLEN when executing in hypervisor-extended supervisor mode (HS-mode)
Hypervisor EEI	Provides multiple supervisor-level execution environments for guest operating systems.
IALIGN	We use the term IALIGN (measured in bits) to refer to the instruction-address alignment constraint the implementation enforces. IALIGN is 32 bits in the base ISA, but some ISA extensions, including the compressed ISA extension, relax IALIGN to 16 bits. IALIGN may not take on any value other than 16 or 32.
ILEN	We use the term ILEN (measured in bits) to refer to the maximum instruction length supported by an implementation, and which is always a multiple of IALIGN. For implementations supporting only a base instruction set, ILEN is 32 bits. Implementations supporting longer instructions have larger values of ILEN.
Interrupt	We use the term <i>interrupt</i> to refer to an external asynchronous event that may cause a RISC-V hart to experience an unexpected transfer of control.
Invisible Trap	The trap is handled transparently by the execution environment and execution resumes normally after the trap is handled. Examples include emulating missing instructions, handling non-resident page faults in a demand-paged virtual-memory system, or handling device interrupts for a different job in a multiprogrammed machine. In these cases, the software running inside the execution environment is not aware of the trap (we ignore timing effects in these definitions).
ISA	Instruction Set Architecture
Memory Word	A <i>word</i> of memory is defined as 32 bits (4 bytes). Correspondingly, a <i>halfword</i> is 16 bits (2 bytes), a <i>doubleword</i> is 64 bits (8 bytes), and a <i>quadword</i> is 128 bits (16 bytes).
MXLEN	The effective XLEN in machine-mode (M-mode).
Nonstandard ISA Extension	An extension that is not defined by the RISC-V Foundation.
Operating System EEI	Provides multiple user-level execution environments by multiplexing user-level harts onto available physical processor threads and by controlling access to memory via virtual memory.
OS	Operating System

SHORT	MEANING
PMA	Physical memory attributes
PTE	Page Table Entry
RC	Release Consistency (memory consistency model)
RCpc	Release consistency with processor-consistent synchronization operations
RCsc	Release Consistency with sequentially-consistent synchronization operations
Requested Trap	The trap is a synchronous exception that is an explicit call to the execution environment requesting an action on behalf of software inside the execution environment. An example is a system call. In this case, execution may or may not resume on the hart after the requested action is taken by the execution environment. For example, a system call could remove the hart or cause an orderly termination of the entire execution environment.
RV32GC	RV32 ISA with G pseudo extension and C extension
RV32I	RISC-V 32-bit Base Integer ISA
RV64GC	RV64 ISA with G pseudo extension and C extension
RV64I	RISC-V 64-bit Base Integer ISA
SBI	RISC-V supervisor binary interface
SEE	Supervisor Execution Environment
SXLEN	The effective XLEN in supervisor mode (S-mode)
Trap	We use the term <i>trap</i> to refer to the transfer of control to a trap handler caused by either an exception or an interrupt.
TLB	Translation lookaside buffer
UNSPECIFIED	<p>The term UNSPECIFIED refers to a behavior or value that is intentionally unconstrained. The definition of these behaviors or values is open to extensions, platform standards, or implementations. Extensions, platform standards, or implementation documentation may provide normative content to further constrain cases that the base architecture defines as UNSPECIFIED.</p> <p>Like the base architecture, extensions should fully describe allowable behavior and values and use the term UNSPECIFIED for cases that are intentionally unconstrained. These cases may be constrained or defined by other extensions, platform standards, or implementations.</p>
UXLEN	The effective XLEN in user mode (U-mode)
VSXLEN	The effective XLEN when executing in virtual S-mode (VS-mode)
XLEN	Refers to the width of an integer register in bits of an ISA

CHAPTER 1 Introduction

ID	REFERENCE	TYPE	DEFINITION			
RVP.1.1	1.0 (p.1)	H	Introduction			
RVP.1.2	1.0 (p.1)	I	This document describes the RISC-V privileged architecture, which covers all aspects of RISC-V systems beyond the unprivileged ISA, including privileged instructions as well as additional functionality required for running operating systems and attaching external devices.			
RVP.1.3	1.0 (p.1)	C	We briefly note that the entire privileged-level design described in this document could be replaced with an entirely different privileged-level design without changing the unprivileged ISA, and possibly without even changing the ABI. In particular, this privileged specification was designed to run existing popular operating systems, and so embodies the conventional level-based protection model. Alternate privileged specifications could embody other more flexible protection-domain models. For simplicity of expression, the text is written as if this was the only possible privileged architecture.			
RVP.1.4	1.1 (p.1)	H	RISC-V Privileged Software Stack Terminology			
RVP.1.5	1.1 (p.1)	I	This section describes the terminology we use to describe components of the wide range of possible privileged software stacks for RISC-V.			
RVP.1.6	1.1 (p.1)	I	Some of the possible software stacks that can be supported by the RISC-V architecture (are given in RVP.1.8, RVP.1.9 and RVP.1.11).			
RVP.1.7	1.1 (p.1)	C	graphical convention represents abstract interfaces using black boxes with white text, to separate them from concrete instances of components implementing the interfaces			
RVP.1.8	1.1 (p.1, p.2) Figure 1.1	I	<table border="1"> <tr><td>Application</td></tr> <tr><td>ABI</td></tr> <tr><td>AEE</td></tr> </table>	Application	ABI	AEE
Application						
ABI						
AEE						

A simple system that supports only a single application running on an application execution environment (AEE). The application is coded to run with a particular application binary interface (ABI). The ABI includes the supported user-level ISA plus a set of ABI calls to interact with the AEE. The ABI hides details of the AEE from the application to allow greater flexibility in implementing the AEE. The same ABI could be implemented natively on multiple different host OSs, or could be supported by a user-mode emulation environment running on a machine with a different native ISA.

ID REFERENCE TYPE DEFINITION

RVP.1.9	1.0 (p.2) Figure 1.1	I	<table border="1"> <tr> <td>Application</td><td>Application</td></tr> <tr> <td>ABI</td><td>ABI</td></tr> <tr> <td>OS</td><td></td></tr> <tr> <td>SBI</td><td></td></tr> <tr> <td>SEE</td><td></td></tr> </table>	Application	Application	ABI	ABI	OS		SBI		SEE		<p>This configuration shows a conventional operating system (OS) that can support multi programmed execution of multiple applications. Each application communicates over an ABI with the OS, which provides the AEE. Just as applications interface with an AEE via an ABI, RISC-V operating systems interface with a supervisor execution environment (SEE) via a supervisor binary interface (SBI). An SBI comprises the user-level and supervisor-level ISA together with a set of SBI function calls. Using a single SBI across all SEE implementations allows a single OS binary image to run on any SEE. The SEE can be a simple boot loader and BIOS-style IO system in a low-end hardware platform, or a hypervisor-provided virtual machine in a high-end server, or a thin translation layer over a host operating system in an architecture simulation environment.</p>																		
Application	Application																															
ABI	ABI																															
OS																																
SBI																																
SEE																																
RVP.1.10	1.1 (p.2)	C		Most supervisor-level ISA definitions do not separate the SBI from the execution environment and/or the hardware platform, complicating virtualization and bring-up of new hardware platforms.																												
RVP.1.11	1.1 (p.2) Figure 1.1	I	<table border="1"> <tr> <td>Application</td> <td>Application</td> <td>Application</td> <td>Application</td> </tr> <tr> <td>ABI</td> <td>ABI</td> <td>ABI</td> <td>ABI</td> </tr> <tr> <td>OS</td> <td></td> <td>OS</td> <td></td> </tr> <tr> <td>SBI</td> <td></td> <td>SBI</td> <td></td> </tr> <tr> <td>Hypervisor</td> <td></td> <td></td> <td></td> </tr> <tr> <td>HBI</td> <td></td> <td></td> <td></td> </tr> <tr> <td>HEE</td> <td></td> <td></td> <td></td> </tr> </table>	Application	Application	Application	Application	ABI	ABI	ABI	ABI	OS		OS		SBI		SBI		Hypervisor				HBI				HEE				<p>This configuration shows a virtual machine monitor configuration where multiple multi programmed OSs are supported by a single hypervisor. Each OS communicates via an SBI with the hypervisor, which provides the SEE. The hypervisor communicates with the hypervisor execution environment (HEE) using a hypervisor binary interface (HBI), to isolate the hypervisor from details of the hardware platform.</p>
Application	Application	Application	Application																													
ABI	ABI	ABI	ABI																													
OS		OS																														
SBI		SBI																														
Hypervisor																																
HBI																																
HEE																																
RVP.1.12	1.1 (p.2)	C		The ABI, SBI, and HBI are still a work-in-progress, but we are now prioritizing support for Type-2 hypervisors where the SBI is provided recursively by an S-mode OS.																												
RVP.1.13	1.1 (p.2)	I		Hardware implementations of the RISC-V ISA will generally require additional features beyond the privileged ISA to support the various execution environments (AEE, SEE, or HEE).																												
RVP.1.14	1.2 (p.2)	H		Privilege Levels																												
RVP.1.15	1.2 (p.2)	R		At any time, a RISC-V hardware thread (hart) is running at some privilege level encoded as a mode in one or more CSRs (control and status registers).																												

ID REFERENCE TYPE DEFINITION

RVP.1.16 1.2 (p.2, p.3) R Table 1.1 Three RISC-V privilege levels are currently defined as shown in the table below.

Level	Encoding	Name	Abbreviation
0	00	User / Application	U
1	01	Supervisor	S
2	10	<i>Reserved</i>	
3	11	Machine	M

RVP.1.17 1.2 (p.2, p.3) R Privilege levels are used to provide protection between different components of the software stack, and attempts to perform operations not permitted by the current privilege mode will cause an exception to be raised.

RVP.1.18 1.2 (p.3) R These (privilege violation) exceptions will normally cause traps into an underlying execution environment.

RVP.1.19 1.2 (p.3) C In the description, we try to separate the privilege level for which code is written, from the privilege mode in which it runs, although the two are often tied. For example, a supervisor-level operating system can run in supervisor-mode on a system with three privilege modes, but can also run in user-mode under a classic virtual machine monitor on systems with two or more privilege modes. In both cases, the same supervisor-level operating system binary code can be used, coded to a supervisor-level SBI and hence expecting to be able to use supervisor-level privileged instructions and CSRs. When running a guest OS in user mode, all supervisor-level actions will be trapped and emulated by the SEE running in the higher-privilege level.

RVP.1.20 1.2 (p.3) R The machine level has the highest privileges and is the only mandatory privilege level for a RISC-V hardware platform.

RVP.1.21 1.2 (p.3) R Code run in machine-mode (M-mode) is usually inherently trusted, as it has low-level access to the machine implementation.

RVP.1.22 1.2 (p.3) R M-mode can be used to manage secure execution environments on RISC-V.

RVP.1.23 1.2 (p.3) R User-mode (U-mode) is intended for conventional application usage.

RVP.1.24 1.2 (p.3) R Supervisor-mode (S-mode) is intended for operating system usage.

RVP.1.25 1.2 (p.3) R Each privilege level has a core set of privileged ISA extensions with optional extensions and variants

RVP.1.26 1.2 (p.3)
Table 1.2 R Implementations might provide anywhere from 1 to 3 privilege modes trading off reduced isolation for lower implementation cost, as shown in the table below

Number of Levels	Supported Modes	Intended Usage
1	M	Simple embedded systems
2	M, U	Secure embedded systems
3	M, S, U	Systems running Unix-like operating systems

RVP.1.27 1.2 (p.3) R All hardware implementations must provide M-mode, as this is the only mode that has unfettered access to the whole machine.

RVP.1.28 1.2 (p.3) O The simplest RISC-V implementations may provide only M-mode, though this will provide no protection against incorrect or malicious application code.

RVP.1.29 1.2 (p.3) C The lock feature of the optional PMP facility can provide some limited protection even with only M-mode implemented.

ID	REFERENCE	TYPE	DEFINITION
RVP.1.30	1.2 (p.4)	I	Many RISC-V implementations will also support at least user mode (U-mode) to protect the rest of the system from application code.
RVP.1.31	1.2 (p.4)	I	Supervisor mode (S-mode) can be added to provide isolation between a supervisor-level operating system and the SEE.
RVP.1.32	1.2 (p.4)	I	A hart normally runs application code in U-mode until some trap (e.g., a supervisor call or a timer interrupt) forces a switch to a trap handler, which usually runs in a more privileged mode. The hart will then execute the trap handler, which will eventually resume execution at or after the original trapped instruction in U-mode.
RVP.1.33	1.2 (p.4)	I	Traps that increase privilege level are termed <i>vertical traps</i>
RVP.1.34	1.2 (p.4)	I	Traps that remain at the same privilege level are termed <i>horizontal traps</i> .
RVP.1.35	1.2 (p.4)	C	Horizontal traps can be implemented as vertical traps that return control to a horizontal trap handler in the less-privileged mode.
RVP.1.36	1.3 (p.5)	H	Debug Mode
RVP.1.37	1.3 (p.5)	R	Implementations may also include a debug mode to support off-chip debugging and/or manufacturing test. Debug mode (D-mode) can be considered an additional privilege mode, with even more access than M-mode. The separate debug specification proposal describes operation of a RISC-V hart in debug mode. Debug mode reserves a few CSR addresses that are only accessible in D-mode, and may also reserve some portions of the physical address space on a platform.

CHAPTER 2 Control and Status Registers (CSRs)

ID	REFERENCE	TYPE	DEFINITION
RVP.2.1	2.0 (p.5)	H	Control and Status Registers (CSRs)
RVP.2.2	2.0 (p.5)	I	The SYSTEM major opcode is used to encode all privileged instructions in the RISC-V ISA.
RVP.2.3	2.0 (p.5)	I	These can be divided into two main classes: those that atomically read-modify-write control and status registers (CSRs), which are defined in the Zicsr extension, and all other privileged instructions.
RVP.2.4	2.0 (p.5)	R	The privileged architecture requires the Zicsr extension;...
RVP.2.5	2.0 (p.5)	I	... which other privileged instructions are required depends on the privileged-architecture feature set.
RVP.2.6	2.0 (p.5)	R	In addition to the unprivileged state described in Volume I of this manual, an implementation may contain additional CSRs, accessible by some subset of the privilege levels using the CSR instructions described in Volume I.
RVP.2.7	2.0 (p.5)	I	In this chapter, we map out the CSR address space.
RVP.2.8	2.0 (p.5)	I	The following chapters describe the function of each of the CSRs according to privilege level, as well as the other privileged instructions which are generally closely associated with a particular privilege level.
RVP.2.9	2.0 (p.5)	R	Note that although CSRs and instructions are associated with one privilege level, they are also accessible at all higher privilege levels.
RVP.2.10	2.0 (p.5)	R	Standard CSRs do not have side effects on reads but may have side effects on writes
RVP.2.11	2.1 (p.5)	H	CSR Address Mapping Conventions
RVP.2.12	2.1 (p.5)	R	The standard RISC-V ISA sets aside a 12-bit encoding space (csr[11:0]) for up to 4,096 CSRs.
RVP.2.13	2.1 (p.5)	R	By convention, the upper 4 bits of the CSR address (csr[11:8]) are used to encode the read and write accessibility of the CSRs according to privilege level
RVP.2.14	2.1 (p.5)	R	The top two bits (csr[11:10]) indicate whether the register is read/write (00, 01, or 10) or read-only (11).
RVP.2.15	2.1 (p.5)	R	The next two bits (csr[9:8]) encode the lowest privilege level that can access the CSR.
RVP.2.16	2.1 (p.5)	C	The CSR address convention uses the upper bits of the CSR address to encode default access privileges. This simplifies error checking in the hardware and provides a larger CSR space, but does constrain the mapping of CSRs into the address space.
RVP.2.17	2.1 (p.5)	C	Implementations might allow a more-privileged level to trap otherwise permitted CSR accesses by a less-privileged level to allow these accesses to be intercepted. This change should be transparent to the less-privileged software.
RVP.2.18	2.1 (p.6)	R	Attempts to access a non-existent CSR raise an illegal instruction exception
RVP.2.19	2.1 (p.6)	R	Attempts to access a CSR without appropriate privilege level or to write a read-only register also raise illegal instruction exceptions.

ID REFERENCE TYPE DEFINITION

RVP.2.20	2.1 (p.6)	R	A read/write register might also contain some bits that are read-only, in which case writes to the read-only bits are ignored																																																										
RVP.2.21	2.1 (p.6)	R	The CSR addresses designated for custom uses will not be redefined by future standard extensions.																																																										
RVP.2.22	2.1 (p.7) Table 2.1	R	Unprivileged and User-Level CSR address space:																																																										
			<table border="1"> <thead> <tr> <th colspan="3">CSR Address</th> <th rowspan="2">Hex</th> <th rowspan="2">Use and Accessibility</th> </tr> <tr> <th>[11:10]</th> <th>[9:8]</th> <th>[7:4]</th> </tr> </thead> <tbody> <tr> <td>00</td> <td>00</td> <td>XXXX</td> <td>0x000-0x0FF</td> <td>Standard read/write</td> </tr> <tr> <td>01</td> <td>00</td> <td>XXXX</td> <td>0x400-0x4FF</td> <td>Standard read/write</td> </tr> <tr> <td>10</td> <td>00</td> <td>XXXX</td> <td>0x800-0x8FF</td> <td>Custom read/write</td> </tr> <tr> <td>11</td> <td>00</td> <td>0XXX</td> <td>0xC00-0xC7F</td> <td>Standard read only</td> </tr> <tr> <td>11</td> <td>00</td> <td>10XX</td> <td>0xC80-0xCB</td> <td>Standard read only</td> </tr> <tr> <td>11</td> <td>00</td> <td>11XX</td> <td>0xCC0-0xCFF</td> <td>Custom read only</td> </tr> </tbody> </table>	CSR Address			Hex	Use and Accessibility	[11:10]	[9:8]	[7:4]	00	00	XXXX	0x000-0x0FF	Standard read/write	01	00	XXXX	0x400-0x4FF	Standard read/write	10	00	XXXX	0x800-0x8FF	Custom read/write	11	00	0XXX	0xC00-0xC7F	Standard read only	11	00	10XX	0xC80-0xCB	Standard read only	11	00	11XX	0xCC0-0xCFF	Custom read only																				
CSR Address			Hex	Use and Accessibility																																																									
[11:10]	[9:8]	[7:4]																																																											
00	00	XXXX	0x000-0x0FF	Standard read/write																																																									
01	00	XXXX	0x400-0x4FF	Standard read/write																																																									
10	00	XXXX	0x800-0x8FF	Custom read/write																																																									
11	00	0XXX	0xC00-0xC7F	Standard read only																																																									
11	00	10XX	0xC80-0xCB	Standard read only																																																									
11	00	11XX	0xCC0-0xCFF	Custom read only																																																									
RVP.2.23	2.1 (p.7) Table 2.1	R	Supervisor-Level CSR address space:																																																										
			<table border="1"> <thead> <tr> <th colspan="3">CSR Address</th> <th rowspan="2">Hex</th> <th rowspan="2">Use and Accessibility</th> </tr> <tr> <th>[11:10]</th> <th>[9:8]</th> <th>[7:4]</th> </tr> </thead> <tbody> <tr> <td>00</td> <td>01</td> <td>XXXX</td> <td>0x100-0x1FF</td> <td>Standard read/write</td> </tr> <tr> <td>01</td> <td>01</td> <td>0XXX</td> <td>0x500-0x57F</td> <td>Standard read/write</td> </tr> <tr> <td>01</td> <td>01</td> <td>10XX</td> <td>0x580-0x5BF</td> <td>Standard read/write</td> </tr> <tr> <td>01</td> <td>01</td> <td>11XX</td> <td>0x5C0-0x5FF</td> <td>Custom read/write</td> </tr> <tr> <td>10</td> <td>01</td> <td>0XXX</td> <td>0x900-0x97F</td> <td>Standard read/write</td> </tr> <tr> <td>10</td> <td>01</td> <td>10XX</td> <td>0x980-0x9BF</td> <td>Standard read/write</td> </tr> <tr> <td>10</td> <td>01</td> <td>11XX</td> <td>0x9C0-0x9FF</td> <td>Custom read/write</td> </tr> <tr> <td>11</td> <td>01</td> <td>0XXX</td> <td>0xD00-0xD7F</td> <td>Standard read only</td> </tr> <tr> <td>11</td> <td>01</td> <td>10XX</td> <td>0xD80-0xDBF</td> <td>Standard read only</td> </tr> <tr> <td>11</td> <td>01</td> <td>11XX</td> <td>0xDC0-0xDFF</td> <td>Custom read only</td> </tr> </tbody> </table>	CSR Address			Hex	Use and Accessibility	[11:10]	[9:8]	[7:4]	00	01	XXXX	0x100-0x1FF	Standard read/write	01	01	0XXX	0x500-0x57F	Standard read/write	01	01	10XX	0x580-0x5BF	Standard read/write	01	01	11XX	0x5C0-0x5FF	Custom read/write	10	01	0XXX	0x900-0x97F	Standard read/write	10	01	10XX	0x980-0x9BF	Standard read/write	10	01	11XX	0x9C0-0x9FF	Custom read/write	11	01	0XXX	0xD00-0xD7F	Standard read only	11	01	10XX	0xD80-0xDBF	Standard read only	11	01	11XX	0xDC0-0xDFF	Custom read only
CSR Address			Hex	Use and Accessibility																																																									
[11:10]	[9:8]	[7:4]																																																											
00	01	XXXX	0x100-0x1FF	Standard read/write																																																									
01	01	0XXX	0x500-0x57F	Standard read/write																																																									
01	01	10XX	0x580-0x5BF	Standard read/write																																																									
01	01	11XX	0x5C0-0x5FF	Custom read/write																																																									
10	01	0XXX	0x900-0x97F	Standard read/write																																																									
10	01	10XX	0x980-0x9BF	Standard read/write																																																									
10	01	11XX	0x9C0-0x9FF	Custom read/write																																																									
11	01	0XXX	0xD00-0xD7F	Standard read only																																																									
11	01	10XX	0xD80-0xDBF	Standard read only																																																									
11	01	11XX	0xDC0-0xDFF	Custom read only																																																									
RVP.2.24	2.1 (p.7) Table 2.1	R	Hypervisor and VS CSR address space:																																																										
			<table border="1"> <thead> <tr> <th colspan="3">CSR Address</th> <th rowspan="2">Hex</th> <th rowspan="2">Use and Accessibility</th> </tr> <tr> <th>[11:10]</th> <th>[9:8]</th> <th>[7:4]</th> </tr> </thead> <tbody> <tr> <td>00</td> <td>10</td> <td>XXXX</td> <td>0x200-0x2FF</td> <td>Standard read/write</td> </tr> <tr> <td>01</td> <td>10</td> <td>0XXX</td> <td>0x600-0x67F</td> <td>Standard read/write</td> </tr> <tr> <td>01</td> <td>10</td> <td>10XX</td> <td>0x680-0x6BF</td> <td>Standard read/write</td> </tr> <tr> <td>01</td> <td>10</td> <td>11XX</td> <td>0x6C0-0x6FF</td> <td>Custom read/write</td> </tr> <tr> <td>10</td> <td>10</td> <td>0XXX</td> <td>0xA00-0xA7F</td> <td>Standard read/write</td> </tr> <tr> <td>10</td> <td>10</td> <td>10XX</td> <td>0xA80-0xABF</td> <td>Standard read/write</td> </tr> <tr> <td>10</td> <td>10</td> <td>11XX</td> <td>0xAC0-0xAF</td> <td>Custom read/write</td> </tr> <tr> <td>11</td> <td>10</td> <td>0XXX</td> <td>0xE00-0xE7F</td> <td>Standard read only</td> </tr> <tr> <td>11</td> <td>10</td> <td>10XX</td> <td>0xE80-0xEB</td> <td>Standard read only</td> </tr> <tr> <td>11</td> <td>10</td> <td>11XX</td> <td>0xEC0-0xEFF</td> <td>Custom read only</td> </tr> </tbody> </table>	CSR Address			Hex	Use and Accessibility	[11:10]	[9:8]	[7:4]	00	10	XXXX	0x200-0x2FF	Standard read/write	01	10	0XXX	0x600-0x67F	Standard read/write	01	10	10XX	0x680-0x6BF	Standard read/write	01	10	11XX	0x6C0-0x6FF	Custom read/write	10	10	0XXX	0xA00-0xA7F	Standard read/write	10	10	10XX	0xA80-0xABF	Standard read/write	10	10	11XX	0xAC0-0xAF	Custom read/write	11	10	0XXX	0xE00-0xE7F	Standard read only	11	10	10XX	0xE80-0xEB	Standard read only	11	10	11XX	0xEC0-0xEFF	Custom read only
CSR Address			Hex	Use and Accessibility																																																									
[11:10]	[9:8]	[7:4]																																																											
00	10	XXXX	0x200-0x2FF	Standard read/write																																																									
01	10	0XXX	0x600-0x67F	Standard read/write																																																									
01	10	10XX	0x680-0x6BF	Standard read/write																																																									
01	10	11XX	0x6C0-0x6FF	Custom read/write																																																									
10	10	0XXX	0xA00-0xA7F	Standard read/write																																																									
10	10	10XX	0xA80-0xABF	Standard read/write																																																									
10	10	11XX	0xAC0-0xAF	Custom read/write																																																									
11	10	0XXX	0xE00-0xE7F	Standard read only																																																									
11	10	10XX	0xE80-0xEB	Standard read only																																																									
11	10	11XX	0xEC0-0xEFF	Custom read only																																																									

ID REFERENCE TYPE DEFINITION

RVP.2.25 2.1 (p.7)
Table 2.1 R Machine-Level CSR address space:

CSR Address			Hex	Use and Accessibility
[11:10]	[9:8]	[7:4]		
00	11	XXXX	0x300-0x3FF	Standard read/write
01	11	0XXX	0x700-0x77F	Standard read/write
01	11	100X	0x780-0x79F	Standard read/write
01	11	1010	0x7A0-0x7AF	Standard read/write debug CSRs
01	11	1011	0x7B0-0x7BF	Debug-mode-only CSRs
01	11	11XX	0x7C0-0x7FF	Custom read/write
10	11	0XXX	0xB00-0xB7F	Standard read/write
10	11	10XX	0xB80-0xBBF	Standard read/write
10	11	11XX	0xBC0-0xBFF	Custom read/write
11	11	0XXX	0xF00-0xF7F	Standard read only
11	11	10XX	0xF80-0xFB0	Standard read only
11	11	11XX	0xFC0-0xFFFF	Custom read only

RVP.2.26 2.1 (p.6) R Implementations should raise illegal instruction exceptions on machine-mode access to the debug mode only registers.

RVP.2.27 2.2 (p.8)
Table 2.2 R Allocated unprivileged floating-point CSRs

Number	Access	Name	Description
0x001	Read/Write	fflags	Floating-Point Accrued Exceptions
0x002	Read/Write	frm	Floating-Point Dynamic Rounding Mode
0x003	Read/Write	fcsr	Floating-Point Control and Status Register (frm + fflags).

RVP.2.28 2.2 (p.8)
Table 2.2 R Allocated unprivileged counter/timer CSRs

Number	Access	Name	Description
0xC00	Read Only	cycle	Cycle counter for RD CYCLE instruction
0xC01	Read Only	time	Timer for RD TIME instruction
0xC02	Read Only	instret	Instructions-retired counter for RD INSTRET instruction
0xC03	Read Only	hpmcounter3	Performance-monitoring counter
0xC04	Read Only	hpmcounter4	Performance-monitoring counter
...			
0xC1F	Read Only	hpmcounter31	Performance-monitoring counter
0xC80	Read Only	cycleh	Upper 32 bits of cycle, RV32 only.
0xC81	Read Only	timeh	Upper 32 bits of time, RV32 only
0xC82	Read Only	instreth	Upper 32 bits of instret, RV32 only.
0xC83	Read Only	hpmcounter3h	Upper 32 bits of hpmcounter3, RV32 only
0xC84	Read Only	hpmcounter4h	Upper 32 bits of hpmcounter4, RV32 only
...			
0xC9F	Read Only	hpmcounter31h	Upper 32 bits of hpmcounter31, RV32 only

ID REFERENCE TYPE DEFINITION

RVP.2.29 2.2 (p.8)
Table 2.3 R Allocated supervisor trap setup CSRs

Number	Access	Name	Description
0x100	Read/Write	sstatus	Supervisor status register
0x104	Read/Write	sie	Supervisor interrupt-enable register
0x105	Read/Write	stvec	Supervisor trap handler base address
0x106	Read/Write	scounteren	Supervisor counter enable.

RVP.2.30 2.2 (p.8)
Table 2.3 R Allocated supervisor configuration CSRs

Number	Access	Name	Description
0x10A	Read/Write	senvcfg	Supervisor environment configuration register

RVP.2.31 2.2 (p.8)
Table 2.2 R Allocated supervisor trap handling CSRs

Number	Access	Name	Description
0x140	Read/Write	sscratch	Scratch register for supervisor trap handlers
0x141	Read/Write	sepc	Supervisor exception program counter
0x142	Read/Write	scause	Supervisor trap cause.
0x143	Read/Write	stval	Supervisor bad address or instruction
0x144	Read/Write	sip	Supervisor interrupt pending

RVP.2.32 2.2 (p.8)
Table 2.3 R Allocated supervisor protection and translation CSRs

Number	Access	Name	Description
0x180	Read/Write	satp	Supervisor address translation and protection

RVP.2.33 2.2 (p.8)
Table 2.3 R Allocated supervisor debug/trace registers CSRs

Number	Access	Name	Description
0x5A8	Read/Write	scontext	Supervisor-mode context register

RVP.2.34 2.2 (p.9)
Table 2.4 R Allocated hypervisor trap setup CSRs

Number	Access	Name	Description
0x600	Read/Write	hstatus	Hypervisor status register
0x602	Read/Write	hdeleg	Hypervisor exception delegation register
0x603	Read/Write	hideleg	Hypervisor interrupt delegation register
0x604	Read/Write	hie	Hypervisor interrupt-enable register
0x606	Read/Write	hcounteren	Hypervisor counter enable.
0x607	Read/Write	hgeie	Hypervisor guest external interrupt-enable register.

RVP.2.35 2.2 (p.9)
Table 2.4 R Allocated hypervisor trap handling CSRs

Number	Access	Name	Description
0x643	Read/Write	htval	Hypervisor bad guest physical address
0x644	Read/Write	hip	Hypervisor interrupt pending
0x645	Read/Write	hvip	Hypervisor virtual interrupt pending
0x64A	Read/Write	htinst	Hypervisor trap instruction (transformed)
0xE12	Read Only	hgeip	Hypervisor guest external interrupt pending

ID REFERENCE TYPE DEFINITION

RVP.2.36 2.2 (p.9)
Table 2.4 R Allocated hypervisor configuration CSRs

Number	Access	Name	Description
0x60A	Read/Write	henvcfg	Hypervisor environment configuration register
0x61A	Read/Write	henvcfg_h	Additional hypervisor env. conf. register, RV32 only

RVP.2.37 2.2 (p.9)
Table 2.4 R Allocated hypervisor protection and translation CSRs

Number	Access	Name	Description
0x680	Read/Write	hgatp	Hypervisor guest address translation and protection

RVP.2.38 2.2 (p.9)
Table 2.4 R Allocated hypervisor debug/trace registers CSRs

Number	Access	Name	Description
0x6A8	Read/Write	hcontext	Hypervisor-mode context register

RVP.2.39 2.2 (p.9)
Table 2.4 R Allocated hypervisor counter/timer virtualization registers CSRs

Number	Access	Name	Description
0x605	Read/Write	htimedelta	Delta for VS/VU-mode timer
0x615	Read/Write	htimedeltah	Upper 32 bits of htimedelta, HSXLEN=32 only.

RVP.2.40 2.2 (p.9)
Table 2.4 R Allocated virtual supervisor registers CSRs

Number	Access	Name	Description
0x200	Read/Write	vsstatus	Virtual supervisor status register
0x204	Read/Write	vsie	Virtual supervisor interrupt-enable register
0x205	Read/Write	vstvec	Virtual supervisor trap handler base address
0x240	Read/Write	vsscratch	Virtual supervisor scratch register
0x241	Read/Write	vsepc	Virtual supervisor exception program counter
0x242	Read/Write	vscause	Virtual supervisor trap cause
0x243	Read/Write	vstval	Virtual supervisor bad address or instruction
0x244	Read/Write	vsip	Virtual supervisor interrupt pending
0x280	Read/Write	vsatp	Virtual supervisor address translation and protection

RVP.2.41 2.2 (p.10)
Table 2.5 R Allocated machine information registers CSRs

Number	Access	Name	Description
0xF11	Read Only	mvendorid	Vendor ID
0xF12	Read Only	marchid	Architecture ID
0xF13	Read Only	mimpid	Implementation ID
0xF14	Read Only	mhartid	Hardware thread ID
0xF15	Read Only	mconfigptr	Pointer to configuration data structure

ID REFERENCE TYPE DEFINITION

RVP.2.42 2.2 (p.10) R Allocated machine trap setup CSRs
 Table 2.5

Number	Access	Name	Description
0x300	Read/Write	mstatus	Machine status register
0x301	Read/Write	misa	ISA and extensions
0x302	Read/Write	medeleg	Machine exception delegation register.
0x303	Read/Write	mideleg	Machine interrupt delegation register
0x304	Read/Write	mie	Machine interrupt-enable register
0x305	Read/Write	mtvec	Machine trap-handler base address.
0x306	Read/Write	mcounteren	Machine counter enable.
0x310	Read/Write	mstatush	Additional machine status register, RV32 only.

RVP.2.43 2.2 (p.10) R Allocated machine trap handling CSRs
 Table 2.5

Number	Access	Name	Description
0x340	Read/Write	mscratch	Scratch register for machine trap handlers
0x341	Read/Write	mepc	Machine exception program counter
0x342	Read/Write	mcause	Machine trap cause
0x343	Read/Write	mtval	Machine bad address or instruction
0x344	Read/Write	mip	Machine interrupt pending
0x34A	Read/Write	mtinst	Machine trap instruction (transformed)
0x34B	Read/Write	mtval2	Machine bad guest physical address

RVP.2.44 2.2 (p.10) R Allocated machine configuration CSRs
 Table 2.5

Number	Access	Name	Description
0x30A	Read/Write	menvcfg	Machine environment configuration register.
0x31A	Read/Write	menvcfgfh	Additional machine env. conf. register, RV32 only
0x747	Read/Write	mseccfg	Machine security configuration register
0x757	Read/Write	mseccfgfh	Additional machine security conf. register, RV32 only

ID REFERENCE TYPE DEFINITION

RVP.2.45 2.2 (p.10)
Table 2.5 R Allocated machine memory protection CSRs

Number	Access	Name	Description
0x3A0	Read/Write	pmpcfg0	Physical memory protection configuration
0x3A1	Read/Write	pmpcfg1	Physical memory protection configuration, RV32 only
0x3A2	Read/Write	pmpcfg2	Physical memory protection configuration
0x3A3	Read/Write	pmpcfg3	Physical memory protection configuration, RV32 only
...			
0x3AE	Read/Write	pmpcfg14	Physical memory protection configuration
0x3AF	Read/Write	pmpcfg15	Physical memory protection configuration, RV32 only
0x3B0	Read/Write	pmpaddr0	Physical memory protection address register
0x3B1	Read/Write	pmpaddr1	Physical memory protection address register
...			
0x3EF	Read/Write	pmpaddr63	Physical memory protection address register.

RVP.2.46 2.2 (p.6) R Note that not all registers are required on all implementations.

RVP.2.47 2.3 (p.12) H CSR Field Specifications

RVP.2.48 2.3 (p.12) I The following definitions and abbreviations are used in specifying the behavior of fields within the CSRs.

RVP.2.49 2.3 (p.12) R **Reserved Writes Preserve Values, Reads Ignore Values (WPRI)**

Some whole read/write fields are reserved for future use. Software should ignore the values read from these fields, and should preserve the values held in these fields when writing values to other fields of the same register. For forward compatibility, implementations that do not furnish these fields must make them read-only zero. These fields are labeled **WPRI** in the register descriptions.

RVP.2.50 2.3 (p.12) C To simplify the software model, any backward-compatible future definition of previously reserved fields within a CSR must cope with the possibility that a non-atomic read/modify/write sequence is used to update other fields in the CSR. Alternatively, the original CSR definition must specify that subfields can only be updated atomically, which may require a two-instruction clear bit/set bit sequence in general that can be problematic if intermediate values are not legal.

RVP.2.51 2.3 (p.12) R **Write/Read Only Legal Values (WLRL)**

Some read/write CSR fields specify behavior for only a subset of possible bit encodings, with other bit encodings reserved. Software should not write anything other than legal values to such a field, and should not assume a read will return a legal value unless the last write was of a legal value, or the register has not been written since another operation (e.g., reset) set the register to a legal value. These fields are labeled **WLRL** in the register descriptions.

RVP.2.52 2.3 (p.12) C Hardware implementations need only implement enough state bits to differentiate between the supported values, but must always return the complete specified bit-encoding of any supported value when read.

ID REFERENCE TYPE DEFINITION

RVP.2.53	2.3 (p.12)	R	Implementations are permitted but not required to raise an illegal instruction exception if an instruction attempts to write a non-supported value to a WLRL field. Implementations can return arbitrary bit patterns on the read of a WLRL field when the last write was of an illegal value, but the value returned should deterministically depend on the illegal written value and the value of the field prior to the write.
RVP.2.54	2.3 (p.12)	R	Write Any Values, Reads Legal Values (WARL) Some read/write CSR fields are only defined for a subset of bit encodings, but allow any value to be written while guaranteeing to return a legal value whenever read. Assuming that writing the CSR has no other side effects, the range of supported values can be determined by attempting to write a desired setting then reading to see if the value was retained. These fields are labeled WARL in the register descriptions.
RVP.2.55	2.3 (p.13)	R	Implementations will not raise an exception on writes of unsupported values to a WARL field. Implementations can return any legal value on the read of a WARL field when the last write was of an illegal value, but the legal value returned should deterministically depend on the illegal written value and the architectural state of the hart
RVP.2.56	2.4 (p.13)	H	CSR Field Modulation
RVP.2.57	2.4 (p.13)	R	If a write to one CSR changes the set of legal values allowed for a field of a second CSR, then unless specified otherwise, the second CSR's field immediately gets an UNSPECIFIED value from among its new legal values. This is true even if the field's value before the write remains legal after the write; the value of the field may be changed in consequence of the write to the controlling CSR.
RVP.2.58	2.4 (p.13)	R	A change to the value of a CSR for this reason is not a write to the affected CSR and thus does not trigger any side effects specified for that CSR.
RVP.2.59	2.4 (p.13)	C	As a special case of this rule, the value written to one CSR may control whether a field of a second CSR is writable (with multiple legal values) or is read-only. When a write to the controlling CSR causes the second CSR's field to change from previously read-only to now writable, that field immediately gets an UNSPECIFIED but legal value, unless specified otherwise.
RVP.2.60	2.4 (p.13)	C	Some CSR fields are, when writable, defined as aliases of other CSR fields. Let x be such a CSR field, and let y be the CSR field it aliases when writable. If a write to a controlling CSR causes field x to change from previously read-only to now writable, the new value of x is not UNSPECIFIED but instead immediately reflects the existing value of its alias y, as required
RVP.2.61	2.5 (p.13)	H	Implicit Reads of CSRs
RVP.2.62	2.5 (p.13)	R	Implementations sometimes perform implicit reads of CSRs. (For example, all S-mode instruction fetches implicitly read the satp CSR.) Unless otherwise specified, the value returned by an implicit read of a CSR is the same value that would have been returned by an explicit read of the CSR, using a CSR-access instruction in a sufficient privilege mode.
RVP.2.63	2.6 (p.13)	H	CSR Width Modulation

ID REFERENCE TYPE DEFINITION

RVP.2.64	2.6 (p.13, p.14)	R	If the width of a CSR is changed (for example, by changing MXLEN or UXLEN, as described in Section 3.1.6.2), the values of the <i>writable</i> fields and bits of the new-width CSR are, unless specified otherwise, determined from the previous-width CSR as though by this algorithm: 1. The value of the previous-width CSR is copied to a temporary register of the same width. 2. For the read-only bits of the previous-width CSR, the bits at the same positions in the temporary register are set to zeros. 3. The width of the temporary register is changed to the new width. If the new width W is narrower than the previous width, the least-significant W bits of the temporary register are retained and the more-significant bits are discarded. If the new width is wider than the previous width, the temporary register is zero-extended to the wider width. 4. Each writable field of the new-width CSR takes the value of the bits at the same positions in the temporary register.
RVP.2.65	2.6 (p.14)	R	Changing the width of a CSR is not a read or write of the CSR and thus does not trigger any side effects.

CHAPTER 3 Machine-Level ISA

ID	REFERENCE	TYPE	DEFINITION																								
RVP.3.1	3.0 (p.15)	H	Machine-Level ISA																								
RVP.3.2	3.0 (p.15) preface (p.i)	I	Machine Level ISA extension version is 1.12 and status is ratified.																								
RVP.3.3	3.0 (p.15)	I	This chapter describes the machine-level operations available in machine-mode (M-mode), which is the highest privilege mode in a RISC-V system. M-mode is used for low-level access to a hardware platform and is the first mode entered at reset. M-mode can also be used to implement features that are too difficult or expensive to implement in hardware directly. The RISC-V machine-level ISA contains a common core that is extended depending on which other privilege levels are supported and other details of the hardware implementation.																								
RVP.3.4	3.1 (p.15)	H	Machine-Level CSRs																								
RVP.3.5	3.1 (p.15)	R	In addition to the machine-level CSRs described in this section, M-mode code can access all CSRs at lower privilege levels																								
RVP.3.6	3.1.1 (p.15)	H	Machine ISA Register <code>misa</code>																								
RVP.3.7	3.1.1 (p.15)	R	The <code>misa</code> CSR is a WARL read-write register reporting the ISA supported by the hart.																								
RVP.3.8	3.1.1 (p.15)	R	The <code>misa</code> register must be readable in any implementation, but a value of zero can be returned to indicate the <code>misa</code> register has not been implemented, requiring that CPU capabilities be determined through a separate non-standard mechanism.																								
RVP.3.9	3.1.1 (p.15) Figure 3.1	R	The <code>misa</code> register bit fields <table border="1"> <tr> <td>MXLEN-1</td> <td>MXLEN-2</td> <td>MXLEN-3</td> <td>...</td> <td>26</td> <td>25</td> <td>24</td> <td>23</td> <td>...</td> <td>2</td> <td>1</td> <td>0</td> </tr> <tr> <td>MXL[1:0] (WARL)</td> <td colspan="3">0 (WARL)</td> <td colspan="8">Extensions[25:0] (WARL)</td> </tr> </table>	MXLEN-1	MXLEN-2	MXLEN-3	...	26	25	24	23	...	2	1	0	MXL[1:0] (WARL)	0 (WARL)			Extensions[25:0] (WARL)							
MXLEN-1	MXLEN-2	MXLEN-3	...	26	25	24	23	...	2	1	0																
MXL[1:0] (WARL)	0 (WARL)			Extensions[25:0] (WARL)																							
RVP.3.10	3.1.1 (p.15, p.16) Table 3.1	R	The MXL (Machine XLEN) field encodes the native base integer ISA width as shown in the table below <table border="1"> <thead> <tr> <th>MXL</th> <th>XLEN</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>32</td> </tr> <tr> <td>2</td> <td>64</td> </tr> <tr> <td>3</td> <td>128</td> </tr> </tbody> </table>	MXL	XLEN	1	32	2	64	3	128																
MXL	XLEN																										
1	32																										
2	64																										
3	128																										
RVP.3.11	3.1.1 (p.15)	R	The MXL field may be writable in implementations that support multiple base ISAs.																								
RVP.3.12	3.1.1 (p.15)	R	The effective XLEN in M-mode, <code>MXLEN</code> , is given by the setting of MXL, or has a fixed value if <code>misa</code> is zero																								
RVP.3.13	3.1.1 (p.15)	R	The MXL field is always set to the widest supported ISA variant at reset																								
RVP.3.14	3.1.1 (p.16)	R	The <code>misa</code> CSR is MXLEN bits wide.																								
RVP.3.15	3.1.1 (p.16)	R	If the value read from <code>misa</code> is nonzero, field MXL of that value always denotes the current MXLEN.																								
RVP.3.16	3.1.1 (p.16)	R	If a write to <code>misa</code> causes MXLEN to change, the position of MXL moves to the most-significant two bits of <code>misa</code> at the new width																								

ID REFERENCE TYPE DEFINITION

RVP.3.17	3.1.1 (p.16)	C	The base width can be quickly ascertained using branches on the sign of the returned misa value, and possibly a shift left by one and a second branch on the sign. These checks can be written in assembly code without knowing the register width (XLEN) of the machine. The base width is given by $XLEN = 2^{\text{MXL}+4}$.
RVP.3.18	3.1.1 (p.16)	C	The base width can also be found if <code>misa</code> is zero, by placing the immediate 4 in a register then shifting the register left by 31 bits at a time. If zero after one shift, then the machine is RV32. If zero after two shifts, then the machine is RV64, else RV128.
RVP.3.19	3.1.1 (p.16)	R	The Extensions field encodes the presence of the standard extensions, with a single bit per letter of the alphabet (bit 0 encodes presence of extension "A", bit 1 encodes presence of extension "B", through to bit 25 which encodes "Z").
RVP.3.20	3.1.1 (p.16)	R	The "I" bit will be set for RV32I, RV64I, RV128I base ISAs, and the "E" bit will be set for RV32E.
RVP.3.21	3.1.1 (p.16)	R	The Extensions field is a WARL field that can contain writable bits where the implementation allows the supported ISA to be modified.
RVP.3.22	3.1.1 (p.16)	R	At reset, the Extensions field shall contain the maximal set of supported extensions, and I shall be selected over E if both are available.
RVP.3.23	3.1.1 (p.16)	R	When a standard extension is disabled by clearing its bit in misa, the instructions and CSRs defined or modified by the extension revert to their defined or reserved behaviors as if the extension is not implemented.
RVP.3.24	3.1.1 (p.16)	R	The "U" and "S" bits will be set if there is support for user and supervisor modes respectively.
RVP.3.25	3.1.1 (p.16)	R	The "X" bit will be set if there are any non-standard extensions.

ID **REFERENCE TYPE DEFINITION**

RVP.3.26 3.1.1 (p.17) R Encoding of Extensions field in `misa`
 Table 3.2

Bit	Character	Description
0	A	Atomic extension
1	B	Tentatively reserved for Bit-Manipulation extension
2	C	Compressed extension
3	D	Double-precision floating-point extension
4	E	RV32E base ISA
5	F	Single-precision floating-point extension
6	G	Reserved
7	H	Hypervisor extension
8	I	RV32I/64I/128I base ISA
9	J	Tentatively reserved for Dynamically Translated Languages extension
10	K	Reserved
11	L	Reserved
12	M	Integer Multiply/Divide extension
13	N	Tentatively reserved for User-Level Interrupts extension
14	O	Reserved
15	P	Tentatively reserved for Packed-SIMD extension
16	Q	Quad-precision floating-point extension
17	R	Reserved
18	S	Supervisor mode implemented
19	T	Reserved
20	U	User mode implemented
21	V	Tentatively reserved for Vector extension
22	W	Reserved
23	X	Non-standard extensions present
24	Y	Reserved
25	Z	Reserved

RVP.3.27 3.1.1 (p.17) R Bits that are reserved for future use must return zero when read.

RVP.3.28 3.1.1 (p.18) R The “E” bit is read-only. Unless `misa` is all read-only zero, the “E” bit always reads as the complement of the “I” bit. An implementation that supports both RV32E and RV32I can select RV32E by clearing the “I” bit.

RVP.3.29 3.1.1 (p.18) R If an ISA feature *x* depends on an ISA feature *y*, then attempting to enable feature *x* but disable feature *y* results in both features being disabled. For example, setting “F”=0 and “D”=1 results in both “F” and “D” being cleared.

RVP.3.30 3.1.1 (p.18) R An implementation may impose additional constraints on the collective setting of two or more `misa` fields, in which case they function collectively as a single WARL field. An attempt to write an unsupported combination causes those bits to be set to some supported combination

RVP.3.31 3.1.1 (p.18) R Writing `misa` may increase IALIGN, e.g., by disabling the “C” extension. If an instruction that would write `misa` increases IALIGN, and the subsequent instruction’s address is not IALIGN-bit aligned, the write to `misa` is suppressed, leaving `misa` unchanged.

RVP.3.32 3.1.1 (p.18) R When software enables an extension that was previously disabled, then all state uniquely associated with that extension is UNSPECIFIED, unless otherwise specified by that extension

ID	REFERENCE	TYPE	DEFINITION														
RVP.3.33	3.1.2 (p.18)	H	Machine Vendor ID Register <code>mvendorid</code>														
RVP.3.34	3.1.2 (p.18)	R	The <code>mvendorid</code> CSR is a 32-bit read-only register providing the JEDEC manufacturer ID of the provider of the core														
RVP.3.35	3.1.2 (p.18)	R	The <code>mvendorid</code> register must be readable in any implementation, but a value of 0 can be returned to indicate the field is not implemented or that this is a non-commercial implementation														
RVP.3.36	3.1.2 (p.18) Figure 3.2	R	Vendor ID register (<code>mvendorid</code>)														
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>31</td> <td>...</td> <td>7</td> <td>6</td> <td>...</td> <td>0</td> </tr> <tr> <td colspan="4">Bank</td> <td colspan="2">offset</td> </tr> </table>	31	...	7	6	...	0	Bank				offset			
31	...	7	6	...	0												
Bank				offset													
RVP.3.37	3.1.2 (p.18)	R	JEDEC manufacturer IDs are ordinarily encoded as a sequence of one-byte continuation codes <code>0x7f</code> , terminated by a one-byte ID not equal to <code>0x7f</code> , with an odd parity bit in the most-significant bit of each byte. <code>mvendorid</code> encodes the number of one-byte continuation codes in the Bank field, and encodes the final byte in the Offset field, discarding the parity bit. For example, the JEDEC manufacturer ID <code>0x7f 0x7f 0x8a</code> (twelve continuation codes followed by <code>0x8a</code>) would be encoded in the <code>mvendorid</code> CSR as <code>0x60a</code> .														
RVP.3.38	3.1.2 (p.18)	C	In JEDEC's parlance, the bank number is one greater than the number of continuation codes; hence, the <code>mvendorid</code> Bank field encodes a value that is one less than the JEDEC bank number.														
RVP.3.39	3.1.2 (p.18)	C	Previously the vendor ID was to be a number allocated by RISC-V International, but this duplicates the work of JEDEC in maintaining a manufacturer ID standard. At time of writing, registering a manufacturer ID with JEDEC has a one-time cost of \$500.														
RVP.3.40	3.1.3 (p.19)	H	Machine Architecture ID Register <code>marchid</code>														
RVP.3.41	3.1.3 (p.19)	R	The <code>marchid</code> CSR is an MXLEN-bit read-only register encoding the base microarchitecture of the hart.														
RVP.3.42	3.1.3 (p.19)	R	The <code>marchid</code> register must be readable in any implementation, but a value of 0 can be returned to indicate the field is not implemented														
RVP.3.43	3.1.3 (p.19)	I	The combination of <code>mvendorid</code> and <code>marchid</code> should uniquely identify the type of hart microarchitecture that is implemented														
RVP.3.44	3.1.3 (p.19) Figure 3.3	R	Machine Architecture ID register (<code>marchid</code>)														
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>MXLEN-1</td> <td>MXLEN-2</td> <td>...</td> <td>3</td> <td>2</td> <td>1</td> <td>0</td> </tr> <tr> <td colspan="7">Architecture ID</td> </tr> </table>	MXLEN-1	MXLEN-2	...	3	2	1	0	Architecture ID						
MXLEN-1	MXLEN-2	...	3	2	1	0											
Architecture ID																	
RVP.3.45	3.1.3 (p.19)	R	Open-source project architecture IDs are allocated globally by RISC-V International, and have non-zero architecture IDs with a zero most-significant-bit (MSB).														
RVP.3.46	3.1.3 (p.19)	R	Commercial architecture IDs are allocated by each commercial vendor independently, but must have the MSB set and cannot contain zero in the remaining MXLEN-1 bits.														

ID REFERENCE TYPE DEFINITION

RVP.3.47	3.1.3 (p.19)	C	<p>The intent is for the architecture ID to represent the microarchitecture associated with the repo around which development occurs rather than a particular organization. Commercial fabrications of open-source designs should (and might be required by the license to) retain the original architecture ID. This will aid in reducing fragmentation and tool support costs, as well as provide attribution. Open-source architecture IDs are administered by RISC-V International and should only be allocated to released, functioning open-source projects. Commercial architecture IDs can be managed independently by any registered vendor but are required to have IDs disjoint from the open-source architecture IDs (MSB set) to prevent collisions if a vendor wishes to use both closed-source and open-source microarchitectures.</p> <p>The convention adopted within the following Implementation field can be used to segregate branches of the same architecture design, including by organization. The <code>misa</code> register also helps distinguish different variants of a design.</p>														
RVP.3.48	3.1.4 (p.19)	H	Machine Implementation ID Register <code>mimpid</code>														
RVP.3.49	3.1.4 (p.19)	R	The <code>mimpid</code> CSR provides a unique encoding of the version of the processor implementation														
RVP.3.50	3.1.4 (p.19)	R	The <code>mimpid</code> register must be readable in any implementation, but a value of 0 can be returned to indicate that the field is not implemented.														
RVP.3.51	3.1.4 (p.19)	R	The Implementation value should reflect the design of the RISC-V processor itself and not any surrounding system.														
RVP.3.52	3.1.4 (p.19) Figure 3.4	R	Machine Implementation ID register (<code>mimpid</code>).														
			<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">MXLEN-1</td> <td style="padding: 2px;">MXLEN-2</td> <td style="padding: 2px;">...</td> <td style="padding: 2px; border: none;">3</td> <td style="padding: 2px; border: none;">2</td> <td style="padding: 2px; border: none;">1</td> <td style="padding: 2px; border: none;">0</td> </tr> <tr> <td colspan="6" style="padding: 0;"></td> <td style="padding: 2px; border: none;">Implementation</td> </tr> </table>	MXLEN-1	MXLEN-2	...	3	2	1	0							Implementation
MXLEN-1	MXLEN-2	...	3	2	1	0											
						Implementation											
RVP.3.53	3.1.4 (p.19)	C	The format of this field is left to the provider of the architecture source code, but will often be printed by standard tools as a hexadecimal string without any leading or trailing zeros, so the Implementation value can be left-justified (i.e., filled in from most-significant nibble down) with subfields aligned on nibble boundaries to ease human readability.														
RVP.3.54	3.1.5 (p.20)	H	Hart ID Register <code>mhartid</code>														
RVP.3.55	3.1.5 (p.20)	R	The <code>mhartid</code> CSR is an MXLEN-bit read-only register containing the integer ID of the hardware thread running the code.														
RVP.3.56	3.1.5 (p.20)	R	The <code>mhartid</code> register must be readable in any implementation.														
RVP.3.57	3.1.5 (p.20)	R	Hart IDs might not necessarily be numbered contiguously in a multiprocessor system, but at least one hart must have a hart ID of zero.														
RVP.3.58	3.1.5 (p.20)	R	Hart IDs must be unique within the execution environment														
RVP.3.59	3.1.5 (p.20) Figure 3.5	R	Hart ID register (<code>mhartid</code>).														
			<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">MXLEN-1</td> <td style="padding: 2px;">MXLEN-2</td> <td style="padding: 2px;">...</td> <td style="padding: 2px; border: none;">3</td> <td style="padding: 2px; border: none;">2</td> <td style="padding: 2px; border: none;">1</td> <td style="padding: 2px; border: none;">0</td> </tr> <tr> <td colspan="6" style="padding: 0;"></td> <td style="padding: 2px; border: none;">Hart ID</td> </tr> </table>	MXLEN-1	MXLEN-2	...	3	2	1	0							Hart ID
MXLEN-1	MXLEN-2	...	3	2	1	0											
						Hart ID											
RVP.3.60	3.1.5 (p.20)	C	In certain cases, we must ensure exactly one hart runs some code (e.g., at reset), and so require one hart to have a known hart ID of zero.														
RVP.3.61	3.1.5 (p.20)	C	For efficiency, system implementers should aim to reduce the magnitude of the largest hart ID used in a system.														
RVP.3.62	3.1.6 (p.20)	H	Machine Status Registers (<code>mstatus</code> and <code>mstatush</code>)														

ID REFERENCE TYPE DEFINITION

RVP.3.63	3.1.6 (p.20)	R	The <code>mstatus</code> register keeps track of and controls the hart's current operating state.																																		
RVP.3.64	3.1.6 (p.20)	R	The <code>mstatus</code> register is an MXLEN-bit read/write register																																		
RVP.3.65	3.1.6 (p.20)	R	A restricted view of <code>mstatus</code> appears as the <code>sstatus</code> register in the S-level ISA																																		
RVP.3.66	3.1.6 (p.20) Figure 3.6	R	Machine-mode status register (<code>mstatus</code>) for RV32.																																		
			<table border="1"> <tr> <td>31</td><td>30</td><td>29</td><td>28</td><td>27</td><td>26</td><td>25</td><td>24</td><td>23</td><td>22</td><td>21</td><td>20</td><td>19</td><td>18</td><td>17</td> </tr> <tr> <td>SD</td><td colspan="6">WPRI</td><td>TSR</td><td>TW</td><td>TVM</td><td>MXR</td><td>SUM</td><td>MPRV</td><td></td><td></td> </tr> </table>	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	SD	WPRI						TSR	TW	TVM	MXR	SUM	MPRV						
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17																							
SD	WPRI						TSR	TW	TVM	MXR	SUM	MPRV																									
			<table border="1"> <tr> <td>16</td><td>15</td><td>14</td><td>13</td><td>12</td><td>11</td><td>10</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>XS</td><td>FS</td><td>MPP</td><td>VS</td><td>SPP</td><td>MPIE</td><td>UBE</td><td>SPIE</td><td>WPRI</td><td>MIE</td><td>WPRI</td><td>SIE</td><td>WPRI</td><td></td><td></td><td></td><td></td> </tr> </table>	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	XS	FS	MPP	VS	SPP	MPIE	UBE	SPIE	WPRI	MIE	WPRI	SIE	WPRI				
16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0																					
XS	FS	MPP	VS	SPP	MPIE	UBE	SPIE	WPRI	MIE	WPRI	SIE	WPRI																									
RVP.3.67	3.1.6 (p.20, p.21) Figure 3.8	R	Additional machine-mode status register (<code>mstatusush</code>) for RV32																																		
			<table border="1"> <tr> <td>31</td><td>30</td><td colspan="3">...</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td colspan="6">WPRI</td><td>MBE</td><td>SBE</td><td colspan="4">WPRI</td><td></td><td></td> </tr> </table>	31	30	...			7	6	5	4	3	2	1	0	WPRI						MBE	SBE	WPRI												
31	30	...			7	6	5	4	3	2	1	0																									
WPRI						MBE	SBE	WPRI																													
RVP.3.68	3.1.6 (p.20) Figure 3.7	R	Machine-mode status register (<code>mstatus</code>) for RV64.																																		
			<table border="1"> <tr> <td>63</td><td>62</td><td>61</td><td colspan="3">...</td><td>39</td><td>38</td><td>37</td><td>36</td><td>35</td><td>34</td><td>33</td><td>32</td> </tr> <tr> <td>SD</td><td colspan="6">WPRI</td><td>MBE</td><td>SBE</td><td colspan="2">SXL</td><td colspan="3">UXL</td> </tr> </table>	63	62	61	...			39	38	37	36	35	34	33	32	SD	WPRI						MBE	SBE	SXL		UXL								
63	62	61	...			39	38	37	36	35	34	33	32																								
SD	WPRI						MBE	SBE	SXL		UXL																										
			<table border="1"> <tr> <td>31</td><td>30</td><td>29</td><td>28</td><td>27</td><td>26</td><td>25</td><td>24</td><td>23</td><td>22</td><td>21</td><td>20</td><td>19</td><td>18</td><td>17</td> </tr> <tr> <td colspan="8">WPRI</td><td>TSR</td><td>TW</td><td>TVM</td><td>MXR</td><td>SUM</td><td>MPRV</td><td></td> </tr> </table>	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	WPRI								TSR	TW	TVM	MXR	SUM	MPRV					
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17																							
WPRI								TSR	TW	TVM	MXR	SUM	MPRV																								
			<table border="1"> <tr> <td>16</td><td>15</td><td>14</td><td>13</td><td>12</td><td>11</td><td>10</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>XS</td><td>FS</td><td>MPP</td><td>VS</td><td>SPP</td><td>MPIE</td><td>UBE</td><td>SPIE</td><td>WPRI</td><td>MIE</td><td>WPRI</td><td>SIE</td><td>WPRI</td><td></td><td></td><td></td><td></td> </tr> </table>	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	XS	FS	MPP	VS	SPP	MPIE	UBE	SPIE	WPRI	MIE	WPRI	SIE	WPRI				
16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0																					
XS	FS	MPP	VS	SPP	MPIE	UBE	SPIE	WPRI	MIE	WPRI	SIE	WPRI																									
RVP.3.69	3.1.6 (p.20)	R	For RV32 only, <code>mstatusush</code> is a 32-bit read/write register																																		
RVP.3.70	3.1.6 (p.20)	R	Bits 30:4 of <code>mstatusush</code> generally contain the same fields found in bits 62:36 of <code>mstatus</code> for RV64. Fields SD, SXL, and UXL do not exist in <code>mstatusush</code> .																																		
RVP.3.71	3.1.6.1 (p.21)	H	Privilege and Global Interrupt-Enable Stack in <code>mstatus</code> register																																		
RVP.3.72	3.1.6.1 (p.21)	R	Global interrupt-enable bits, MIE and SIE, are provided for M-mode and S-mode respectively. These bits are primarily used to guarantee atomicity with respect to interrupt handlers in the current privilege mode.																																		
RVP.3.73	3.1.6.1 (p.21)	C	The global xIE bits are located in the low-order bits of <code>mstatus</code> , allowing them to be atomically set or cleared with a single CSR instruction.																																		
RVP.3.74	3.1.6.1 (p.21)	R	When a hart is executing in privilege mode x, interrupts are globally enabled when xIE=1 and globally disabled when xIE=0.																																		
RVP.3.75	3.1.6.1 (p.21)	R	(When a hart is executing in privilege mode x) Interrupts for lower-privilege modes, w<x, are always globally disabled regardless of the setting of any global wIE bit for the lower-privilege mode.																																		
RVP.3.76	3.1.6.1 (p.21)	R	(When a hart is executing in privilege mode x) Interrupts for higher-privilege modes, y>x, are always globally enabled regardless of the setting of the global yIE bit for the higher-privilege mode.																																		

ID	REFERENCE	TYPE	DEFINITION
RVP.3.77	3.1.6.1 (p.21)	R	Higher-privilege-level code can use separate per-interrupt enable bits to disable selected higher-privilege-mode interrupts before ceding control to a lower-privilege mode.
RVP.3.78	3.1.6.1 (p.21)	C	A higher-privilege mode y could disable all of its interrupts before ceding control to a lower-privilege mode but this would be unusual as it would leave only a synchronous trap, non-maskable interrupt, or reset as means to regain control of the hart.
RVP.3.79	3.1.6.1 (p.21)	R	To support nested traps, each privilege mode x that can respond to interrupts has a two-level stack of interrupt-enable bits and privilege modes.
RVP.3.80	3.1.6.1 (p.21)	R	$xPIE$ holds the value of the interrupt-enable bit active prior to the trap
RVP.3.81	3.1.6.1 (p.21)	R	xPP holds the previous privilege mode.
RVP.3.82	3.1.6.1 (p.21)	R	The xPP fields can only hold privilege modes up to x , so MPP is two bits wide and SPP is one bit wide.
RVP.3.83	3.1.6.1 (p.21)	R	When a trap is taken from privilege mode y into privilege mode x , $xPIE$ is set to the value of xIE ; xIE is set to 0; and xPP is set to y .
RVP.3.84	3.1.6.1 (p.21)	C	For lower privilege modes, any trap (synchronous or asynchronous) is usually taken at a higher privilege mode with interrupts disabled upon entry. The higher-level trap handler will either service the trap and return using the stacked information, or, if not returning immediately to the interrupted context, will save the privilege stack before re-enabling interrupts, so only one entry per stack is required.
RVP.3.85	3.1.6.1 (p.21)	R	An MRET or SRET instruction is used to return from a trap in M-mode or S-mode respectively.
RVP.3.86	3.1.6.1 (p.21)	R	When executing an xRET instruction, supposing xPP holds the value y , xIE is set to $xPIE$; the privilege mode is changed to y ; $xPIE$ is set to 1; and xPP is set to the least-privileged supported mode (U if U-mode is implemented, else M). If $xPP \neq M$, xRET also sets MPRV=0.
RVP.3.87	3.1.6.1 (p.21)	C	Setting xPP to the least-privileged supported mode on an xRET helps identify software bugs in the management of the two-level privilege-mode stack.
RVP.3.88	3.1.6.1 (p.22)	R	xPP fields are WARL fields that can hold only privilege mode x and any implemented privilege mode lower than x .
RVP.3.89	3.1.6.1 (p.22)	R	If privilege mode x is not implemented, then xPP must be read-only 0.
RVP.3.90	3.1.6.1 (p.22)	C	M-mode software can determine whether a privilege mode is implemented by writing that mode to MPP then reading it back.
RVP.3.91	3.1.6.1 (p.22)	C	If the machine provides only U and M modes, then only a single hardware storage bit is required to represent either 00 or 11 in MPP.
RVP.3.92	3.1.6.2 (p.22)	H	Base ISA Control in <code>mstatus</code> Register
RVP.3.93	3.1.6.2 (p.22)	R	For RV64 systems, the SXL and UXL fields are WARL fields that control the value of XLEN for S-mode and U-mode, respectively.
RVP.3.94	3.1.6.2 (p.22)	R	The encoding of SXL and UXL fields is the same as the MXL field of misa
RVP.3.95	3.1.6.2 (p.22)	R	The effective XLEN in S-mode and U-mode are termed SXLEN and UXLEN, respectively.
RVP.3.96	3.1.6.2 (p.22)	R	For RV32 systems, the SXL and UXL fields do not exist, and SXLEN=32 and UXLEN=32.

ID	REFERENCE	TYPE	DEFINITION
RVP.3.97	3.1.6.2 (p.22)	R	For RV64 systems, if S-mode is not supported, then SXL is read-only zero.
RVP.3.98	3.1.6.2 (p.22)	R	Otherwise (For RV64 systems, if S-mode is supported), it is a WARL field that encodes the current value of SXLEN.
RVP.3.99	3.1.6.2 (p.22)	R	In particular, an implementation may make SXL be a read-only field whose value always ensures that SXLEN=MXLEN
RVP.3.100	3.1.6.2 (p.22)	R	For RV64 systems, if U-mode is not supported, then UXL is read-only zero.
RVP.3.101	3.1.6.2 (p.22)	R	Otherwise (For RV64 systems, if U-mode is supported), it is a WARL field that encodes the current value of UXLEN.
RVP.3.102	3.1.6.2 (p.22)	R	In particular, an implementation may make UXL be a read-only field whose value always ensures that UXLEN=MXLEN or UXLEN=SXLEN.
RVP.3.103	3.1.6.2 (p.22)	R	Whenever XLEN in any mode is set to a value less than the widest supported XLEN, all operations must ignore source operand register bits above the configured XLEN, and must sign-extend results to fill the entire widest supported XLEN in the destination register.
RVP.3.104	3.1.6.2 (p.22)	R	Similarly, pc bits above XLEN are ignored, and when the pc is written, it is sign-extended to fill the widest supported XLEN.
RVP.3.105	3.1.6.2 (p.22)	C	We require that operations always fill the entire underlying hardware registers with defined values to avoid implementation-defined behavior.
RVP.3.106	3.1.6.2 (p.22)	C	To reduce hardware complexity, the architecture imposes no checks that lower-privilege modes have XLEN settings less than or equal to the next-higher privilege mode. In practice, such settings would almost always be a software bug, but machine operation is well-defined even in this case.
RVP.3.107	3.1.6.2 (p.22)	R	If MXLEN is changed from 32 to a wider width, each of mstatus fields SXL and UXL, if not restricted to a single value, gets the value corresponding to the widest supported width not wider than the new MXLEN.
RVP.3.108	3.1.6.3 (p.22)	H	Memory Privilege in mstatus Register
RVP.3.109	3.1.6.3 (p.22)	R	The MPRV (Modify PRiVilege) bit modifies the <i>effective privilege mode</i> , i.e., the privilege level at which loads and stores execute.
RVP.3.110	3.1.6.3 (p.22)	R	When MPRV=0, loads and stores behave as normal, using the translation and protection mechanisms of the current privilege mode.
RVP.3.111	3.1.6.3 (p.22)	R	When MPRV=1, load and store memory addresses are translated and protected, and endianness is applied, as though the current privilege mode were set to MPP.
RVP.3.112	3.1.6.3 (p.23)	R	Instruction address-translation and protection are unaffected by the setting of MPRV.
RVP.3.113	3.1.6.3 (p.23)	R	MPRV is read-only 0 if U-mode is not supported.
RVP.3.114	3.1.6.3 (p.23)	R	An MRET or SRET instruction that changes the privilege mode to a mode less privileged than M also sets MPRV=0.
RVP.3.115	3.1.6.3 (p.23)	R	The MXR (Make eXecutable Readable) bit modifies the privilege with which loads access virtual memory.
RVP.3.116	3.1.6.3 (p.23)	R	When MXR=0, only loads from pages marked readable (R=1 in Figure 4.18) will succeed.
RVP.3.117	3.1.6.3 (p.23)	R	When MXR=1, loads from pages marked either readable or executable (R=1 or X=1) will succeed.

ID	REFERENCE	TYPE	DEFINITION
RVP.3.118	3.1.6.3 (p.23)	R	MXR has no effect when page-based virtual memory is not in effect.
RVP.3.119	3.1.6.3 (p.23)	R	MXR is read-only 0 if S-mode is not supported.
RVP.3.120	3.1.6.3 (p.23)	C	The MPRV and MXR mechanisms were conceived to improve the efficiency of M-mode routines that emulate missing hardware features, e.g., misaligned loads and stores. MPRV obviates the need to perform address translation in software. MXR allows instruction words to be loaded from pages marked execute-only.
RVP.3.121	3.1.6.3 (p.23)	C	The current privilege mode and the privilege mode specified by MPP might have different XLEN settings. When MPRV=1, load and store memory addresses are treated as though the current XLEN were set to MPP's XLEN, following the rules in Section 3.1.6.2.
RVP.3.122	3.1.6.3 (p.23)	R	The SUM (permit Supervisor User Memory access) bit modifies the privilege with which S-mode loads and stores access virtual memory.
RVP.3.123	3.1.6.3 (p.23)	R	When SUM=0, S-mode memory accesses to pages that are accessible by U-mode (U=1 in Figure 4.18) will fault. When SUM=1, these accesses are permitted.
RVP.3.124	3.1.6.3 (p.23)	R	SUM has no effect when page-based virtual memory is not in effect.
RVP.3.125	3.1.6.3 (p.23)	R	Note that, while SUM is ordinarily ignored when not executing in S-mode, it is in effect when MPRV=1 and MPP=S.
RVP.3.126	3.1.6.3 (p.23)	R	SUM is read-only 0 if S-mode is not supported or if satp.MODE is read-only 0.
RVP.3.127	3.1.6.3 (p.23)	R	The MXR and SUM mechanisms only affect the interpretation of permissions encoded in page-table entries. In particular, they have no impact on whether access-fault exceptions are raised due to PMAs or PMP.
RVP.3.128	3.1.6.4 (p.23)	H	Endianness Control in <code>mstatus</code> and <code>mstatush</code> Registers
RVP.3.129	3.1.6.4 (p.23)	R	The MBE, SBE, and UBE bits in <code>mstatus</code> and <code>mstatush</code> are WARL fields that control the endianness of memory accesses other than instruction fetches.
RVP.3.130	3.1.6.4 (p.23)	R	Instruction fetches are always little-endian.
RVP.3.131	3.1.6.4 (p.23)	R	MBE controls whether non-instruction-fetch memory accesses made from M-mode (assuming <code>mstatus.MPRV=0</code>) are little-endian (MBE=0) or big-endian (MBE=1).
RVP.3.132	3.1.6.4 (p.23)	R	If S-mode is not supported, SBE is read-only 0.
RVP.3.133	3.1.6.4 (p.23)	R	Otherwise (If S-mode is supported), SBE controls whether explicit load and store memory accesses made from S-mode are little-endian (SBE=0) or big-endian (SBE=1).
RVP.3.134	3.1.6.4 (p.23)	R	If U-mode is not supported, UBE is read-only 0.
RVP.3.135	3.1.6.4 (p.23)	R	Otherwise (If U-mode is supported), UBE controls whether explicit load and store memory accesses made from U-mode are little-endian (UBE=0) or big-endian (UBE=1).
RVP.3.136	3.1.6.4 (p.23)	R	For <i>implicit</i> accesses to supervisor-level memory management data structures, such as page tables, endianness is always controlled by SBE.
RVP.3.137	3.1.6.4 (p.23, p.24)	R	Since changing SBE alters the implementation's interpretation of these data structures, if any such data structures remain in use across a change to SBE, M-mode software must follow such a change to SBE by executing an SFENCE.VMA instruction with <code>rs1=x0</code> and <code>rs2=x0</code> .

ID REFERENCE TYPE DEFINITION

RVP.3.138	3.1.6.4 (p.24)	C	Only in contrived scenarios will a given memory-management data structure be interpreted as both little-endian and big-endian. In practice, SBE will only be changed at runtime on world switches, in which case neither the old nor new memory-management data structure will be reinterpreted in a different endianness. In this case, no additional SFENCE.VMA is necessary, beyond what would ordinarily be required for a world switch.
RVP.3.139	3.1.6.4 (p.24)	R	If S-mode is supported, an implementation may make SBE be a read-only copy of MBE.
RVP.3.140	3.1.6.4 (p.24)	R	If U-mode is supported, an implementation may make UBE be a read-only copy of either MBE or SBE.
RVP.3.141	3.1.6.4 (p.24)	C	An implementation supports only little-endian memory accesses if fields MBE, SBE, and UBE are all read-only 0. An implementation supports only big-endian memory accesses (aside from instruction fetches) if MBE is read-only 1 and SBE and UBE are each read-only 1 when S-mode and U-mode are supported.
RVP.3.142	3.1.6.4 (p.24)	C	Volume I defines a hart's address space as a circular sequence of 2^{XLEN} bytes at consecutive addresses. The correspondence between addresses and byte locations is fixed and not affected by any endianness mode. Rather, the applicable endianness mode determines the order of mapping between memory bytes and a multibyte quantity (halfword, word, etc.).
RVP.3.143	3.1.6.4 (p.24)	C	Standard RISC-V ABIs are expected to be purely little-endian-only or big-endian-only, with no accommodation for mixing endianness. Nevertheless, endianness control has been defined so as to permit, for instance, an OS of one endianness to execute user-mode programs of the opposite endianness. Consideration has been given also to the possibility of nonstandard usages whereby software flips the endianness of memory accesses as needed.
RVP.3.144	3.1.6.4 (p.24)	C	RISC-V instructions are uniformly little-endian to decouple instruction encoding from the current endianness settings, for the benefit of both hardware and software. Otherwise, for instance, a RISC-V assembler or disassembler would always need to know the intended active endianness, despite that the endianness mode might change dynamically during execution. In contrast, by giving instructions a fixed endianness, it is sometimes possible for carefully written software to be endianness-agnostic even in binary form, much like position-independent code.
RVP.3.145	3.1.6.4 (p.24)	C	The choice to have instructions be only little-endian does have consequences, however, for RISC-V software that encodes or decodes machine instructions. In big-endian mode, such software must account for the fact that explicit loads and stores have endianness opposite that of instructions, for example by swapping byte order after loads and before stores.
RVP.3.146	3.1.6.5 (p.24)	H	Virtualization Support in <code>mstatus</code> Register
RVP.3.147	3.1.6.5 (p.24)	R	The TVM (Trap Virtual Memory) bit is a WARL field that supports intercepting supervisor virtual-memory management operations.
RVP.3.148	3.1.6.5 (p.24)	R	When TVM=1, attempts to read or write the satp CSR or execute an SFENCE.VMA or SINVAL.VMA instruction while executing in S-mode will raise an illegal instruction exception.
RVP.3.149	3.1.6.5 (p.24)	R	When TVM=0, these operations are permitted in S-mode. TVM is read-only 0 when S-mode is not supported.

ID	REFERENCE	TYPE	DEFINITION
RVP.3.150	3.1.6.5 (p.25)	C	The TVM mechanism improves virtualization efficiency by permitting guest operating systems to execute in S-mode, rather than classically virtualizing them in U-mode. This approach obviates the need to trap accesses to most S-mode CSRs.
RVP.3.151	3.1.6.5 (p.25)	C	Trapping <code>satp</code> accesses and the SFENCE.VMA and SINVAL.VMA instructions provides the hooks necessary to lazily populate shadow page tables.
RVP.3.152	3.1.6.5 (p.25)	R	The TW (Timeout Wait) bit is a WARL field that supports intercepting the WFI instruction (see Section 3.3.3).
RVP.3.153	3.1.6.5 (p.25)	R	When TW=0, the WFI instruction may execute in lower privilege modes when not prevented for some other reason.
RVP.3.154	3.1.6.5 (p.25)	R	When TW=1, then if WFI is executed in any less-privileged mode, and it does not complete within an implementation-specific, bounded time limit, the WFI instruction causes an illegal instruction exception.
RVP.3.155	3.1.6.5 (p.25)	R	The time limit may always be 0, in which case WFI always causes an illegal instruction exception in less-privileged modes when TW=1.
RVP.3.156	3.1.6.5 (p.25)	R	TW is read-only 0 when there are no modes less privileged than M.
RVP.3.157	3.1.6.5 (p.25)	C	Trapping the WFI instruction can trigger a world switch to another guest OS, rather than wastefully idling in the current guest.
RVP.3.158	3.1.6.5 (p.25)	R	When S-mode is implemented, then executing WFI in U-mode causes an illegal instruction exception, unless it completes within an implementation-specific, bounded time limit.
RVP.3.159	3.1.6.5 (p.25)	I	A future revision of this specification might add a feature that allows S-mode to selectively permit WFI in U-mode. Such a feature would only be active when TW=0.
RVP.3.160	3.1.6.5 (p.25)	R	The TSR (Trap SRET) bit is a WARL field that supports intercepting the supervisor exception return instruction, SRET.
RVP.3.161	3.1.6.5 (p.25)	R	When TSR=1, attempts to execute SRET while executing in S-mode will raise an illegal instruction exception.
RVP.3.162	3.1.6.5 (p.25)	R	When TSR=0, this operation (SRET) is permitted in S-mode.
RVP.3.163	3.1.6.5 (p.25)	R	TSR is read-only 0 when S-mode is not supported.
RVP.3.164	3.1.6.5 (p.25)	C	Trapping SRET is necessary to emulate the hypervisor extension (see Chapter 8) on implementations that do not provide it.
RVP.3.165	3.1.6.6 (p.25)	H	Extension Context Status in <code>mstatus</code> Register
RVP.3.166	3.1.6.6 (p.25)	R	Supporting substantial extensions is one of the primary goals of RISC-V, and hence we define a standard interface to allow unchanged privileged-mode code, particularly a supervisor-level OS, to support arbitrary user-mode state extensions.
RVP.3.167	3.1.6.6 (p.25)	C	To date, the V extension is the only standard extension that defines additional state beyond the floating-point CSR and data registers.
RVP.3.168	3.1.6.6 (p.25)	R	The FS[1:0] and VS[1:0] WARL fields and the XS[1:0] read-only field are used to reduce the cost of context save and restore by setting and tracking the current state of the floating-point unit and any other user-mode extensions respectively
RVP.3.169	3.1.6.6 (p.25)	R	The FS field encodes the status of the floating-point unit state, including the floating-point registers f0–f31 and the CSRs <code>fcsr</code> , <code>frm</code> , and <code>fflags</code> .

ID REFERENCE TYPE DEFINITION

RVP.3.170	3.1.6.6 (p.25)	R	The VS field encodes the status of the vector extension state, including the vector registers v0–v31 and the CSRs <code>vcsr</code> , <code>vxrm</code> , <code>vxsat</code> , <code>vstart</code> , <code>vl</code> , <code>vtype</code> , and <code>vlenb</code> .															
RVP.3.171	3.1.6.6 (p.25)	R	The XS field encodes the status of additional user-mode extensions and associated state.															
RVP.3.172	3.1.6.6 (p.25, p.26)	R	These fields can be checked by a context switch routine to quickly determine whether a state save or restore is required. If a save or restore is required, additional instructions and CSRs are typically required to effect and optimize the process.															
RVP.3.173	3.1.6.6 (p.26)	C	The design anticipates that most context switches will not need to save/restore state in either or both of the floating-point unit or other extensions, so provides a fast check via the SD bit.															
RVP.3.174	3.1.6.6 (p.26) Table 3.3	R	The FS, VS, and XS fields use the same status encoding as shown in the table below, with the four possible status values being Off, Initial, Clean, and Dirty.															
			<table border="1"> <thead> <tr> <th>Status</th><th>FS and VS Meaning</th><th>XS Meaning</th></tr> </thead> <tbody> <tr> <td>0</td><td>Off</td><td>All off</td></tr> <tr> <td>1</td><td>Initial</td><td>None dirty or clean, some on</td></tr> <tr> <td>2</td><td>Clea</td><td>None dirty, some clean</td></tr> <tr> <td>3</td><td>Dirty</td><td>Some dirty</td></tr> </tbody> </table>	Status	FS and VS Meaning	XS Meaning	0	Off	All off	1	Initial	None dirty or clean, some on	2	Clea	None dirty, some clean	3	Dirty	Some dirty
Status	FS and VS Meaning	XS Meaning																
0	Off	All off																
1	Initial	None dirty or clean, some on																
2	Clea	None dirty, some clean																
3	Dirty	Some dirty																
RVP.3.175	3.1.6.6 (p.26)	R	If the F extension is implemented, the FS field shall not be read-only zero.															
RVP.3.176	3.1.6.6 (p.26)	R	If neither the F extension nor S-mode is implemented, then FS is read-only zero.															
RVP.3.177	3.1.6.6 (p.26)	R	If S-mode is implemented but the F extension is not, FS may optionally be read-only zero.															
RVP.3.178	3.1.6.6 (p.26)	C	Implementations with S-mode but without the F extension are permitted, but not required, to make the FS field be read-only zero. Some such implementations will choose not to have the FS field be read-only zero, so as to enable emulation of the F extension for both S-mode and U-mode via invisible traps into M-mode.															
RVP.3.179	3.1.6.6 (p.26)	R	If the v registers are implemented, the VS field shall not be read-only zero.															
RVP.3.180	3.1.6.6 (p.26)	R	If neither the v registers nor S-mode is implemented, then VS is read-only zero.															
RVP.3.181	3.1.6.6 (p.26)	R	If S-mode is implemented but the v registers are not, VS may optionally be read-only zero.															
RVP.3.182	3.1.6.6 (p.26)	R	In systems without additional user extensions requiring new state, the XS field is read-only zero.															
RVP.3.183	3.1.6.6 (p.26)	R	Every additional extension with state provides a CSR field that encodes the equivalent of the XS states. The XS field represents a summary of all extensions' status															
RVP.3.184	3.1.6.6 (p.26)	C	The XS field effectively reports the maximum status value across all user-extension status fields, though individual extensions can use a different encoding than XS.															
RVP.3.185	3.1.6.6 (p.26)	R	The SD bit is a read-only bit that summarizes whether either the FS, VS, or XS fields signal the presence of some dirty state that will require saving extended user context to memory.															
RVP.3.186	3.1.6.6 (p.26)	R	If FS, XS, and VS are all read-only zero, then SD is also always zero.															

ID	REFERENCE	TYPE	DEFINITION
RVP.3.187	3.1.6.6 (p.26)	R	When an extension's status is set to Off, any instruction that attempts to read or write the corresponding state will cause an illegal instruction exception.
RVP.3.188	3.1.6.6 (p.26)	R	When the status is Initial, the corresponding state should have an initial constant value.
RVP.3.189	3.1.6.6 (p.26)	R	When the status is Clean, the corresponding state is potentially different from the initial value, but matches the last value stored on a context swap.
RVP.3.190	3.1.6.6 (p.26)	R	When the status is Dirty, the corresponding state has potentially been modified since the last context save.
RVP.3.191	3.1.6.6 (p.27)	R	During a context save, the responsible privileged code need only write out the corresponding state if its status is Dirty, and can then reset the extension's status to Clean.
RVP.3.192	3.1.6.6 (p.27)	R	During a context restore, the context need only be loaded from memory if the status is Clean (it should never be Dirty at restore).
RVP.3.193	3.1.6.6 (p.27)	R	If the status is Initial, the context must be set to an initial constant value on context restore to avoid a security hole, but this can be done without accessing memory. For example, the floating-point registers can all be initialized to the immediate value 0.
RVP.3.194	3.1.6.6 (p.27)	R	The FS and XS fields are read by the privileged code before saving the context.
RVP.3.195	3.1.6.6 (p.27)	R	The FS field is set directly by privileged code when resuming a user context.
RVP.3.196	3.1.6.6 (p.27)	R	While (when resuming a user context) the XS field is set indirectly by writing to the status register of the individual extensions.
RVP.3.197	3.1.6.6 (p.27)	R	The status fields will also be updated during execution of instructions, regardless of privilege mode.
RVP.3.198	3.1.6.6 (p.27)	R	Extensions to the user-mode ISA often include additional user-mode state, and this state can be considerably larger than the base integer registers.
RVP.3.199	3.1.6.6 (p.27)	R	The extensions might only be used for some applications, or might only be needed for short phases within a single application.
RVP.3.200	3.1.6.6 (p.27)	R	To improve performance, the user-mode extension can define additional instructions to allow user-mode software to return the unit to an initial state or even to turn off the unit.
RVP.3.201	3.1.6.6 (p.27)	I	For example, a coprocessor might require to be configured before use and can be "unconfigured" after use. The unconfigured state would be represented as the Initial state for context save. If the same application remains running between the unconfigure and the next configure (which would set status to Dirty), there is no need to actually reinitialize the state at the unconfigure instruction, as all state is local to the user process, i.e., the Initial state may only cause the coprocessor state to be initialized to a constant value at context restore, not at every unconfigure.
RVP.3.202	3.1.6.6 (p.27)	R	Executing a user-mode instruction to disable a unit and place it into the Off state will cause an illegal instruction exception to be raised if any subsequent instruction tries to use the unit before it is turned back on.
RVP.3.203	3.1.6.6 (p.27)	R	A user-mode instruction to turn a unit on must also ensure the unit's state is properly initialized, as the unit might have been used by another context meantime.

ID REFERENCE TYPE DEFINITION

RVP.3.204	3.1.6.6 (p.27)	R	Changing the setting of FS has no effect on the contents of the floating-point register state. In particular, setting FS=Off does not destroy the state, nor does setting FS=Initial clear the contents.															
RVP.3.205	3.1.6.6 (p.27)	R	Similarly, the setting of VS has no effect on the contents of the vector register state.															
RVP.3.206	3.1.6.6 (p.27)	R	Other extensions, however, might not preserve state when set to Off.															
RVP.3.207	3.1.6.6 (p.27)	R	Implementations may choose to track the dirtiness of the floating-point register state imprecisely by reporting the state to be dirty even when it has not been modified.															
RVP.3.208	3.1.6.6 (p.27)	R	On some implementations, some instructions that do not mutate the floating-point state may cause the state to transition from Initial or Clean to Dirty.															
RVP.3.209	3.1.6.6 (p.27)	R	On other implementations, dirtiness might not be tracked at all, in which case the valid FS states are Off and Dirty, and an attempt to set FS to Initial or Clean causes it to be set to Dirty.															
RVP.3.210	3.1.6.6 (p.27)	C	This definition of FS does not disallow setting FS to Dirty as a result of errant speculation. Some platforms may choose to disallow speculatively writing FS to close a potential side channel.															
RVP.3.211	3.1.6.6 (p.27)	R	If an instruction explicitly or implicitly writes a floating-point register or the fcsr but does not alter its contents, and FS=Initial or FS=Clean, it is implementation-defined whether FS transitions to Dirty.															
RVP.3.212	3.1.6.6 (p.28)	R	Implementations may choose to track the dirtiness of the vector register state in an analogous imprecise fashion, including possibly setting VS to Dirty when software attempts to set VS=Initial or VS=Clean. When VS=Initial or VS=Clean, it is implementation-defined whether an instruction that writes a vector register or vector CSR but does not alter its contents causes VS to transition to Dirty.															
RVP.3.213	3.1.6.6 (p.28)	R Table 3.4	All the possible state transitions for the FS, VS, or XS status bits: At context save in privileged code															
			<table border="1"> <thead> <tr> <th>Current State</th><th>Off</th><th>Initial</th><th>Clean</th><th>Dirty</th></tr> </thead> <tbody> <tr> <td>Save State?</td><td>No</td><td>No</td><td>No</td><td>Yes</td></tr> <tr> <td>Next State</td><td>Off</td><td>Initial</td><td>Clean</td><td>Clean</td></tr> </tbody> </table>	Current State	Off	Initial	Clean	Dirty	Save State?	No	No	No	Yes	Next State	Off	Initial	Clean	Clean
Current State	Off	Initial	Clean	Dirty														
Save State?	No	No	No	Yes														
Next State	Off	Initial	Clean	Clean														
RVP.3.214	3.1.6.6 (p.28)	R Table 3.4	All the possible state transitions for the FS, VS, or XS status bits: At context restore in privileged code															
			<table border="1"> <thead> <tr> <th>Current State</th><th>Off</th><th>Initial</th><th>Clean</th><th>Dirty</th></tr> </thead> <tbody> <tr> <td>Restore State?</td><td>No</td><td>Yes, to Initial</td><td>Yes, from memory</td><td>N/A</td></tr> <tr> <td>Next State</td><td>Off</td><td>Initial</td><td>Clean</td><td>N/A</td></tr> </tbody> </table>	Current State	Off	Initial	Clean	Dirty	Restore State?	No	Yes, to Initial	Yes, from memory	N/A	Next State	Off	Initial	Clean	N/A
Current State	Off	Initial	Clean	Dirty														
Restore State?	No	Yes, to Initial	Yes, from memory	N/A														
Next State	Off	Initial	Clean	N/A														
RVP.3.215	3.1.6.6 (p.28)	R Table 3.4	All the possible state transitions for the FS, VS, or XS status bits: Execute instruction to read state															
			<table border="1"> <thead> <tr> <th>Current State</th><th>Off</th><th>Initial</th><th>Clean</th><th>Dirty</th></tr> </thead> <tbody> <tr> <td>Action?</td><td>Exception</td><td>Execute</td><td>Execute</td><td>Execute</td></tr> <tr> <td>Next State</td><td>Off</td><td>Initial</td><td>Clean</td><td>Dirty</td></tr> </tbody> </table>	Current State	Off	Initial	Clean	Dirty	Action?	Exception	Execute	Execute	Execute	Next State	Off	Initial	Clean	Dirty
Current State	Off	Initial	Clean	Dirty														
Action?	Exception	Execute	Execute	Execute														
Next State	Off	Initial	Clean	Dirty														
RVP.3.216	3.1.6.6 (p.28)	R Table 3.4	All the possible state transitions for the FS, VS, or XS status bits: Execute instruction that possibly modifies state, including configuration															
			<table border="1"> <thead> <tr> <th>Current State</th><th>Off</th><th>Initial</th><th>Clean</th><th>Dirty</th></tr> </thead> <tbody> <tr> <td>Action?</td><td>Exception</td><td>Execute</td><td>Execute</td><td>Execute</td></tr> <tr> <td>Next State</td><td>Off</td><td>Dirty</td><td>Dirty</td><td>Dirty</td></tr> </tbody> </table>	Current State	Off	Initial	Clean	Dirty	Action?	Exception	Execute	Execute	Execute	Next State	Off	Dirty	Dirty	Dirty
Current State	Off	Initial	Clean	Dirty														
Action?	Exception	Execute	Execute	Execute														
Next State	Off	Dirty	Dirty	Dirty														

ID REFERENCE TYPE DEFINITION

RVP.3.217	3.1.6.6 (p.28)	R	All the possible state transitions for the FS, VS, or XS status bits: Execute instruction to unconfigure unit															
		Table 3.4	<table border="1"> <thead> <tr> <th>Current State</th><th>Off</th><th>Initial</th><th>Clean</th><th>Dirty</th></tr> </thead> <tbody> <tr> <td>Action?</td><td>Exception</td><td>Execute</td><td>Execute</td><td>Execute</td></tr> <tr> <td>Next State</td><td>Off</td><td>Initial</td><td>Initial</td><td>Initial</td></tr> </tbody> </table>	Current State	Off	Initial	Clean	Dirty	Action?	Exception	Execute	Execute	Execute	Next State	Off	Initial	Initial	Initial
Current State	Off	Initial	Clean	Dirty														
Action?	Exception	Execute	Execute	Execute														
Next State	Off	Initial	Initial	Initial														
RVP.3.218	3.1.6.6 (p.28)	R	All the possible state transitions for the FS, VS, or XS status bits: Execute instruction to disable unit															
		Table 3.4	<table border="1"> <thead> <tr> <th>Current State</th><th>Off</th><th>Initial</th><th>Clean</th><th>Dirty</th></tr> </thead> <tbody> <tr> <td>Action?</td><td>Execute</td><td>Execute</td><td>Execute</td><td>Execute</td></tr> <tr> <td>Next State</td><td>Off</td><td>Off</td><td>Off</td><td>Off</td></tr> </tbody> </table>	Current State	Off	Initial	Clean	Dirty	Action?	Execute	Execute	Execute	Execute	Next State	Off	Off	Off	Off
Current State	Off	Initial	Clean	Dirty														
Action?	Execute	Execute	Execute	Execute														
Next State	Off	Off	Off	Off														
RVP.3.219	3.1.6.6 (p.28)	R	All the possible state transitions for the FS, VS, or XS status bits: Execute instruction to enable unit															
		Table 3.4	<table border="1"> <thead> <tr> <th>Current State</th><th>Off</th><th>Initial</th><th>Clean</th><th>Dirty</th></tr> </thead> <tbody> <tr> <td>Action?</td><td>Execute</td><td>Execute</td><td>Execute</td><td>Execute</td></tr> <tr> <td>Next State</td><td>Initial</td><td>Initial</td><td>Initial</td><td>Initial</td></tr> </tbody> </table>	Current State	Off	Initial	Clean	Dirty	Action?	Execute	Execute	Execute	Execute	Next State	Initial	Initial	Initial	Initial
Current State	Off	Initial	Clean	Dirty														
Action?	Execute	Execute	Execute	Execute														
Next State	Initial	Initial	Initial	Initial														
RVP.3.220	3.1.6.6 (p.28)	R	Note that the standard floating-point and vector extensions do not support user-mode unconfigure or disable/enable instructions.															
RVP.3.221	3.1.6.6 (p.28)	R	Standard privileged instructions to initialize, save, and restore extension state are provided to insulate privileged code from details of the added extension state by treating the state as an opaque object.															
RVP.3.222	3.1.6.6 (p.28)	C	Many coprocessor extensions are only used in limited contexts that allows software to safely unconfigure or even disable units when done. This reduces the context-switch overhead of large stateful coprocessors.															
RVP.3.223	3.1.6.6 (p.28)	C	We separate out floating-point state from other extension state, as when a floating-point unit is present the floating-point registers are part of the standard calling convention, and so user-mode software cannot know when it is safe to disable the floating-point unit.															
RVP.3.224	3.1.6.6 (p.29)	R	The XS field provides a summary of all added extension state, but additional microarchitectural bits might be maintained in the extension to further reduce context save and restore overhead.															
RVP.3.225	3.1.6.6 (p.29)	R	The SD bit is read-only and is set when either the FS, VS, or XS bits encode a Dirty state (i.e., $SD=((FS==11) \text{ OR } (XS==11) \text{ OR } (VS==11))$). This allows privileged code to quickly determine when no additional context save is required beyond the integer register set and PC.															
RVP.3.226	3.1.6.6 (p.29)	R	The floating-point unit state is always initialized, saved, and restored using standard instructions (F, D, and/or Q), and privileged code must be aware of FLEN to determine the appropriate space to reserve for each f register.															
RVP.3.227	3.1.6.6 (p.29)	R	Machine and Supervisor modes share a single copy of the FS, VS, and XS bits.															
RVP.3.228	3.1.6.6 (p.29)	R	Supervisor-level software normally uses the FS, VS, and XS bits directly to record the status with respect to the supervisor-level saved context.															
RVP.3.229	3.1.6.6 (p.29)	R	Machine-level software must be more conservative in saving and restoring the extension state in their corresponding version of the context.															
RVP.3.230	3.1.6.6 (p.29)	C	In any reasonable use case, the number of context switches between user and supervisor level should far outweigh the number of context switches to other privilege levels. Note that coprocessors should not require their context to be saved and restored to service asynchronous interrupts, unless the interrupt results in a user-level context swap.															

ID REFERENCE TYPE DEFINITION

- RVP.3.231 3.1.7 (p.29) H Machine Trap-Vector Base-Address Register (`mtvec`)
- RVP.3.232 3.1.7 (p.29) R The `mtvec` (machine trap-vector base-address) register is an MXLEN-bit WARL read/write register that holds trap vector configuration, consisting of a vector base address (BASE) and a vector mode (MODE).
- RVP.3.233 3.1.7 (p.29)
Figure 3.9 R Machine trap-vector base-address register (`mtvec`)
- | | | | | |
|-----------------|-----|---|------|---|
| MXLEN-1 | ... | 2 | 1 | 0 |
| BASE[MXLEN-1:2] | | | MODE | |
- RVP.3.234 3.1.7 (p.29) R The `mtvec` register must always be implemented, but can contain a read-only value.
- RVP.3.235 3.1.7 (p.29) R If `mtvec` is writable, the set of values the register may hold can vary by implementation.
- RVP.3.236 3.1.7 (p.29) R The value in the BASE field must always be aligned on a 4-byte boundary, and the MODE setting may impose additional alignment constraints on the value in the BASE field.
- RVP.3.237 3.1.7 (p.29) R BASE field is a WARL field.
- RVP.3.238 3.1.7 (p.29) R MODE field is a WARL field.
- RVP.3.239 3.1.7 (p.29) C We allow for considerable flexibility in implementation of the trap vector base address. On the one hand, we do not wish to burden low-end implementations with a large number of state bits, but on the other hand, we wish to allow flexibility for larger systems.
- RVP.3.240 3.1.7 (p.29)
Table 3.5 R Encoding of `mtvec` MODE field
- | Value | Name | Description |
|----------|----------|---|
| 0 | Direct | All exceptions set pc to BASE |
| 1 | Vectored | Asynchronous interrupts set pc to BASE+4×cause. |
| ≥ 2 | - | Reserved |
- RVP.3.241 3.1.7 (p.30) R When MODE=Direct, all traps into machine mode cause the pc to be set to the address in the BASE field.
- RVP.3.242 3.1.7 (p.30) R When MODE=Vectored, all synchronous exceptions into machine mode cause the pc to be set to the address in the BASE field, whereas interrupts cause the pc to be set to the address in the BASE field plus four times the interrupt cause number.
- RVP.3.243 3.1.7 (p.30) I For example, a machine-mode timer interrupt (see Table 3.6 on page 39) causes the `pc` to be set to BASE+0x1c.
- RVP.3.244 3.1.7 (p.30) C When vectored interrupts are enabled, interrupt cause 0, which corresponds to user-mode software interrupts, are vectored to the same location as synchronous exceptions. This ambiguity does not arise in practice, since user-mode software interrupts are either disabled or delegated to user mode.
- RVP.3.245 3.1.7 (p.30) R An implementation may have different alignment constraints for different modes. In particular, MODE=Vectored may have stricter alignment constraints than MODE=Direct.
- RVP.3.246 3.1.7 (p.30) C Allowing coarser alignments in Vectored mode enables vectoring to be implemented without a hardware adder circuit.
- RVP.3.247 3.1.7 (p.30) C Reset and NMI vector locations are given in a platform specification.
- RVP.3.248 3.1.8 (p.30) H Machine Trap Delegation Registers (`medeleg` and `mideleg`)

ID	REFERENCE	TYPE	DEFINITION
RVP.3.249	3.1.8 (p.30)	R	By default, all traps at any privilege level are handled in machine mode, though a machine-mode handler can redirect traps back to the appropriate level with the MRET instruction (Section 3.3.2).
RVP.3.250	3.1.8 (p.30)	R	To increase performance, implementations can provide individual read/write bits within <code>medeleg</code> (machine exception delegation register) and <code>mideleg</code> (machine interrupt delegation register) to indicate that certain exceptions and interrupts should be processed directly by a lower privilege level.
RVP.3.251	3.1.8 (p.30)	R	The machine exception delegation register (<code>medeleg</code>) is a MXLEN-bit read/write (WARL) register.
RVP.3.252	3.1.8 (p.30)	R	The machine interrupt delegation register (<code>mideleg</code>) is a MXLEN-bit read/write (WARL) register.
RVP.3.253	3.1.8 (p.30)	R	In systems with S-mode, the <code>medeleg</code> and <code>mideleg</code> registers must exist, and setting a bit in <code>medeleg</code> or <code>mideleg</code> will delegate the corresponding trap, when occurring in S-mode or U-mode, to the Smode trap handler.
RVP.3.254	3.1.8 (p.30)	R	In systems without S-mode, the <code>medeleg</code> and <code>mideleg</code> registers should not exist.
RVP.3.255	3.1.8 (p.30)	C	In versions 1.9.1 and earlier, these registers existed but were hardwired to zero in M-mode only, or M/U without N systems. There is no reason to require they return zero in those cases, as the <code>misa</code> register indicates whether they exist.
RVP.3.256	3.1.8 (p.30)	R	When a trap is delegated to S-mode, the <code>scause</code> register is written with the trap cause;
RVP.3.257	3.1.8 (p.30)	R	(When a trap is delegated to S-mode) the <code>sepc</code> register is written with the virtual address of the instruction that took the trap;
RVP.3.258	3.1.8 (p.30)	R	(When a trap is delegated to S-mode) the <code>stval</code> register is written with an exception-specific datum;
RVP.3.259	3.1.8 (p.30)	R	(When a trap is delegated to S-mode) the SPP field of <code>mstatus</code> is written with the active privilege mode at the time of the trap;
RVP.3.260	3.1.8 (p.30)	R	(When a trap is delegated to S-mode) the SPIE field of <code>mstatus</code> is written with the value of the SIE field at the time of the trap;
RVP.3.261	3.1.8 (p.30)	R	(When a trap is delegated to S-mode) and the SIE field of <code>mstatus</code> is cleared.
RVP.3.262	3.1.8 (p.30)	R	(When a trap is delegated to S-mode) The <code>mcause</code> , <code>mepc</code> , and <code>mtval</code> registers and the MPP and MPIE fields of <code>mstatus</code> are not written.
RVP.3.263	3.1.8 (p.31)	R	An implementation can choose to subset the delegatable traps, with the supported delegatable bits found by writing one to every bit location, then reading back the value in <code>medeleg</code> or <code>mideleg</code> to see which bit positions hold a one.
RVP.3.264	3.1.8 (p.31)	R	An implementation shall not have any bits of <code>medeleg</code> be read-only one, i.e., any synchronous trap that can be delegated must support not being delegated.
RVP.3.265	3.1.8 (p.31)	R	Similarly, an implementation shall not fix as read-only one any bits of <code>mideleg</code> corresponding to machine-level interrupts (but may do so for lower-level interrupts).
RVP.3.266	3.1.8 (p.31)	C	Version 1.11 and earlier prohibited having any bits of <code>mideleg</code> be read-only one. Platform standards may always add such restrictions.

ID REFERENCE TYPE DEFINITION

- RVP.3.267 3.1.8 (p.31) R Traps never transition from a more-privileged mode to a less-privileged mode.
- RVP.3.268 3.1.8 (p.31) I For example, if M-mode has delegated illegal instruction exceptions to S-mode, and M-mode software later executes an illegal instruction, the trap is taken in M-mode, rather than being delegated to S-mode.
- RVP.3.269 3.1.8 (p.31) R By contrast, traps may be taken horizontally.
- RVP.3.270 3.1.8 (p.31) I Using the same example, if M-mode has delegated illegal instruction exceptions to S-mode, and S-mode software later executes an illegal instruction, the trap is taken in S-mode.
- RVP.3.271 3.1.8 (p.31) R Delegated interrupts result in the interrupt being masked at the delegator privilege level.
- RVP.3.272 3.1.8 (p.31) I For example, if the supervisor timer interrupt (STI) is delegated to S-mode by setting `mideleg[5]`, STIs will not be taken when executing in M-mode. By contrast, if `mideleg[5]` is clear, STIs can be taken in any mode and regardless of current mode will transfer control to M-mode.
- RVP.3.273 3.1.8 (p.31) R `medeleg` has a bit position allocated for every synchronous exception shown in RVP.3.389, with the index of the bit position equal to the value returned in the `mcause` register (i.e., setting bit 8 allows user-mode environment calls to be delegated to a lower-privilege trap handler).
- RVP.3.274 3.1.8 (p.31)
Figure 3.10 R Machine Exception Delegation Register `medeleg`

MXLEN-1	...	0
Synchronous Exceptions (WARL)		
- RVP.3.275 3.1.8 (p.31) R `mideleg` holds trap delegation bits for individual interrupts, with the layout of bits matching those in the `mip` register (i.e., STIP interrupt delegation control is located in bit 5).
- RVP.3.276 3.1.8 (p.31)
Figure 3.11 R Machine Interrupt Delegation Register `mideleg`.

MXLEN-1	...	0
Interrupts (WARL)		
- RVP.3.277 3.1.8 (p.31) R For exceptions that cannot occur in less privileged modes, the corresponding `medeleg` bits should be read-only zero. In particular, `medeleg[11]` is read-only zero.
- RVP.3.278 3.1.9 (p.31) H Machine Interrupt Registers (`mip` and `mie`)
- RVP.3.279 3.1.9 (p.31) R The `mip` (Machine Interrupt-Pending) register is an MXLEN-bit read/write (WARL) register containing information on pending interrupts, ...
- RVP.3.280 3.1.9 (p.31) R ... while `mie` (Machine Interrupt-Enable) register is the corresponding MXLEN-bit read/write (WARL) register containing interrupt enable bits.
- RVP.3.281 3.1.9 (p.32) R Interrupt cause number *i* (as reported in CSR `mcause`, Section 3.1.15) corresponds with bit *i* in both `mip` and `mie`.
- RVP.3.282 3.1.9 (p.32) R Bits 15:0 (of `mip` and `mie`) are allocated to standard interrupt causes only, while bits 16 and above are designated for platform or custom use.
- RVP.3.283 3.1.9 (p.32)
Figure 3.12 R Machine Interrupt-Pending Register (`mip`).

MXLEN-1	...	0
Interrupts (WARL)		

ID REFERENCE TYPE DEFINITION

- RVP.3.284 3.1.9 (p.32)
Figure 3.13 R Machine Interrupt-Enable Register (`mie`).

MXLEN-1	...	0
Interrupts (WARL)		
- RVP.3.285 3.1.9 (p.32) R An interrupt i will trap to M-mode (causing the privilege mode to change to M-mode) if all of the following are true:
 (a) either the current privilege mode is M and the MIE bit in the `mstatus` register is set, or the current privilege mode has less privilege than M-mode;
 (b) bit i is set in both `mip` and `mie`; and
 (c) if register `mideleg` exists, bit i is not set in `mideleg`.
- RVP.3.286 3.1.9 (p.32) R These conditions for an interrupt trap to occur must be evaluated in a bounded amount of time from when an interrupt becomes, or ceases to be, pending in `mip`, and must also be evaluated immediately following the execution of an `xRET` instruction or an explicit write to a CSR on which these interrupt trap conditions expressly depend (including `mip`, `mie`, `mstatus`, and `mideleg`).
- RVP.3.287 3.1.9 (p.32) R Interrupts to M-mode take priority over any interrupts to lower privilege modes.
- RVP.3.288 3.1.9 (p.32) R Each individual bit in register `mip` may be writable or may be read-only.
- RVP.3.289 3.1.9 (p.32) R When bit i in `mip` is writable, a pending interrupt i can be cleared by writing 0 to this bit.
- RVP.3.290 3.1.9 (p.32) R If interrupt i can become pending but bit i in `mip` is read-only, the implementation must provide some other mechanism for clearing the pending interrupt.
- RVP.3.291 3.1.9 (p.32) R A bit in `mie` must be writable if the corresponding interrupt can ever become pending.
- RVP.3.292 3.1.9 (p.32) R Bits of `mie` that are not writable must be read-only zero.
- RVP.3.293 3.1.9 (p.32)
Figure 3.14 R The standard portions (bits 15:0) of registers `mip` are formatted as shown below

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	MEIP	0	SEIP	0	MTIP	0	STIP	0	MSIP	0	SSIP	0
- RVP.3.294 3.1.9 (p.32)
Figure 3.15 R The standard portions (bits 15:0) of registers `mie` are formatted as shown below

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	MEIE	0	SEIE	0	MTIE	0	STIE	0	MSIE	0	SSIE	0
- RVP.3.295 3.1.9 (p.32) C The machine-level interrupt registers handle a few root interrupt sources which are assigned a fixed service priority for simplicity, while separate external interrupt controllers can implement a more complex prioritization scheme over a much larger set of interrupts that are then muxed into the machine-level interrupt sources.
- RVP.3.296 3.1.9 (p.32) C The non-maskable interrupt is not made visible via the `mip` register as its presence is implicitly known when executing the NMI trap handler.
- RVP.3.297 3.1.9 (p.33) R Bits `mip.MEIP` and `mie.MEIE` are the interrupt-pending and interrupt-enable bits for machine level external interrupts.

ID	REFERENCE	TYPE	DEFINITION
RVP.3.298	3.1.9 (p.33)	R	MEIP is read-only in <code>mip</code> , and is set and cleared by a platform-specific interrupt controller.
RVP.3.299	3.1.9 (p.33)	R	Bits <code>mip.MTIP</code> and <code>mie.MTIE</code> are the interrupt-pending and interrupt-enable bits for machine timer interrupts.
RVP.3.300	3.1.9 (p.33)	R	MTIP is read-only in <code>mip</code> , and is cleared by writing to the memory-mapped machine-mode timer compare register.
RVP.3.301	3.1.9 (p.33)	R	Bits <code>mip.MSIP</code> and <code>mie.MSIE</code> are the interrupt-pending and interrupt-enable bits for machine level software interrupts.
RVP.3.302	3.1.9 (p.33)	R	MSIP is read-only in <code>mip</code> , and is written by accesses to memory-mapped control registers, which are used by remote harts to provide machine-level interprocessor interrupts.
RVP.3.303	3.1.9 (p.33)	R	A hart can write its own MSIP bit using the same memory-mapped control register.
RVP.3.304	3.1.9 (p.33)	R	If a system has only one hart, or if a platform standard supports the delivery of machine-level interprocessor interrupts through external interrupts (MEI) instead, then <code>mip.MSIP</code> and <code>mie.MSIE</code> may both be read-only zeros.
RVP.3.305	3.1.9 (p.33)	R	If supervisor mode is not implemented, bits SEIP, STIP, and SSIP of <code>mip</code> and SEIE, STIE, and SSIE of <code>mie</code> are read-only zeros.
RVP.3.306	3.1.9 (p.33)	R	If supervisor mode is implemented, bits <code>mip.SEIP</code> and <code>mie.SEIE</code> are the interrupt-pending and interrupt-enable bits for supervisor-level external interrupts.
RVP.3.307	3.1.9 (p.33)	R	SEIP is writable in <code>mip</code> , and may be written by M-mode software to indicate to S-mode that an external interrupt is pending.
RVP.3.308	3.1.9 (p.33)	R	Additionally, the platform-level interrupt controller may generate supervisor-level external interrupts.
RVP.3.309	3.1.9 (p.33)	R	Supervisor-level external interrupts are made pending based on the logical-OR of the software-writable SEIP bit and the signal from the external interrupt controller.
RVP.3.310	3.1.9 (p.33)	R	When <code>mip</code> is read with a CSR instruction, the value of the SEIP bit returned in the <code>rd</code> destination register is the logical-OR of the software-writable bit and the interrupt signal from the interrupt controller, but the signal from the interrupt controller is not used to calculate the value written to SEIP. Only the software-writable SEIP bit participates in the read-modify-write sequence of a CSRRS or CSRRRC instruction.
RVP.3.311	3.1.9 (p.33)	C	For example, if we name the software-writable SEIP bit B and the signal from the external interrupt controller E, then if <code>csrrs t0, mip, t1</code> is executed, <code>t0[9]</code> is written with <code>B E</code> , then B is written with <code>B t1[9]</code> . If <code>csrrw t0, mip, t1</code> is executed, then <code>t0[9]</code> is written with <code>B E</code> , and B is simply written with <code>t1[9]</code> . In neither case does B depend upon E.
RVP.3.312	3.1.9 (p.33)	C	The SEIP field behavior is designed to allow a higher privilege layer to mimic external interrupts cleanly, without losing any real external interrupts. The behavior of the CSR instructions is slightly modified from regular CSR accesses as a result.
RVP.3.313	3.1.9 (p.34)	R	If supervisor mode is implemented, bits <code>mip.STIP</code> and <code>mie.STIE</code> are the interrupt-pending and interrupt-enable bits for supervisor-level timer interrupts.

ID	REFERENCE	TYPE	DEFINITION
RVP.3.314	3.1.9 (p.34)	R	STIP is writable in <code>mip</code> , and may be written by M-mode software to deliver timer interrupts to S-mode.
RVP.3.315	3.1.9 (p.34)	R	If supervisor mode is implemented, bits <code>mip.SSIP</code> and <code>mie.SSIE</code> are the interrupt-pending and interrupt-enable bits for supervisor-level software interrupts.
RVP.3.316	3.1.9 (p.34)	R	SSIP is writable in <code>mip</code> and may also be set to 1 by a platform-specific interrupt controller.
RVP.3.317	3.1.9 (p.34)	R	Multiple simultaneous interrupts destined for M-mode are handled in the following decreasing priority order: MEI, MSI, MTI, SEI, SSI, STI.
RVP.3.318	3.1.9 (p.34)	C	The machine-level interrupt fixed-priority ordering rules were developed with the following rationale. Interrupts for higher privilege modes must be serviced before interrupts for lower privilege modes to support preemption. The platform-specific machine-level interrupt sources in bits 16 and above have platform-specific priority, but are typically chosen to have the highest service priority to support very fast local vectored interrupts. External interrupts are handled before internal (timer/software) interrupts as external interrupts are usually generated by devices that might require low interrupt service times. Software interrupts are handled before internal timer interrupts, because internal timer interrupts are usually intended for time slicing, where time precision is less important, whereas software interrupts are used for inter-processor messaging. Software interrupts can be avoided when high-precision timing is required, or high-precision timer interrupts can be routed via a different interrupt path. Software interrupts are located in the lowest four bits of <code>mip</code> as these are often written by software, and this position allows the use of a single CSR instruction with a five-bit immediate.
RVP.3.319	3.1.9 (p.34)	R	Restricted views of the <code>mip</code> and <code>mie</code> registers appear as the <code>sip</code> and <code>sie</code> registers for supervisor level.
RVP.3.320	3.1.9 (p.34)	R	If an interrupt is delegated to S-mode by setting a bit in the <code>mideleg</code> register, it becomes visible in the <code>sip</code> register and is maskable using the <code>sie</code> register. Otherwise, the corresponding bits in <code>sip</code> and <code>sie</code> are read-only zero.
RVP.3.321	3.1.10 (p.34)	H	Hardware Performance Monitor
RVP.3.322	3.1.10 (p.34)	I	M-mode includes a basic hardware performance-monitoring facility.
RVP.3.323	3.1.10 (p.34)	R	The <code>mcycle</code> CSR counts the number of clock cycles executed by the processor core on which the hart is running.
RVP.3.324	3.1.10 (p.34)	R	The <code>minstret</code> CSR counts the number of instructions the hart has retired.
RVP.3.325	3.1.10 (p.34)	R	The <code>mcycle</code> and <code>minstret</code> registers have 64-bit precision on all RV32 and RV64 systems.
RVP.3.326	3.1.10 (p.34)	R	The counter registers have an arbitrary value after the hart is reset, and can be written with a given value.
RVP.3.327	3.1.10 (p.34)	R	Any CSR write takes effect after the writing instruction has otherwise completed.
RVP.3.328	3.1.10 (p.34)	R	The <code>mcycle</code> CSR may be shared between harts on the same core, in which case writes to <code>mcycle</code> will be visible to those harts.

ID REFERENCE TYPE DEFINITION

RVP.3.329	3.1.10 (p.34)	R	The platform should provide a mechanism to indicate which harts share an <code>mcycle</code> CSR.																				
RVP.3.330	3.1.10 (p.34) Figure 3.16	R	The hardware performance monitor includes 29 additional 64-bit event counters, <code>mhpmcntr3</code> – <code>mhpmcntr31</code> .																				
RVP.3.331	3.1.10 (p.34) Figure 3.16	R	The event selector CSRs, <code>mhpmevent3</code> – <code>mhpmevent31</code> , are MXLEN-bit WARL registers that control which event causes the corresponding counter to increment.																				
RVP.3.332	3.1.10 (p.34, p.35)	R	The meaning of these events is defined by the platform, but event 0 is defined to mean “no event.” All counters should be implemented, but a legal implementation is to make both the counter and its corresponding event selector be read-only 0.																				
RVP.3.333	3.1.10 (p.35)	R	The <code>mhpmcntrs</code> are WARL registers that support up to 64 bits of precision on RV32 and RV64.																				
RVP.3.334	3.1.10 (p.35)	C	A future revision of this specification will define a mechanism to generate an interrupt when a hardware performance monitor counter overflows.																				
RVP.3.335	3.1.10 (p.35) Figure 3.17	R	When MXLEN=32, reads of the <code>mcycle</code> , <code>minstret</code> , and <code>mhpmcntrn</code> CSRs return bits 31–0 of the corresponding counter, and writes change only bits 31–0; reads of the <code>mcycleh</code> , <code>minstreth</code> , and <code>mhpmcntrnh</code> CSRs return bits 63–32 of the corresponding counter, and writes change only bits 63–32.																				
RVP.3.336	3.1.11 (p.35)	H	Machine Counter-Enable Register (<code>mcounteren</code>)																				
RVP.3.337	3.1.11 (p.35)	R	The counter-enable register <code>mcounteren</code> is a 32-bit register that controls the availability of the hardware performance-monitoring counters to the next-lowest privileged mode.																				
RVP.3.338	3.1.11 (p.35) Figure 3.18	R	Counter-enable register (<code>mcounteren</code>). <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>31</td><td>30</td><td>29</td><td>...</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>HPM31</td><td>HPM30</td><td>HPM29</td><td>...</td><td>HPM5</td><td>HPM4</td><td>HPM3</td><td>IR</td><td>TM</td><td>CY</td> </tr> </table>	31	30	29	...	5	4	3	2	1	0	HPM31	HPM30	HPM29	...	HPM5	HPM4	HPM3	IR	TM	CY
31	30	29	...	5	4	3	2	1	0														
HPM31	HPM30	HPM29	...	HPM5	HPM4	HPM3	IR	TM	CY														
RVP.3.339	3.1.11 (p.36)	R	The settings in this register only control accessibility.																				
RVP.3.340	3.1.11 (p.36)	R	The act of reading or writing this register does not affect the underlying counters, which continue to increment even when not accessible.																				
RVP.3.341	3.1.11 (p.36)	R	When the CY, TM, IR, or HPM _n bit in the <code>mcounteren</code> register is clear, attempts to read the <code>cycle</code> , <code>time</code> , <code>instret</code> , or <code>hpmcounter</code> register while executing in S-mode or U-mode will cause an illegal instruction exception.																				
RVP.3.342	3.1.11 (p.36)	R	When one of these bits (CY, TM, IR, or HPM _n bit) is set, access to the corresponding register is permitted in the next implemented privilege mode (S-mode if implemented, otherwise U-mode).																				
RVP.3.343	3.1.11 (p.36)	C	The counter-enable bits support two common use cases with minimal hardware. For systems that do not need high-performance timers and counters, machine-mode software can trap accesses and implement all features in software. For systems that need high-performance timers and counters but are not concerned with obfuscating the underlying hardware counters, the counters can be directly exposed to lower privilege modes.																				
RVP.3.344	3.1.11 (p.36)	R	The <code>cycle</code> , <code>instret</code> , and <code>hpmcounter</code> CSRs are read-only shadows of <code>mcycle</code> , <code>minstret</code> , and <code>mhpmcntr</code> , respectively.																				

ID REFERENCE TYPE DEFINITION

- RVP.3.345 3.1.11 (p.36) R The `time` CSR is a read-only shadow of the memory-mapped `mtime` register.
- RVP.3.346 3.1.11 (p.36) R Analogously, on RV32I the `cycleh`, `instreth` and `hpmcounternh` CSRs are read-only shadows of `mcycleh`, `minstreth` and `mhpmpcounternh`, respectively.
- RVP.3.347 3.1.11 (p.36) R On RV32I the `timeh` CSR is a read-only shadow of the upper 32 bits of the memory-mapped `mtime` register, while `time` shadows only the lower 32 bits of `mtime`.
- RVP.3.348 3.1.11 (p.36) C Implementations can convert reads of the `time` and `timeh` CSRs into loads to the memory-mapped `mtime` register, or emulate this functionality in M-mode software.
- RVP.3.349 3.1.11 (p.36) R In systems with U-mode, the `mcounteren` must be implemented, but all fields are WARL and may be read-only zero, indicating reads to the corresponding counter will cause an illegal instruction exception when executing in a less-privileged mode.
- RVP.3.350 3.1.11 (p.36) R In systems without U-mode, the `mcounteren` register should not exist.
- RVP.3.351 3.1.12 (p.36) H Machine Counter-Inhibit CSR (`mcountinhhibit`)
- RVP.3.352 3.1.12 (p.36) R The counter-inhibit register `mcountinhhibit` is a 32-bit WARL register that controls which of the hardware performance-monitoring counters increment. The settings in this register only control whether the counters increment; their accessibility is not affected by the setting of this register.
- RVP.3.353 3.1.12 (p.36) R Figure 3.19 Counter-inhibit register (`mcountinhhibit`)

31	30	29	...	5	4	3	2	1	0
HPM31	HPM30	HPM29	...	HPM5	HPM4	HPM3	IR	0	CY
- RVP.3.354 3.1.12 (p.36) R When the CY, IR, or `HPMn` bit in the `mcountinhhibit` register is clear, the `cycle`, `instret`, or `hpmcountern` register increments as usual.
- RVP.3.355 3.1.12 (p.36) R When the CY, IR, or `HPMn` bit is set, the corresponding counter does not increment.
- RVP.3.356 3.1.12 (p.36) R The `mcycle` CSR may be shared between harts on the same core, in which case the `mcountinhhibit.CY` field is also shared between those harts, and so writes to `mcountinhhibit.CY` will be visible to those harts.
- RVP.3.357 3.1.12 (p.37) R If the `mcountinhhibit` register is not implemented, the implementation behaves as though the register were set to zero.
- RVP.3.358 3.1.12 (p.37) C When the `cycle` and `instret` counters are not needed, it is desirable to conditionally inhibit them to reduce energy consumption. Providing a single CSR to inhibit all counters also allows the counters to be atomically sampled.
- RVP.3.359 3.1.12 (p.37) C Because the `time` counter can be shared between multiple cores, it cannot be inhibited with the `mcountinhhibit` mechanism.
- RVP.3.360 3.1.13 (p.37) H Machine Scratch Register (`mscratch`)
- RVP.3.361 3.1.13 (p.37) R The `mscratch` register is an MXLEN-bit read/write register dedicated for use by machine mode.
- RVP.3.362 3.1.13 (p.37) R Typically, it (`mscratch` register) is used to hold a pointer to a machine-mode hart-local context space and swapped with a user register upon entry to an M-mode trap handler.

ID REFERENCE TYPE DEFINITION

RVP.3.363	3.1.13 (p.37)	R Figure 3.20	Machine-mode scratch register.						
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>MXLEN-1</td> <td>...</td> <td>0</td> </tr> <tr> <td colspan="2">mscratch</td> <td></td> </tr> </table>	MXLEN-1	...	0	mscratch		
MXLEN-1	...	0							
mscratch									
RVP.3.364	3.1.13 (p.37)	C	The MIPS ISA allocated two user registers (k0/k1) for use by the operating system. Although the MIPS scheme provides a fast and simple implementation, it also reduces available user registers, and does not scale to further privilege levels, or nested traps. It can also require both registers are cleared before returning to user level to avoid a potential security hole and to provide deterministic debugging behavior.						
RVP.3.365	3.1.13 (p.37)	C	The RISC-V user ISA was designed to support many possible privileged system environments and so we did not want to infect the user-level ISA with any OS-dependent features. The RISCV CSR swap instructions can quickly save/restore values to the <code>mscratch</code> register. Unlike the MIPS design, the OS can rely on holding a value in the <code>mscratch</code> register while the user context is running.						
RVP.3.366	3.1.14 (p.37)	H	Machine Exception Program Counter (<code>mepc</code>)						
RVP.3.367	3.1.14 (p.37)	R	<code>Mepc</code> is an MXLEN-bit read/write register						
RVP.3.368	3.1.14 (p.37)	R	The low bit of <code>mepc</code> (<code>mepc[0]</code>) is always zero.						
RVP.3.369	3.1.14 (p.37)	R	On implementations that support only IALIGN=32, the two low bits (<code>mepc[1:0]</code>) are always zero						
RVP.3.370	3.1.13 (p.38) Figure 3.21	R	Machine exception program counter register						
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>MXLEN-1</td> <td>...</td> <td>0</td> </tr> <tr> <td colspan="2">mepc</td> <td></td> </tr> </table>	MXLEN-1	...	0	mepc		
MXLEN-1	...	0							
mepc									
RVP.3.371	3.1.14 (p.37)	R	If an implementation allows IALIGN to be either 16 or 32 (by changing CSR <code>misa</code> , for example), then, whenever IALIGN=32, bit <code>mepc[1]</code> is masked on reads so that it appears to be 0. This masking occurs also for the implicit read by the MRET instruction.						
RVP.3.372	3.1.14 (p.37)	R	Though masked, <code>mepc[1]</code> remains writable when IALIGN=32.						
RVP.3.373	3.1.14 (p.37)	R	<code>mepc</code> is a WARL register that must be able to hold all valid virtual addresses. It need not be capable of holding all possible invalid addresses.						
RVP.3.374	3.1.14 (p.37)	R	Prior to writing <code>mepc</code> , implementations may convert an invalid address into some other invalid address that <code>mepc</code> is capable of holding.						
RVP.3.375	3.1.14 (p.38)	C	When address translation is not in effect, virtual addresses and physical addresses are equal. Hence, the set of addresses <code>mepc</code> must be able to represent includes the set of physical addresses that can be used as a valid <code>pc</code> or effective address						
RVP.3.376	3.1.14 (p.38)	R	When a trap is taken into M-mode, <code>mepc</code> is written with the virtual address of the instruction that was interrupted or that encountered the exception. Otherwise, <code>mepc</code> is never written by the implementation, though it may be explicitly written by software.						
RVP.3.377	3.1.15 (p.38)	H	Machine Cause Register (<code>mcause</code>)						
RVP.3.378	3.1.15 (p.38)	R	The <code>mcause</code> register is an MXLEN-bit read-write register.						

ID	REFERENCE	TYPE	DEFINITION										
RVP.3.379	3.1.15 (p.38) Figure 3.22	R	Machine Cause Register (<code>mcause</code>):										
			<table border="1"> <tr> <td>MXLEN-1</td> <td>MXLEN-2</td> <td>...</td> <td>1</td> <td>0</td> </tr> <tr> <td>Interrupt</td> <td colspan="3">Exception Code (WLRL)</td> <td></td> </tr> </table>	MXLEN-1	MXLEN-2	...	1	0	Interrupt	Exception Code (WLRL)			
MXLEN-1	MXLEN-2	...	1	0									
Interrupt	Exception Code (WLRL)												
RVP.3.380	3.1.15 (p.38)	R	When a trap is taken into M-mode, <code>mcause</code> is written with a code indicating the event that caused the trap.										
RVP.3.381	3.1.15 (p.38)	R	Otherwise (other than a trap is taken into M-mode), <code>mcause</code> is never written by the implementation, though it may be explicitly written by software.										
RVP.3.382	3.1.15 (p.38)	R	The Interrupt bit in the <code>mcause</code> register is set if the trap was caused by an interrupt										
RVP.3.383	3.1.15 (p.38)	R	The Exception Code field contains a code identifying the last exception or interrupt.										
RVP.3.384	3.1.15 (p.38)	R	RVP.3.389 lists the possible machine-level exception codes.										
RVP.3.385	3.1.15 (p.38)	R	The Exception Code is a WLRL field, so is only guaranteed to hold supported exception codes.										
RVP.3.386	3.1.15 (p.38)	I	Note that load and load-reserved instructions generate load exceptions, whereas store, store conditional, and AMO instructions generate store/AMO exceptions.										
RVP.3.387	3.1.15 (p.38)	C	Interrupts can be separated from other traps with a single branch on the sign of the <code>mcause</code> register value. A shift left can remove the interrupt bit and scale the exception codes to index into a trap vector table.										
RVP.3.388	3.1.15 (p.38)	C	We do not distinguish privileged instruction exceptions from illegal opcode exceptions. This simplifies the architecture and also hides details of which higher-privilege instructions are supported by an implementation. The privilege level servicing the trap can implement a policy on whether these need to be distinguished, and if so, whether a given opcode should be treated as illegal or privileged.										

ID REFERENCE TYPE DEFINITION

RVP.3.389 3.1.15 (p.39) R Machine cause register (`mcause`) values after trap (the possible machine-level exception codes)
Table 3.6

Interrupt	Exception Code	Description
1	0	Reserved
1	1	Supervisor software interrupt
1	2	Reserved
1	3	Machine software interrupt
1	4	Reserved
1	5	Supervisor timer interrupt
1	6	Reserved
1	7	Machine timer interrupt
1	8	Reserved
1	9	Supervisor external interrupt
1	10	Reserved
1	11	Machine external interrupt
1	12 - 15	Reserved
1	≥ 16	Designated for platform use
0	0	Instruction address misaligned
0	1	Instruction access fault
0	2	Illegal instruction
0	3	Breakpoint
0	4	Load address misaligned
0	5	Load access fault
0	6	Store/AMO address misaligned
0	7	Store/AMO access fault
0	8	Environment call from U-mode
0	9	Environment call from S-mode
0	10	Reserved
0	11	Environment call from M-mode
0	12	Instruction page fault
0	13	Load page fault
0	14	Reserved
0	15	Store/AMO page fault
0	16 - 23	Reserved
0	24 - 31	Designated for custom use
0	32 - 47	Reserved
0	48 - 63	Designated for custom use
0	≥ 64	Reserved

RVP.3.390 3.1.15 (p.38) R If an instruction may raise multiple synchronous exceptions, the decreasing priority order of RVP.3.392 indicates which exception is taken and reported in `mcause`.

RVP.3.391 3.1.15 (p.38) R The priority of any custom synchronous exceptions is implementation-defined.

ID REFERENCE TYPE DEFINITION

RVP.3.392 3.1.15 (p.40) R Synchronous exception priority in decreasing priority order.
Table 3.7

Priority	Exception Code	Description
Highest	3	Instruction address breakpoint
	12, 1	During instruction address translation: First encountered page fault or access fault
	1	With physical address for instruction: Instruction access fault
	2	Illegal instruction
	0	Instruction address misaligned
	8, 9, 11	Environment call
	3	Environment break
	3	Load/store/AMO address breakpoint
	4, 6	Optionally: Load/store/AMO address misaligned
	13, 15, 5, 7	During address translation for an explicit memory access: First encountered page fault or access fault
	5, 7	With physical address for an explicit memory access: Load/store/AMO access fault
Lowest	4, 6	If not higher priority: Load/store/AMO address misaligned

RVP.3.393 3.1.15 (p.40) R When a virtual address is translated into a physical address, the address translation algorithm determines what specific exception may be raised.

RVP.3.394 3.1.15 (p.40) R Load/store/AMO address-misaligned exceptions may have either higher or lower priority than load/store/AMO page-fault and access-fault exceptions.

RVP.3.395 3.1.15 (p.40) C The relative priority of load/store/AMO address-misaligned and page-fault exceptions is implementation-defined to flexibly cater to two design points. Implementations that never support misaligned accesses can unconditionally raise the misaligned-address exception without performing address translation or protection checks. Implementations that support misaligned accesses only to some physical addresses must translate and check the address before determining whether the misaligned access may proceed, in which case raising the page-fault exception or access is more appropriate.

RVP.3.396 3.1.15 (p.40) C Instruction address breakpoints have the same cause value as, but different priority than, data address breakpoints (a.k.a. watchpoints) and environment break exceptions (which are raised by the EBREAK instruction).

RVP.3.397 3.1.15 (p.40) C Instruction address misaligned exceptions are raised by control-flow instructions with misaligned targets, rather than by the act of fetching an instruction. Therefore, these exceptions have lower priority than other instruction address exceptions.

RVP.3.398 3.1.16 (p.41) H Machine Trap Value Register (`mtval`)

RVP.3.399 3.1.16 (p.41) R The `mtval` register is an MXLEN-bit read-write register

RVP.3.400 3.1.16 (p.41) R Machine Trap Value register, (`mtval`):
Figure 3.23

MXLEN-1	...	0
mtval		

ID REFERENCE TYPE DEFINITION

RVP.3.401	3.1.16 (p.41)	R	When a trap is taken into M-mode, <code>mtval</code> is either set to zero or written with exception-specific information to assist software in handling the trap.
RVP.3.402	3.1.16 (p.41)	R	Otherwise (other than when a trap is taken into M-mode), <code>mtval</code> is never written by the implementation, though it may be explicitly written by software.
RVP.3.403	3.1.16 (p.41)	R	The hardware platform will specify which exceptions must set <code>mtval</code> informatively and which may unconditionally set it to zero.
RVP.3.404	3.1.16 (p.41)	R	If the hardware platform specifies that no exceptions set <code>mtval</code> to a nonzero value, then <code>mtval</code> is read-only zero.
RVP.3.405	3.1.16 (p.41)	R	If <code>mtval</code> is written with a nonzero value when a breakpoint, address-misaligned, access-fault, or page-fault exception occurs on an instruction fetch, load, or store, then <code>mtval</code> will contain the faulting virtual address.
RVP.3.406	3.1.16 (p.41)	C	When page-based virtual memory is enabled, <code>mtval</code> is written with the faulting virtual address, even for physical-memory access-fault exceptions. This design reduces datapath cost for most implementations, particularly those with hardware page-table walkers.
RVP.3.407	3.1.16 (p.41)	R	If <code>mtval</code> is written with a nonzero value when a misaligned load or store causes an access-fault or page-fault exception, then <code>mtval</code> will contain the virtual address of the portion of the access that caused the fault.
RVP.3.408	3.1.16 (p.41)	R	If <code>mtval</code> is written with a nonzero value when an instruction access-fault or page-fault exception occurs on a system with variable-length instructions, then <code>mtval</code> will contain the virtual address of the portion of the instruction that caused the fault, while <code>mepc</code> will point to the beginning of the instruction.
RVP.3.409	3.1.16 (p.41)	R	The <code>mtval</code> register can optionally also be used to return the faulting instruction bits on an illegal instruction exception (<code>mepc</code> points to the faulting instruction in memory).
RVP.3.410	3.1.16 (p.41)	R	If <code>mtval</code> is written with a nonzero value when an illegal-instruction exception occurs, then <code>mtval</code> will contain the shortest of: <ul style="list-style-type: none"> • the actual faulting instruction • the first ILEN bits of the faulting instruction • the first MXLEN bits of the faulting instruction
RVP.3.411	3.1.16 (p.41)	R	The value loaded into <code>mtval</code> on an illegal-instruction exception is right-justified and all unused upper bits are cleared to zero.
RVP.3.412	3.1.16 (p.41)	C	Capturing the faulting instruction in <code>mtval</code> reduces the overhead of instruction emulation, potentially avoiding several partial instruction loads if the instruction is misaligned, and likely data cache misses or slow uncached accesses when loads are used to fetch the instruction into a data register. There is also a problem of atomicity if another agent is manipulating the instruction memory, as might occur in a dynamic translation system.
RVP.3.413	3.1.16 (p.42)	C	A requirement is that the entire instruction (or at least the first MXLEN bits) are fetched into <code>mtval</code> before taking the trap. This should not constrain implementations, which would typically fetch the entire instruction before attempting to decode the instruction, and avoids complicating software handlers.

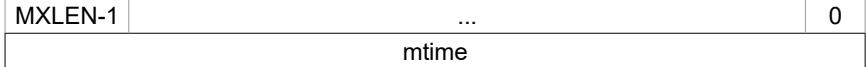
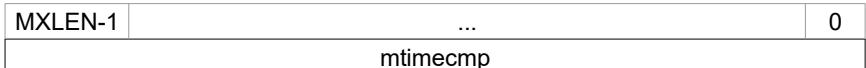
ID REFERENCE TYPE DEFINITION

- RVP.3.414 3.1.16 (p.42) C A value of zero in `mtval` signifies either that the feature is not supported, or an illegal zero instruction was fetched. A load from the instruction memory pointed to by `mepc` can be used to distinguish these two cases (or alternatively, the system configuration information can be interrogated to install the appropriate trap handling before runtime).
- RVP.3.415 3.1.16 (p.42) R For other traps, `mtval` is set to zero, but a future standard may redefine `mtval`'s setting for other traps.
- RVP.3.416 3.1.16 (p.42) R If `mtval` is not read-only zero, it is a WARL register that must be able to hold all valid virtual addresses and the value zero. It need not be capable of holding all possible invalid addresses.
- RVP.3.417 3.1.16 (p.42) R Prior to writing `mtval`, implementations may convert an invalid address into some other invalid address that `mtval` is capable of holding.
- RVP.3.418 3.1.16 (p.42) O If the feature to return the faulting instruction bits is implemented, `mtval` must also be able to hold all values less than $2N$, where N is the smaller of `MXLEN` and `ILEN`.
- RVP.3.419 3.1.17 (p.42) H Machine Configuration Pointer Register (`mconfigptr`)
- RVP.3.420 3.1.17 (p.42) R `mconfigptr` is an `MXLEN`-bit read-only CSR that holds the physical address of a configuration data structure.
- RVP.3.421 3.1.17 (p.42) R Machine Configuration Pointer register, (`mconfigptr`):
Figure 3.24
- | | | |
|-------------------------|-----|---|
| MXLEN-1 | ... | 0 |
| <code>mconfigptr</code> | | |
- RVP.3.422 3.1.17 (p.42) R Software can traverse this data structure to discover information about the harts, the platform, and their configuration
- RVP.3.423 3.1.17 (p.42) R The pointer alignment in bits must be no smaller than the greatest supported `MXLEN`: i.e., if the greatest supported `MXLEN` is $8 \times n$, then `mconfigptr[\log_2 n - 1 : 0]` must be zero.
- RVP.3.424 3.1.17 (p.42) R `mconfigptr` must be implemented, but it may be zero to indicate the configuration data structure does not exist or that an alternative mechanism must be used to locate it.
- RVP.3.425 3.1.17 (p.42) C The format and schema of the configuration data structure have yet to be standardized
- RVP.3.426 3.1.17 (p.42) C While `mconfigptr` will simply be hardwired in some implementations, other implementations may provide a means to configure the value returned on CSR reads. For example, `mconfigptr` might present the value of a memory-mapped register that is programmed by the platform or by M-mode software towards the beginning of the boot process.
- RVP.3.427 3.1.18 (p.43) H Machine Environment Configuration Registers (`menvcfg` and `menvcfgh`)
- RVP.3.428 3.1.18 (p.43) R The `menvcfg` CSR is an `MXLEN`-bit read/write register that controls certain characteristics of the execution environment for modes less privileged than M.
- RVP.3.429 3.1.18 (p.43) R The register `menvcfg` formatted for `MXLEN=64`
Figure 3.25
- | | | | | | | | | | | | | |
|------|-------|------|-----|---|------|-------|------|------|---|---|------|---|
| 63 | 62 | 61 | ... | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| STCE | PBMTE | WPRI | | | CBZE | CBCFE | CBIE | WPRI | | | FIOM | |

ID REFERENCE TYPE DEFINITION

- RVP.3.430 3.1.18 (p.43) R If bit FIOM (Fence of I/O implies Memory) is set to one in `menvcfg`, FENCE instructions executed in modes less privileged than M are modified so the requirement to order accesses to device I/O implies also the requirement to order main memory accesses.
- RVP.3.431 3.1.18 (p.43) R Table 3.8 The table below details the modified interpretation of FENCE instruction bits PI, PO, SI, and SO for modes less privileged than M when FIOM=1.
- | Instruction bit | Meaning when set |
|-----------------|--|
| PI | Predecessor device input and memory reads (PR implied) |
| PO | Predecessor device output and memory writes (PW implied) |
| SI | Successor device input and memory reads (SR implied) |
| SO | Successor device output and memory writes (SW implied) |
- RVP.3.432 3.1.18 (p.43) R Similarly, for modes less privileged than M when FIOM=1, if an atomic instruction that accesses a region ordered as device I/O has its `aq` and/or `rl` bit set, then that instruction is ordered as though it accesses both device I/O and memory.
- RVP.3.433 3.1.18 (p.43) R If S-mode is not supported, or if `satp.MODE` is read-only zero (always Bare), the implementation may make FIOM read-only zero.
- RVP.3.434 3.1.18 (p.43) C Bit FIOM is needed in `menvcfg` so M-mode can emulate the hypervisor extension of Chapter 8, which has an equivalent FIOM bit in the hypervisor CSR `henvcfg`.
- RVP.3.435 3.1.18 (p.43) R The PBMTE bit controls whether the Svpbmt extension is available for use in S-mode and G-stage address translation (i.e., for page tables pointed to by `satp` or `hgatp`).
- RVP.3.436 3.1.18 (p.43) R When PBMTE=1, Svpbmt is available for S-mode and G-stage address translation.
- RVP.3.437 3.1.18 (p.43) R When PBMTE=0, the implementation behaves as though Svpbmt were not implemented.
- RVP.3.438 3.1.18 (p.43) R If Svpbmt is not implemented, PBMTE is read-only zero.
- RVP.3.439 3.1.18 (p.43) R Furthermore, for implementations with the hypervisor extension, `henvcfg.PBMTE` is read-only zero if `menvcfg.PBMTE` is zero.
- RVP.3.440 3.1.18 (p.43) I The definition of the STCE field will be furnished by the forthcoming Sstc extension. Its allocation within `menvcfg` may change prior to the ratification of that extension.
- RVP.3.441 3.1.18 (p.43) I The definition of the CBZE field will be furnished by the forthcoming Zicboz extension. Its allocation within `menvcfg` may change prior to the ratification of that extension.
- RVP.3.442 3.1.18 (p.44) I The definitions of the CBCFE and CBIE fields will be furnished by the forthcoming Zicbom extension. Their allocations within `menvcfg` may change prior to the ratification of that extension.
- RVP.3.443 3.1.18 (p.44) R When MXLEN=32, `menvcfg` contains the same fields as bits 31:0 of `menvcfg` when MXLEN=64.
- RVP.3.444 3.1.18 (p.44) R Additionally, when MXLEN=32, `menvcfg` is a 32-bit read/write register that contains the same fields as bits 63:32 of `menvcfg` when MXLEN=64.
- RVP.3.445 3.1.18 (p.44) R Register `menvcfg` does not exist when MXLEN=64.

ID REFERENCE TYPE DEFINITION

RVP.3.446	3.1.18 (p.44)	R	If U-mode is not supported, then registers <code>menvcfg</code> and <code>menvcfgh</code> do not exist.
RVP.3.447	3.1.19 (p.44)	H	Machine Security Configuration Register (<code>mseccfg</code>)
RVP.3.448	3.1.19 (p.44)	R	<code>mseccfg</code> is an optional MXLEN-bit read/write register that controls security features.
RVP.3.449	3.1.19 (p.44) Figure 3.26	R	Machine security configuration register (<code>mseccfg</code>). 
RVP.3.450	3.1.19 (p.44)	R	When MXLEN=32 only, <code>mseccfgh</code> is a 32-bit read/write register that contains the same fields as <code>mseccfg</code> bits 63:32 when MXLEN=64.
RVP.3.451	3.1.19 (p.44)	I	The definitions of the SSEED and USEED fields will be furnished by the forthcoming entropy source extension, Zkr. Their allocations within <code>mseccfg</code> may change prior to the ratification of that extension.
RVP.3.452	3.1.19 (p.44)	I	The definitions of the RLB, MMWP, and MML fields will be furnished by the forthcoming PMP enhancement extension, Smpmp. Their allocations within <code>mseccfg</code> may change prior to the ratification of that extension.
RVP.3.453	3.2 (p.44)	H	Machine-Level Memory-Mapped Registers
RVP.3.454	3.2.1 (p.44)	H	Machine Timer Registers (<code>mtime</code> and <code>mtimecmp</code>)
RVP.3.455	3.2.1 (p.44)	R	Platforms provide a real-time counter, exposed as a memory-mapped machine-mode read-write register, <code>mtime</code> .
RVP.3.456	3.2.1 (p.44)	R	<code>mtime</code> must increment at constant frequency, and the platform must provide a mechanism for determining the period of an <code>mtime</code> tick.
RVP.3.457	3.2.1 (p.44)	R	The <code>mtime</code> register will wrap around if the count overflows.
RVP.3.458	3.2.1 (p.44)	R	The <code>mtime</code> register has a 64-bit precision on all RV32 and RV64 systems.
RVP.3.459	3.2.1 (p.44)	R	Platforms provide a 64-bit memory-mapped machine-mode timer compare register (<code>mtimecmp</code>).
RVP.3.460	3.2.1 (p.44)	R	A machine timer interrupt becomes pending whenever <code>mtime</code> contains a value greater than or equal to <code>mtimecmp</code> , treating the values as unsigned integers.
RVP.3.461	3.2.1 (p.44)	R	The interrupt remains posted until <code>mtimecmp</code> becomes greater than <code>mtime</code> (typically as a result of writing <code>mtimecmp</code>).
RVP.3.462	3.2.1 (p.44)	R	The interrupt will only be taken if interrupts are enabled and the MTIE bit is set in the <code>mie</code> register.
RVP.3.463	3.2.1 (p.45) Figure 3.27	R	Machine time register (memory-mapped control register) (<code>mtime</code>): 
RVP.3.464	3.2.1 (p.45) Figure 3.28	R	Machine time compare register (memory-mapped control register (<code>mtimecmp</code>)): 

ID	REFERENCE	TYPE	DEFINITION
RVP.3.465	3.2.1 (p.45)	C	The timer facility is defined to use wall-clock time rather than a cycle counter to support modern processors that run with a highly variable clock frequency to save energy through dynamic voltage and frequency scaling.
RVP.3.466	3.2.1 (p.45)	C	Accurate real-time clocks (RTCs) are relatively expensive to provide (requiring a crystal or MEMS oscillator) and have to run even when the rest of system is powered down, and so there is usually only one in a system located in a different frequency/voltage domain from the processors. Hence, the RTC must be shared by all the harts in a system and accesses to the RTC will potentially incur the penalty of a voltage-level-shifter and clock-domain crossing. It is thus more natural to expose mtime as a memory-mapped register than as a CSR.
RVP.3.467	3.2.1 (p.45)	C	Lower privilege levels do not have their own timecmp registers. Instead, machine-mode software can implement any number of virtual timers on a hart by multiplexing the next timer interrupt into the mtimetcmp register.
RVP.3.468	3.2.1 (p.45)	C	Simple fixed-frequency systems can use a single clock for both cycle counting and wall-clock time.
RVP.3.469	3.2.1 (p.45)	R	Writes to <code>mtime</code> and <code>mtimetcmp</code> are guaranteed to be reflected in MTIP eventually, but not necessarily immediately.
RVP.3.470	3.2.1 (p.45)	C	A spurious timer interrupt might occur if an interrupt handler increments <code>mtimetcmp</code> then immediately returns, because MTIP might not yet have fallen in the interim. All software should be written to assume this event is possible, but most software should assume this event is extremely unlikely. It is almost always more performant to incur an occasional spurious timer interrupt than to poll MTIP until it falls.
RVP.3.471	3.2.1 (p.45)	R	In RV32, memory-mapped writes to <code>mtimetcmp</code> modify only one 32-bit part of the register. The following code sequence sets a 64-bit <code>mtimetcmp</code> value without spuriously generating a timer interrupt due to the intermediate value of the comparand
RVP.3.472	3.2.1 (p.45)	R	For RV64, naturally aligned 64-bit memory accesses to the <code>mtime</code> and <code>mtimetcmp</code> registers are additionally supported and are atomic.
RVP.3.473	3.2.1 (p.46) Figure 3.29	I	Sample code for setting the 64-bit time comparand in RV32, assuming a little-endian memory system and that the registers live in a strongly ordered I/O region. Storing -1 to the low-order bits of <code>mtimetcmp</code> prevents <code>mtimetcmp</code> from temporarily becoming smaller than the lesser of the old and new values.
			<pre># New comparand is in a1:a0. li t0, -1 la t1, mtimetcmp sw t0, 0(t1) # No smaller than old value. sw a1, 4(t1) # No smaller than new value. sw a0, 0(t1) # New value.</pre>
RVP.3.474	3.3 (p.46)	H	Machine-Mode Privileged Instructions
RVP.3.475	3.3.1 (p.46)	H	Environment Call and Breakpoint
RVP.3.476	3.3.1 (p.46)	R	The ECALL instruction is used to make a request to the supporting execution environment.
RVP.3.477	3.3.1 (p.46)	R	When executed in U-mode, S-mode, or M-mode, it (ECALL) generates an environment-call-from-U-mode exception, environment-call-from-S-mode exception, or environment-call-from-M-mode exception, respectively, and performs no other operation.

ID REFERENCE TYPE DEFINITION

RVP.3.478	3.3.1 (p.46)	C	ECALL generates a different exception for each originating privilege mode so that environment call exceptions can be selectively delegated. A typical use case for Unix-like operating systems is to delegate to S-mode the environment-call-from-U-mode exception but not the others.																																																																																																																															
RVP.3.479	3.3.1 (p.46)	R	The EBREAK instruction is used by debuggers to cause control to be transferred back to a debugging environment. It generates a breakpoint exception and performs no other operation.																																																																																																																															
RVP.3.480	3.3.1 (p.46)	C	As described in the “C” Standard Extension for Compressed Instructions in Volume I of this manual, the C.EBREAK instruction performs the same operation as the EBREAK instruction.																																																																																																																															
RVP.3.481	3.3.1 (p.46)	R	ECALL and EBREAK cause the receiving privilege mode’s <code>epc</code> register to be set to the address of the ECALL or EBREAK instruction itself, not the address of the following instruction.																																																																																																																															
RVP.3.482	3.3.1 (p.46)	R	As ECALL and EBREAK cause synchronous exceptions, they are not considered to retire, and should not increment the <code>minstret</code> CSR.																																																																																																																															
RVP.3.483	3.3.2 (p.47)	H	Trap-Return Instructions																																																																																																																															
RVP.3.484	3.3.2 (p.47) 9.0 (p.138)	R	MRET Instruction Machine mode trap return instruction Encoding: Special I-Type																																																																																																																															
			<table border="1" style="width: 100%; text-align: center;"> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td></td><td>rs1</td><td></td><td>P<small>RIV</small></td><td></td><td>rd</td><td></td><td></td><td>S<small>YSTEM</small></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td></td><td></td><td></td> </tr> </table>	3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0											0	0	1	1	0	0	0	0	0	0	0	1	0		rs1		P <small>RIV</small>		rd			S <small>YSTEM</small>																								0	0	0						1	1	1	0	0	1	1			
3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																																			
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																													
0	0	1	1	0	0	0	0	0	0	0	1	0		rs1		P <small>RIV</small>		rd			S <small>YSTEM</small>																																																																																																													
													0	0	0						1	1	1	0	0	1	1																																																																																																							
			Valid Base: RV32, RV64, RV128 Task: PC = <code>xepc</code> Explanation: An MRET instruction is used to return from a trap in M-mode. In addition to manipulating the privilege stack as described in Section 3.1.6.1, <code>xRET</code> sets the pc to the value stored in the <code>xepc</code> register. Special Case: none Exception: none																																																																																																																															
RVP.3.485	3.3.2 (p.47) 9.0 (p.138)	R	SRET Instruction Supervisor mode trap return instruction Encoding: Special I-Type																																																																																																																															
			<table border="1" style="width: 100%; text-align: center;"> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td></td><td>rs1</td><td></td><td>P<small>RIV</small></td><td></td><td>rd</td><td></td><td></td><td>S<small>YSTEM</small></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td></td><td></td><td></td><td>0</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td></td><td></td><td></td> </tr> </table>	3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0											0	0	0	1	0	0	0	0	0	0	0	1	0		rs1		P <small>RIV</small>		rd			S <small>YSTEM</small>														0	0	0								0	0	0					1	1	1	0	0	1	1			
3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																																		
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																													
0	0	0	1	0	0	0	0	0	0	0	1	0		rs1		P <small>RIV</small>		rd			S <small>YSTEM</small>																																																																																																													
			0	0	0								0	0	0					1	1	1	0	0	1	1																																																																																																								
			Valid Base: RV32, RV64, RV128 Task: PC = <code>xepc</code> Explanation: An SRET instruction is used to return from a trap in S-mode. In addition to manipulating the privilege stack as described in Section 3.1.6.1, <code>xRET</code> sets the pc to the value stored in the <code>xepc</code> register. Special Case: none Exception: none																																																																																																																															
RVP.3.486	3.3.2 (p.47)	R	To return after handling a trap, there are separate trap return instructions per privilege level, MRET and SRET. MRET is always provided.																																																																																																																															
RVP.3.487	3.3.2 (p.47)	R	SRET must be provided if supervisor mode is supported, and should raise an illegal instruction exception otherwise.																																																																																																																															

ID	REFERENCE	TYPE	DEFINITION																																																																																																																																		
RVP.3.488	3.3.2 (p.47)	R	SRET should also raise an illegal instruction exception when TSR=1 in mstatus, as described in Section 3.1.6.5.																																																																																																																																		
RVP.3.489	3.3.2 (p.47)	R	An xRET instruction can be executed in privilege mode x or higher, where executing a lower-privilege xRET instruction will pop the relevant lower-privilege interrupt enable and privilege mode stack.																																																																																																																																		
RVP.3.490	3.3.2 (p.47)	R	If the A extension is supported, the xRET instruction is allowed to clear any outstanding LR address reservation but is not required to. Trap handlers should explicitly clear the reservation if required (e.g., by using a dummy SC) before executing the xRET.																																																																																																																																		
RVP.3.491	3.3.2 (p.47)	C	If xRET instructions always cleared LR reservations, it would be impossible to single-step through LR/SC sequences using a debugger.																																																																																																																																		
RVP.3.492	3.3.3 (p.47)	H	Wait for Interrupt																																																																																																																																		
RVP.3.493	3.3.3 (p.47) 9.0 (p.138)	R	WFI Instruction Wait for interrupt instruction Encoding: Special I-Type																																																																																																																																		
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td></td><td>rs1</td><td></td><td></td><td>PRIV</td><td></td><td></td><td>rd</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>SYSTEM</td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td> </tr> </table>	3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0										0	0	0	1	0	0	0	0	0	1	0	1		rs1			PRIV			rd											SYSTEM																	0	0	0													1	1	1	0	0	1	1
3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																																								
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																																
0	0	0	1	0	0	0	0	0	1	0	1		rs1			PRIV			rd											SYSTEM																																																																																																							
																0	0	0													1	1	1	0	0	1	1																																																																																																
			Valid Base: RV32, RV64, RV128 Task: – Explanation: The Wait for Interrupt instruction (WFI) provides a hint to the implementation that the current hart can be stalled until an interrupt might need servicing. Execution of the WFI instruction can also be used to inform the hardware platform that suitable interrupts should preferentially be routed to this hart. Special Case: none Exception: none																																																																																																																																		
RVP.3.494	3.3.3 (p.47)	R	WFI is available in all privileged modes, and optionally available to U-mode.																																																																																																																																		
RVP.3.495	3.3.3 (p.47)	R	This instruction may raise an illegal instruction exception when TW=1 in mstatus, as described in Section 3.1.6.5.																																																																																																																																		
RVP.3.496	3.3.3 (p.47)	R	If an enabled interrupt is present or later becomes present while the hart is stalled, the interrupt trap will be taken on the following instruction, i.e., execution resumes in the trap handler and $mepc = pc + 4$.																																																																																																																																		
RVP.3.497	3.3.3 (p.47)	C	The following instruction takes the interrupt trap so that a simple return from the trap handler will execute code after the WFI instruction.																																																																																																																																		
RVP.3.498	3.3.3 (p.47)	I	The purpose of the WFI instruction is to provide a hint to the implementation, and so a legal implementation is to simply implement WFI as a NOP.																																																																																																																																		
RVP.3.499	3.3.3 (p.48)	C	If the implementation does not stall the hart on execution of the instruction, then the interrupt will be taken on some instruction in the idle loop containing the WFI, and on a simple return from the handler, the idle loop will resume execution.																																																																																																																																		
RVP.3.500	3.3.3 (p.48)	R	The WFI instruction can also be executed when interrupts are disabled.																																																																																																																																		

ID REFERENCE TYPE DEFINITION

RVP.3.501	3.3.3 (p.48)	R	The operation of WFI must be unaffected by the global interrupt bits in mstatus (MIE and SIE) and the delegation register mideleg (i.e., the hart must resume if a locally enabled interrupt becomes pending, even if it has been delegated to a less-privileged mode), but should honor the individual interrupt enables (e.g, MTIE) (i.e., implementations should avoid resuming the hart if the interrupt is pending but not individually enabled).
RVP.3.502	3.3.3 (p.48)	R	WFI is also required to resume execution for locally enabled interrupts pending at any privilege level, regardless of the global interrupt enable at each privilege level.
RVP.3.503	3.3.3 (p.48)	R	If the event that causes the hart to resume execution does not cause an interrupt to be taken, execution will resume at pc + 4, and software must determine what action to take, including looping back to repeat the WFI if there was no actionable event.
RVP.3.504	3.3.3 (p.48)	C	By allowing wakeup when interrupts are disabled, an alternate entry point to an interrupt handler can be called that does not require saving the current context, as the current context can be saved or discarded before the WFI is executed.
RVP.3.505	3.3.3 (p.48)	C	As implementations are free to implement WFI as a NOP, software must explicitly check for any relevant pending but disabled interrupts in the code following an WFI, and should loop back to the WFI if no suitable interrupt was detected. The mip or sip registers can be interrogated to determine the presence of any interrupt in machine or supervisor mode respectively.
RVP.3.506	3.3.3 (p.48)	C	The operation of WFI is unaffected by the delegation register settings.
RVP.3.507	3.3.3 (p.48)	C	WFI is defined so that an implementation can trap into a higher privilege mode, either immediately on encountering the WFI or after some interval to initiate a machine-mode transition to a lower power state, for example.
RVP.3.508	3.3.3 (p.48)	C	The same “wait-for-event” template might be used for possible future extensions that wait on memory locations changing, or message arrival.
RVP.3.509	3.3.4 (p.48)	H	Custom SYSTEM Instructions
RVP.3.510	3.3.4 (p.48, p.49) Figure 3.30	R	The subspace of the SYSTEM major opcode shown in table below, is designated for custom use. It is recommended that these instructions use bits 29:28 to designate the minimum required privilege mode, as do other SYSTEM instructions.
RVP.3.511	3.4 (p.48)	H	Reset

31 ... 26	25 ... 15	14 ... 12	11 ... 7	6 ... 0	Recommended Purpose
funct6		funct3		opcode	
100011	custom	0	custom	1110011	Unprivileged or User-Level
110011	custom	0	custom	1110011	Unprivileged or User-Level
100111	custom	0	custom	1110011	Supervisor-Level
110111	custom	0	custom	1110011	Supervisor-Level
101011	custom	0	custom	1110011	Hypervisor-Level
111011	custom	0	custom	1110011	Hypervisor-Level
101111	custom	0	custom	1110011	Machine-Level
111111	custom	0	custom	1110011	Machine-Level

ID	REFERENCE	TYPE	DEFINITION
RVP.3.512	3.4 (p.48, p.49)	R	<p>Upon reset,</p> <ul style="list-style-type: none"> • A hart's privilege mode is set to M. • The <code>mstatus</code> fields MIE and MPRV are reset to 0. • If little-endian memory accesses are supported, the <code>mstatus/mstatusush</code> field MBE is reset to 0. • The <code>misa</code> register is reset to enable the maximal set of supported extensions and widest MXLEN, as described in Section 3.1.1. • For implementations with the “A” standard extension, there is no valid load reservation. • The <code>pc</code> is set to an implementation-defined reset vector. • The <code>mcause</code> register is set to a value indicating the cause of the reset. • Writable PMP registers’ A and L fields are set to 0, unless the platform mandates a different reset value for some PMP registers’ A and L fields. • If the hypervisor extension is implemented, the <code>hgatp.MODE</code> and <code>vsatp.MODE</code> fields are reset to 0. • No WARL field contains an illegal value. • All other hart state is UNSPECIFIED.
RVP.3.513	3.4 (p.49)	R	The <code>mcause</code> values after reset have implementation-specific interpretation, but the value 0 should be returned on implementations that do not distinguish different reset conditions.
RVP.3.514	3.4 (p.49)	R	Implementations that distinguish different reset conditions should only use 0 (as the <code>mcause</code> value) to indicate the most complete reset.
RVP.3.515	3.4 (p.49)	C	Some designs may have multiple causes of reset (e.g., power-on reset, external hard reset, brownout detected, watchdog timer elapse, sleep-mode wakeup), which machine-mode software and debuggers may wish to distinguish.
RVP.3.516	3.4 (p.49)	C	<code>mcause</code> reset values may alias <code>mcause</code> values following synchronous exceptions. There should be no ambiguity in this overlap, since on reset the <code>pc</code> is typically set to a different value than on other traps.
RVP.3.517	3.5 (p.49)	H	Non-Maskable Interrupts
RVP.3.518	3.5 (p.49)	R	Non-maskable interrupts (NMIs) are only used for hardware error conditions, and cause an immediate jump to an implementation-defined NMI vector running in M-mode regardless of the state of a hart’s interrupt enable bits.
RVP.3.519	3.5 (p.49)	R	The <code>mepc</code> register is written with the virtual address of the instruction that was interrupted, and <code>mcause</code> is set to a value indicating the source of the NMI.
RVP.3.520	3.5 (p.49)	R	NMI can thus overwrite state in an active machine-mode interrupt handler.
RVP.3.521	3.5 (p.49)	R	The values written to <code>mcause</code> on an NMI are implementation-defined.
RVP.3.522	3.5 (p.49)	R	The high Interrupt bit of <code>mcause</code> should be set to indicate that this was an interrupt.
RVP.3.523	3.5 (p.49)	R	An Exception Code of 0 is reserved to mean “unknown cause” and implementations that do not distinguish sources of NMIs via the <code>mcause</code> register should return 0 in the Exception Code.
RVP.3.524	3.5 (p.49)	R	Unlike resets, NMIs do not reset processor state, enabling diagnosis, reporting, and possible containment of the hardware error.
RVP.3.525	3.6 (p.50)	H	Physical Memory Attributes

ID	REFERENCE TYPE DEFINITION	
RVP.3.526 3.6 (p.50)	I	The physical memory map for a complete system includes various address ranges, some corresponding to memory regions, some to memory-mapped control registers, and some to vacant holes in the address space. Some memory regions might not support reads, writes, or execution; some might not support subword or subblock accesses; some might not support atomic operations; and some might not support cache coherence or might have different memory models. Similarly, memory mapped control registers vary in their supported access widths, support for atomic operations, and whether read and write accesses have associated side effects.
RVP.3.527 3.6 (p.50)	I	In RISC-V systems, these properties and capabilities of each region of the machine's physical address space are termed <i>physical memory attributes</i> (PMAs).
RVP.3.528 3.6 (p.50)	I	This section describes RISC-V PMA terminology and how RISC-V systems implement and check PMAs.
RVP.3.529 3.6 (p.50)	R	PMAs are inherent properties of the underlying hardware and rarely change during system operation. Unlike physical memory protection values described in Section 3.7, PMAs do not vary by execution context.
RVP.3.530 3.6 (p.50)	I	The PMAs of some memory regions are fixed at chip design time: for example, for an on-chip ROM. Others are fixed at board design time, depending, for example, on which other chips are connected to off-chip buses.
RVP.3.531 3.6 (p.50)	I	Off-chip buses might also support devices that could be changed on every power cycle (cold pluggable) or dynamically while the system is running (hot pluggable). Some devices might be configurable at run time to support different uses that imply different PMAs: for example, an on-chip scratchpad RAM might be cached privately by one core in one end-application, or accessed as a shared non-cached memory in another end-application.
RVP.3.532 3.6 (p.50)	I	Most systems will require that at least some PMAs are dynamically checked in hardware later in the execution pipeline after the physical address is known, as some operations will not be supported at all physical memory addresses, and some operations require knowing the current setting of a configurable PMA attribute.
RVP.3.533 3.6 (p.50)	I	While many other architectures specify some PMAs in the virtual memory page tables and use the TLB to inform the pipeline of these properties, this approach injects platform-specific information into a virtualized layer and can cause system errors unless attributes are correctly initialized in each page-table entry for each physical memory region. In addition, the available page sizes might not be optimal for specifying attributes in the physical memory space, leading to address-space fragmentation and inefficient use of expensive TLB entries.
RVP.3.534 3.6 (p.50)	R	For RISC-V, we separate out specification and checking of PMAs into a separate hardware structure, the <i>PMA checker</i> .
RVP.3.535 3.6 (p.50)	I	In many cases, the attributes are known at system design time for each physical address region, and can be hardwired into the PMA checker.
RVP.3.536 3.6 (p.50)	I	Where the attributes are run-time configurable, platform-specific memory-mapped control registers can be provided to specify these attributes at a granularity appropriate to each region on the platform (e.g., for an on-chip SRAM that can be flexibly divided between cacheable and uncachable uses).

ID	REFERENCE	TYPE	DEFINITION
RVP.3.537	3.6 (p.50)	R	PMAs are checked for any access to physical memory, including accesses that have undergone virtual to physical memory translation.
RVP.3.538	3.6 (p.50)	R	To aid in system debugging, we strongly recommend that, where possible, RISC-V processors precisely trap physical memory accesses that fail PMA checks.
RVP.3.539	3.6 (p.50)	R	Precisely trapped PMA violations manifest as instruction, load, or store access-fault exceptions, distinct from virtual-memory page-fault exceptions.
RVP.3.540	3.6 (p.50)	R	Precise PMA traps might not always be possible, for example, when probing a legacy bus architecture that uses access failures as part of the discovery mechanism. In this case, error responses from slave devices will be reported as imprecise bus-error interrupts.
RVP.3.541	3.6 (p.51)	R	PMAs must also be readable by software to correctly access certain devices or to correctly configure other hardware components that access memory, such as DMA engines.
RVP.3.542	3.6 (p.51)	I	As PMAs are tightly tied to a given physical platform's organization, many details are inherently platform-specific, as is the means by which software can learn the PMA values for a platform. Some devices, particularly legacy buses, do not support discovery of PMAs and so will give error responses or time out if an unsupported access is attempted. Typically, platform-specific machine-mode code will extract PMAs and ultimately present this information to higher-level less-privileged software using some standard representation.
RVP.3.543	3.6 (p.51)	R	Where platforms support dynamic reconfiguration of PMAs, an interface will be provided to set the attributes by passing requests to a machine-mode driver that can correctly reconfigure the platform.
RVP.3.544	3.6 (p.51)	I	For example, switching cacheability attributes on some memory regions might involve platform-specific operations, such as cache flushes, that are available only to machine-mode.
RVP.3.545	3.6.1 (p.51)	H	Main Memory versus I/O versus Vacant Regions
RVP.3.546	3.6.1 (p.51)	R	The most important characterization of a given memory address range is whether it holds regular main memory, or I/O devices, or is vacant.
RVP.3.547	3.6.1 (p.51)	I	Regular main memory is required to have a number of properties, specified below, whereas I/O devices can have a much broader range of attributes.
RVP.3.548	3.6.1 (p.51)	R	Memory regions that do not fit into regular main memory, for example, device scratchpad RAMs, are categorized as I/O regions.
RVP.3.549	3.6.1 (p.51)	R	Vacant regions are also classified as I/O regions but with attributes specifying that no accesses are supported.
RVP.3.550	3.6.2 (p.51)	H	Supported Access Type PMAs
RVP.3.551	3.6.2 (p.51)	R	Access types specify which access widths, from 8-bit byte to long multi-word burst, are supported, and also whether misaligned accesses are supported for each access width.
RVP.3.552	3.6.2 (p.51)	C	Although software running on a RISC-V hart cannot directly generate bursts to memory, software might have to program DMA engines to access I/O devices and might therefore need to know which access sizes are supported.
RVP.3.553	3.6.2 (p.51)	R	Main memory regions always support read and write of all access widths required by the attached devices, and can specify whether instruction fetch is supported.

ID	REFERENCE	TYPE	DEFINITION
RVP.3.554	3.6.2 (p.51)	C	Some platforms might mandate that all of main memory support instruction fetch. Other platforms might prohibit instruction fetch from some main memory regions
RVP.3.555	3.6.2 (p.51)	C	In some cases, the design of a processor or device accessing main memory might support other widths, but must be able to function with the types supported by the main memory.
RVP.3.556	3.6.2 (p.51)	R	I/O regions can specify which combinations of read, write, or execute accesses to which data widths are supported.
RVP.3.557	3.6.2 (p.51)	R	For systems with page-based virtual memory, I/O and memory regions can specify which combinations of hardware page-table reads and hardware page-table writes are supported.
RVP.3.558	3.6.2 (p.52)	C	Unix-like operating systems generally require that all of cacheable main memory supports page table walks.
RVP.3.559	3.6.3 (p.52)	H	Atomicity PMAs
RVP.3.560	3.6.3 (p.52)	I	Atomicity PMAs describes which atomic instructions are supported in this address region. Support for atomic instructions is divided into two categories: LR/SC and AMOs.
RVP.3.561	3.6.3 (p.52)	C	Some platforms might mandate that all of cacheable main memory support all atomic operations required by the attached processors.
RVP.3.562	3.6.3.1 (p.52)	H	AMO PMA
RVP.3.563	3.6.3.1 (p.52)	R	Within AMOs, there are four levels of support: <i>AMONone</i> , <i>AMOSwap</i> , <i>AMOLogical</i> , and <i>AMOArimetic</i> .
RVP.3.564	3.6.3.1 (p.52)	R	<i>AMONone</i> indicates that no AMO operations are supported.
RVP.3.565	3.6.3.1 (p.52) Figure 3.9	R	<i>AMOSwap</i> indicates that only <code>amoswap</code> instructions are supported in this address range.
RVP.3.566	3.6.3.1 (p.52) Figure 3.9	R	<i>AMOLogical</i> indicates that swap instructions plus all the logical AMOs (<code>amoand</code> , <code>amoor</code> , <code>amoxor</code>) are supported
RVP.3.567	3.6.3.1 (p.52) Figure 3.9	R	<i>AMOArimetic</i> indicates that all RISC-V AMOs are supported (additionally <code>amoadd</code> , <code>amomin</code> , <code>amomax</code> , <code>amominu</code> , <code>amomaxu</code> instructions)
RVP.3.568	3.6.3.1 (p.52)	R	For each level of support, naturally aligned AMOs of a given width are supported if the underlying memory region supports reads and writes of that width.
RVP.3.569	3.6.3.1 (p.52)	R	Main memory and I/O regions may only support a subset or none of the processor-supported atomic operations.
RVP.3.570	3.6.3.1 (p.52)	C	We recommend providing at least <i>AMOLogical</i> support for I/O regions where possible.
RVP.3.571	3.6.3.2 (p.52)	H	Reservability PMA
RVP.3.572	3.6.3.2 (p.52)	R	For LR/SC, there are three levels of support indicating combinations of the reservability and eventuality properties: <i>RsrvNone</i> , <i>RsrvNonEventual</i> , and <i>RsrvEventual</i> .
RVP.3.573	3.6.3.2 (p.52)	R	<i>RsrvNone</i> indicates that no LR/SC operations are supported (the location is non-reservable).
RVP.3.574	3.6.3.2 (p.52)	R	<i>RsrvNonEventual</i> indicates that the operations are supported (the location is reservable), but without the eventual success guarantee described in the unprivileged ISA specification.

ID	REFERENCE	TYPE	DEFINITION
RVP.3.575	3.6.3.2 (p.52)	R	RsrvEventual indicates that the operations are supported and provide the eventual success guarantee.
RVP.3.576	3.6.3.2 (p.53)	C	We recommend providing RsrvEventual support for main memory regions where possible. Most I/O regions will not support LR/SC accesses, as these are most conveniently built on top of a cache-coherence scheme, but some may support RsrvNonEventual or RsrvEventual.
RVP.3.577	3.6.3.2 (p.53)	C	When LR/SC is used for memory locations marked RsrvNonEventual, software should provide alternative fall-back mechanisms used when lack of progress is detected.
RVP.3.578	3.6.3.3 (p.53)	H	Alignment
RVP.3.579	3.6.3.3 (p.53)	R	Memory regions that support aligned LR/SC or aligned AMOs might also support misaligned LR/SC or misaligned AMOs for some addresses and access widths. If, for a given address and access width, a misaligned LR/SC or AMO generates an address-misaligned exception, then all loads, stores, LRs/SCs, and AMOs using that address and access width must generate address-misaligned exceptions.
RVP.3.580	3.6.3.3 (p.53)	C	The standard “A” extension does not support misaligned AMOs or LR/SC pairs. Support for misaligned AMOs is provided by the standard “Zam” extension. Support for misaligned LR/SC sequences is not currently standardized, so LR and SC to misaligned addresses must raise an exception.
RVP.3.581	3.6.3.3 (p.53)	C	Mandating that misaligned loads and stores raise address-misaligned exceptions wherever misaligned AMOs raise address-misaligned exceptions permits the emulation of misaligned AMOs in an M-mode trap handler. The handler guarantees atomicity by acquiring a global mutex and emulating the access within the critical section. Provided that the handler for misaligned loads and stores uses the same mutex, all accesses to a given address that use the same word size will be mutually atomic.
RVP.3.582	3.6.3.3 (p.53)	R	Implementations may raise access-fault exceptions instead of address-misaligned exceptions for some misaligned accesses, indicating the instruction should not be emulated by a trap handler. If, for a given address and access width, all misaligned LRs/SCs and AMOs generate access-fault exceptions, then regular misaligned loads and stores using the same address and access width are not required to execute atomically.
RVP.3.583	3.6.4 (p.53)	H	Memory-Ordering PMAs
RVP.3.584	3.6.4 (p.53)	R	Regions of the address space are classified as either main memory or I/O for the purposes of ordering by the FENCE instruction and atomic-instruction ordering bits.
RVP.3.585	3.6.4 (p.53)	R	Accesses by one hart to main memory regions are observable not only by other harts but also by other devices with the capability to initiate requests in the main memory system (e.g., DMA engines).
RVP.3.586	3.6.4 (p.53)	R	Coherent main memory regions always have either the RVWMO or RVTSO memory model. Incoherent main memory regions have an implementation-defined memory model.
RVP.3.587	3.6.4 (p.53)	R	Accesses by one hart to an I/O region are observable not only by other harts and bus mastering devices but also by targeted slave I/O devices, and I/O regions may be accessed with either relaxed or strong ordering.

ID	REFERENCE	TYPE	DEFINITION
RVP.3.588	3.6.4 (p.53, p.54)	R	Accesses to an I/O region with relaxed ordering are generally observed by other harts and bus mastering devices in a manner similar to the ordering of accesses to an RVWMO memory region, as discussed in Section A.4.2 in Volume I of this specification.
RVP.3.589	3.6.4 (p.54)	R	By contrast, accesses to an I/O region with strong ordering are generally observed by other harts and bus mastering devices in program order.
RVP.3.590	3.6.4 (p.54)	R	Each strongly ordered I/O region specifies a numbered ordering channel, which is a mechanism by which ordering guarantees can be provided between different I/O regions.
RVP.3.591	3.6.4 (p.54)	R	Channel 0 is used to indicate point-to-point strong ordering only, where only accesses by the hart to the single associated I/O region are strongly ordered.
RVP.3.592	3.6.4 (p.54)	R	Channel 1 is used to provide global strong ordering across all I/O regions.
RVP.3.593	3.6.4 (p.54)	R	Any accesses by a hart to any I/O region associated with channel 1 can only be observed to have occurred in program order by all other harts and I/O devices, including relative to accesses made by that hart to relaxed I/O regions or strongly ordered I/O regions with different channel numbers. In other words, any access to a region in channel 1 is equivalent to executing a fence io,io instruction before and after the instruction.
RVP.3.594	3.6.4 (p.54)	R	Other larger channel numbers provide program ordering to accesses by that hart across any regions with the same channel number.
RVP.3.595	3.6.4 (p.54)	R	Systems might support dynamic configuration of ordering properties on each memory region.
RVP.3.596	3.6.4 (p.54)	C	Strong ordering can be used to improve compatibility with legacy device driver code, or to enable increased performance compared to insertion of explicit ordering instructions when the implementation is known to not reorder accesses.
RVP.3.597	3.6.4 (p.54)	C	Local strong ordering (channel 0) is the default form of strong ordering as it is often straightforward to provide if there is only a single in-order communication path between the hart and the I/O device.
RVP.3.598	3.6.4 (p.54)	C	Generally, different strongly ordered I/O regions can share the same ordering channel without additional ordering hardware if they share the same interconnect path and the path does not reorder requests.
RVP.3.599	3.6.5 (p.54)	H	Coherence and Cacheability PMAs
RVP.3.600	3.6.5 (p.54)	I	Coherence is a property defined for a single physical address, and indicates that writes to that address by one agent will eventually be made visible to other agents in the system. Coherence is not to be confused with the memory consistency model of a system, which defines what values a memory read can return given the previous history of reads and writes to the entire memory system.
RVP.3.601	3.6.5 (p.54)	R	In RISC-V platforms, the use of hardware-incoherent regions is discouraged due to software complexity, performance, and energy impacts.
RVP.3.602	3.6.5 (p.54)	R	The cacheability of a memory region should not affect the software view of the region except for differences reflected in other PMAs, such as main memory versus I/O classification, memory ordering, supported accesses and atomic operations, and coherence. For this reason, we treat cacheability as a platform-level setting managed by machine-mode software only.

ID REFERENCE TYPE DEFINITION

RVP.3.603	3.6.5 (p.54)	R	Where a platform supports configurable cacheability settings for a memory region, a platform-specific machine-mode routine will change the settings and flush caches if necessary, so the system is only incoherent during the transition between cacheability settings. This transitory state should not be visible to lower privilege levels.
RVP.3.604	3.6.5 (p.55)	C	We categorize RISC-V caches into three types: master-private, shared, and slave-private. Master-private caches are attached to a single master agent, i.e., one that issues read/write requests to the memory system. Shared caches are located between masters and slaves and may be hierarchically organized. Slave-private caches do not impact coherence, as they are local to a single slave and do not affect other PMAs at a master, so are not considered further here. We use private cache to mean a master-private cache in the following section, unless explicitly stated otherwise.
RVP.3.605	3.6.5 (p.55)	C	Coherence is straightforward to provide for a shared memory region that is not cached by any agent. The PMA for such a region would simply indicate it should not be cached in a private or shared cache.
RVP.3.606	3.6.5 (p.55)	C	Coherence is also straightforward for read-only regions, which can be safely cached by multiple agents without requiring a cache-coherence scheme. The PMA for this region would indicate that it can be cached, but that writes are not supported.
RVP.3.607	3.6.5 (p.55)	C	Some read-write regions might only be accessed by a single agent, in which case they can be cached privately by that agent without requiring a coherence scheme. The PMA for such regions would indicate they can be cached. The data can also be cached in a shared cache, as other agents should not access the region.
RVP.3.608	3.6.5 (p.55)	C	If an agent can cache a read-write region that is accessible by other agents, whether caching or non-caching, a cache-coherence scheme is required to avoid use of stale values. In regions lacking hardware cache coherence (hardware-incoherent regions), cache coherence can be implemented entirely in software, but software coherence schemes are notoriously difficult to implement correctly and often have severe performance impacts due to the need for conservative software-directed cache-flushing. Hardware cache-coherence schemes require more complex hardware and can impact performance due to the cache-coherence probes, but are otherwise invisible to software.
RVP.3.609	3.6.5 (p.55)	C	For each hardware cache-coherent region, the PMA would indicate that the region is coherent and which hardware coherence controller to use if the system has multiple coherence controllers. For some systems, the coherence controller might be an outer-level shared cache, which might itself access further outer-level cache-coherence controllers hierarchically.
RVP.3.610	3.6.5 (p.55)	C	Most memory regions within a platform will be coherent to software, because they will be fixed as either uncached, read-only, hardware cache-coherent, or only accessed by one agent.
RVP.3.611	3.6.5 (p.55)	R	If a PMA indicates non-cacheability, then accesses to that region must be satisfied by the memory itself, not by any caches.
RVP.3.612	3.6.5 (p.55)	C	For implementations with a cacheability-control mechanism, the situation may arise that a program uncacheably accesses a memory location that is currently cache-resident. In this situation, the cached copy must be ignored. This constraint is necessary to prevent more-privileged modes' speculative cache refills from affecting the behavior of less-privileged modes' uncacheable accesses.

ID	REFERENCE	TYPE	DEFINITION
RVP.3.613	3.6.6 (p.55)	H	Idempotency PMAs
RVP.3.614	3.6.6 (p.55)	I	Idempotency PMAs describe whether reads and writes to an address region are idempotent.
RVP.3.615	3.6.6 (p.55)	R	Main memory regions are assumed to be idempotent.
RVP.3.616	3.6.6 (p.55)	R	For I/O regions, idempotency on reads and writes can be specified separately (e.g., reads are idempotent but writes are not).
RVP.3.617	3.6.6 (p.55)	R	If accesses are nonidempotent, i.e., there is potentially a side effect on any read or write access, then speculative or redundant accesses must be avoided.
RVP.3.618	3.6.6 (p.55)	R	For the purposes of defining the idempotency PMAs, changes in observed memory ordering created by redundant accesses are not considered a side effect.
RVP.3.619	3.6.6 (p.56)	C	While hardware should always be designed to avoid speculative or redundant accesses to memory regions marked as non-idempotent, it is also necessary to ensure software or compiler optimizations do not generate spurious accesses to non-idempotent memory regions.
RVP.3.620	3.6.6 (p.56)	C	Non-idempotent regions might not support misaligned accesses. Misaligned accesses to such regions should raise access-fault exceptions rather than address-misaligned exceptions, indicating that software should not emulate the misaligned access using multiple smaller accesses, which could cause unexpected side effects.
RVP.3.621	3.6.6 (p.56)	R	For non-idempotent regions, implicit reads and writes must not be performed early or speculatively, with the following exceptions. When a non-speculative implicit read is performed, an implementation is permitted to additionally read any of the bytes within a naturally aligned power-of-2 region containing the address of the non-speculative implicit read. Furthermore, when a non-speculative instruction fetch is performed, an implementation is permitted to additionally read any of the bytes within the next naturally aligned power-of-2 region of the same size (with the address of the region taken modulo 2^{XLEN}). The results of these additional reads may be used to satisfy subsequent early or speculative implicit reads. The size of these naturally aligned power-of-2 regions is implementation-defined, but, for systems with page-based virtual memory, must not exceed the smallest supported page size.
RVP.3.622	3.7 (p.56)	H	Physical Memory Protection
RVP.3.623	3.7 (p.56)	I	To support secure processing and contain faults, it is desirable to limit the physical addresses accessible by software running on a hart.
RVP.3.624	3.7 (p.56)	R	An optional physical memory protection (PMP) unit provides per-hart machine-mode control registers to allow physical memory access privileges (read, write, execute) to be specified for each physical memory region.
RVP.3.625	3.7 (p.56)	R	The PMP values are checked in parallel with the PMA checks described in Section 3.6.
RVP.3.626	3.7 (p.56)	R	The granularity of PMP access control settings are platform-specific, but the standard PMP encoding supports regions as small as four bytes.
RVP.3.627	3.7 (p.56)	R	Certain regions' privileges can be hardwired: for example, some regions might only ever be visible in machine mode but in no lower-privilege layers.

ID REFERENCE TYPE DEFINITION

- RVP.3.628 3.7 (p.56) C Platforms vary widely in demands for physical memory protection, and some platforms may provide other PMP structures in addition to or instead of the scheme described in this section.
- RVP.3.629 3.7 (p.56) R PMP checks are applied to all accesses whose effective privilege mode is S or U, including instruction fetches in S and U mode, data accesses in S and U mode when the MPRV bit in the mstatus register is clear, and data accesses in any mode when the MPRV bit in mstatus is set and the MPP field in mstatus contains S or U.
- RVP.3.630 3.7 (p.56) R PMP checks are also applied to page-table accesses for virtual-address translation, for which the effective privilege mode is S.
- RVP.3.631 3.7 (p.56) R Optionally, PMP checks may additionally apply to M-mode accesses, in which case the PMP registers themselves are locked, so that even M-mode software cannot change them until the hart is reset. In effect, PMP can grant permissions to S and U modes, which by default have none, and can revoke permissions from M-mode, which by default has full permissions.
- RVP.3.632 3.7 (p.56) R PMP violations are always trapped precisely at the processor.
- RVP.3.633 3.7.1 (p.57) H Physical Memory Protection CSRs
- RVP.3.634 3.7.1 (p.57) R PMP entries are described by an 8-bit configuration register and one MXLEN-bit address register.
- RVP.3.635 3.7.1 (p.57) R Some PMP settings additionally use the address register associated with the preceding PMP entry.
- RVP.3.636 3.7.1 (p.57) R Up to 64 PMP entries are supported.
- RVP.3.637 3.7.1 (p.57) R Implementations may implement zero, 16, or 64 PMP CSRs; the lowest-numbered PMP CSRs must be implemented first.
- RVP.3.638 3.7.1 (p.57) R All PMP CSR fields are WARL and may be read-only zero.
- RVP.3.639 3.7.1 (p.57) R PMP CSRs are only accessible to M-mode.
- RVP.3.640 3.7.1 (p.57) R The PMP configuration registers are densely packed into CSRs to minimize context-switch time.
- RVP.3.641 3.7.1 (p.57)
Figure 3.31 R For RV32, sixteen CSRs, pmpcfg0–pmpcfg15, hold the configurations pmp0cfg–pmp63cfg for the 64 PMP entries, as shown below:

CFG \ bits	31	...	24	23	...	16	15	...	8	7	...	0
pmpcfg0	pmp3cfg		pmp2cfg		pmp1cfg		pmp0cfg					
pmpcfg1	pmp7cfg		pmp6cfg		pmp5cfg		pmp4cfg					
pmpcfg2	pmp11cfg		pmp10cfg		pmp9cfg		pmp8cfg					
pmpcfg3	pmp15cfg		pmp14cfg		pmp13cfg		pmp12cfg					
pmpcfg4	pmp19cfg		pmp18cfg		pmp17cfg		pmp16cfg					
pmpcfg5	pmp23cfg		pmp22cfg		pmp21cfg		pmp20cfg					
pmpcfg6	pmp27cfg		pmp26cfg		pmp25cfg		pmp24cfg					
pmpcfg7	pmp31cfg		pmp30cfg		pmp29cfg		pmp28cfg					
pmpcfg8	pmp35cfg		pmp34cfg		pmp33cfg		pmp32cfg					
pmpcfg9	pmp39cfg		pmp38cfg		pmp37cfg		pmp36cfg					
pmpcfg10	pmp43cfg		pmp42cfg		pmp41cfg		pmp40cfg					
pmpcfg11	pmp47cfg		pmp46cfg		pmp45cfg		pmp44cfg					
pmpcfg12	pmp51cfg		pmp50cfg		pmp49cfg		pmp48cfg					
pmpcfg13	pmp55cfg		pmp54cfg		pmp53cfg		pmp52cfg					
pmpcfg14	pmp59cfg		pmp58cfg		pmp57cfg		pmp56cfg					
pmpcfg15	pmp63cfg		pmp62cfg		pmp61cfg		pmp60cfg					

ID REFERENCE TYPE DEFINITION

RVP.3.642 3.7.1 (p.57) R For RV64, eight even-numbered CSRs, pmpcfg0, pmpcfg2,..., pmpcfg14, hold the configurations for the 64 PMP entries, as shown below:

CFG \ bits	31	...	24	23	...	16	15	...	8	7	...	0
pmpcfg0	pmp3cfg			pmp2cfg			pmp1cfg		pmp0cfg			
pmpcfg2	pmp11cfg			pmp10cfg			pmp9cfg		pmp8cfg			
pmpcfg4	pmp19cfg			pmp18cfg			pmp17cfg		pmp16cfg			
pmpcfg6	pmp27cfg			pmp26cfg			pmp25cfg		pmp24cfg			
pmpcfg8	pmp35cfg			pmp34cfg			pmp33cfg		pmp32cfg			
pmpcfg10	pmp43cfg			pmp42cfg			pmp41cfg		pmp40cfg			
pmpcfg12	pmp51cfg			pmp50cfg			pmp49cfg		pmp48cfg			
pmpcfg14	pmp59cfg			pmp58cfg			pmp57cfg		pmp56cfg			

CFG \ bits	63	...	56	55	...	48	47	...	40	39	...	32
pmpcfg0	pmp7cfg			pmp6cfg			pmp5cfg		pmp4cfg			
pmpcfg2	pmp15cfg			pmp14cfg			pmp13cfg		pmp12cfg			
pmpcfg4	pmp23cfg			pmp22cfg			pmp21cfg		pmp20cfg			
pmpcfg6	pmp31cfg			pmp30cfg			pmp29cfg		pmp28cfg			
pmpcfg8	pmp39cfg			pmp38cfg			pmp37cfg		pmp36cfg			
pmpcfg10	pmp47cfg			pmp46cfg			pmp45cfg		pmp44cfg			
pmpcfg12	pmp55cfg			pmp54cfg			pmp53cfg		pmp52cfg			
pmpcfg14	pmp63cfg			pmp62cfg			pmp61cfg		pmp60cfg			

RVP.3.643 3.7.1 (p.57) R For RV64, the odd-numbered configuration registers, pmpcfg1, pmpcfg3, ..., pmpcfg15, are illegal.

RVP.3.644 3.7.1 (p.57) C RV64 systems use pmpcfg2, rather than pmpcfg1, to hold configurations for PMP entries 8–15. This design reduces the cost of supporting multiple MXLEN values, since the configurations for PMP entries 8–11 appear in pmpcfg2[31:0] for both RV32 and RV64.

RVP.3.645 3.7.1 (p.57) R The PMP address registers are CSRs named pmpaddr0–pmpaddr63.

RVP.3.646 3.7.1 (p.57)
Figure 3.33 R Each PMP address register encodes bits 33–2 of a 34-bit physical address for RV32.

31	...			
address[33:2]				

RVP.3.647 3.7.1 (p.57)
Figure 3.34 R For RV64, each PMP address register encodes bits 55–2 of a 56-bit physical address

63	...	54	53	...	0
address[55:2]					

RVP.3.648 3.7.1 (p.57) R Not all physical address bits may be implemented, and so the pmpaddr registers are WARL.

RVP.3.649 3.7.1 (p.58)
Figure 3.35 R Layout of a PMP configuration register.

7	6	5	4	3	2	1	0
L	0		A		X	W	R

RVP.3.650 3.7.1 (p.58) R The R, W, and X bits, when set, indicate that the PMP entry permits read, write, and instruction execution, respectively. When one of these bits is clear, the corresponding access type is denied.

ID REFERENCE TYPE DEFINITION

- RVP.3.651 3.7.1 (p.58) R The R, W, and X fields form a collective WARL field for which the combinations with R=0 and W=1 are reserved.
- RVP.3.652 3.7.1 (p.58) R Attempting to fetch an instruction from a PMP region that does not have execute permissions raises an instruction access-fault exception.
- RVP.3.653 3.7.1 (p.58) R Attempting to execute a load or load-reserved instruction which accesses a physical address within a PMP region without read permissions raises a load access-fault exception.
- RVP.3.654 3.7.1 (p.58) R Attempting to execute a store, store-conditional, or AMO instruction which accesses a physical address within a PMP region without write permissions raises a store access-fault exception.
- RVP.3.655 3.7.1 (p.58) R If MXLEN is changed, the contents of the `pmpxcfg` fields are preserved, but appear in the `pmpcfg` CSR prescribed by the new setting of MXLEN. For example, when MXLEN is changed from 64 to 32, `pmp4cfg` moves from `pmpcfg0[39:32]` to `pmpcfg1[7:0]`.
- RVP.3.656 3.7.1 (p.58) R The `pmpaddr` CSRs follow the usual CSR width modulation rules described in Section 2.6.
- RVP.3.657 3.7.1 (p.58) H Address Matching
- RVP.3.658 3.7.1 (p.58, p.59)
Table 3.10 R The A field in a PMP entry's configuration register encodes the address-matching mode of the associated PMP address register.
- | A | Name | Description |
|---|-------|---|
| 0 | OFF | Null region (disabled) |
| 1 | TOR | Top of range |
| 2 | NA4 | Naturally aligned four-byte region |
| 3 | NAPOT | Naturally aligned power-of-two region, ≥ 8 bytes |
- RVP.3.659 3.7.1 (p.58) R When A=0, this PMP entry is disabled and matches no addresses.
- RVP.3.660 3.7.1 (p.58) R Two other address-matching modes are supported: naturally aligned power-of-2 regions (NAPOT), including the special case of naturally aligned four-byte regions (NA4); and the top boundary of an arbitrary range (TOR). These modes support four-byte granularity
- RVP.3.661 3.7.1 (p.59)
Table 3.11 R NAPOT ranges make use of the low-order bits of the associated address register to encode the size of the range,

<code>pmpaddr</code>	<code>pmpcfg.A</code>	Match type and size
yyyy...yyyy	NA4	4-byte NAPOT range
yyyy...yy0	NAPOT	8-byte NAPOT range
yyyy...yy01	NAPOT	16-byte NAPOT range
yyyy...y011	NAPOT	32-byte NAPOT range
...
yy01...1111	NAPOT	2^{XLEN} byte NAPOT range
y011...1111	NAPOT	2^{XLEN+1} byte NAPOT range
0111...1111	NAPOT	2^{XLEN+2} -byte NAPOT range
1111...1111	NAPOT	2^{XLEN+3} -byte NAPOT range

ID	REFERENCE	TYPE	DEFINITION
RVP.3.662	3.7.1 (p.59)	R	If TOR is selected, the associated address register forms the top of the address range, and the preceding PMP address register forms the bottom of the address range. If PMP entry i 's A field is set to TOR, the entry matches any address y such that $\text{ppmaddr}_{i-1} \leq y < \text{ppmaddr}_i$ (irrespective of the value of pppcfg_{i-1}). If PMP entry 0's A field is set to TOR, zero is used for the lower bound, and so it matches any address $y < \text{ppmaddr}_0$.
RVP.3.663	3.7.1 (p.59)	C	If $\text{ppmaddr}_{i-1} \geq \text{ppmaddr}_i$ and $\text{pppcfg}_i.A = \text{TOR}$, then PMP entry i matches no addresses.
RVP.3.664	3.7.1 (p.59)	R	Although the PMP mechanism supports regions as small as four bytes, platforms may specify coarser PMP regions. In general, the PMP grain is 2^{G+2} bytes and must be the same across all PMP regions.
RVP.3.665	3.7.1 (p.59)	R	When $G \geq 1$, the NA4 mode is not selectable.
RVP.3.666	3.7.1 (p.59)	R	When $G \geq 2$ and $\text{pppcfg}_i.A[1]$ is set, i.e. the mode is NAPOT, then bits $\text{ppmaddr}_i[G-2:0]$ read as all ones.
RVP.3.667	3.7.1 (p.59)	R	When $G \geq 1$ and $\text{pppcfg}_i.A[1]$ is clear, i.e. the mode is OFF or TOR, then bits $\text{ppmaddr}_i[G-1:0]$ read as all zeros.
RVP.3.668	3.7.1 (p.59)	R	Bits $\text{ppmaddr}_i[G-1:0]$ do not affect the TOR address-matching logic.
RVP.3.669	3.7.1 (p.59)	R	Although changing $\text{pppcfg}_i.A[1]$ affects the value read from ppmaddr_i , it does not affect the underlying value stored in that register: in particular, $\text{ppmaddr}_i[G-1]$ retains its original value when $\text{pppcfg}_i.A$ is changed from NAPOT to TOR/OFF then back to NAPOT.
RVP.3.670	3.7.1 (p.59)	C	Software may determine the PMP granularity by writing zero to ppm0cfg , then writing all ones to ppmaddr_0 , then reading back ppmaddr_0 . If G is the index of the least-significant bit set, the PMP granularity is 2^{G+2} bytes.
RVP.3.671	3.7.1 (p.60)	R	If the current XLEN is greater than MXLEN, the PMP address registers are zero-extended from MXLEN to XLEN bits for the purposes of address matching.
RVP.3.672	3.7.1 (p.60)	H	Locking and Privilege Mode
RVP.3.673	3.7.1 (p.60)	R	The L bit indicates that the PMP entry is locked, i.e., writes to the configuration register and associated address registers are ignored.
RVP.3.674	3.7.1 (p.60)	R	Locked PMP entries remain locked until the hart is reset.
RVP.3.675	3.7.1 (p.60)	R	If PMP entry i is locked, writes to pppicfg and ppmaddr_i are ignored.
RVP.3.676	3.7.1 (p.60)	R	Additionally, if PMP entry i is locked and $\text{pppicfg}.A$ is set to TOR, writes to ppmaddr_{i-1} are ignored.
RVP.3.677	3.7.1 (p.60)	C	Setting the L bit locks the PMP entry even when the A field is set to OFF.
RVP.3.678	3.7.1 (p.60)	R	In addition to locking the PMP entry, the L bit indicates whether the R/W/X permissions are enforced on M-mode accesses. When the L bit is set, these permissions are enforced for all privilege modes. When the L bit is clear, any M-mode access matching the PMP entry will succeed; the R/W/X permissions apply only to S and U modes.
RVP.3.679	3.7.1 (p.60)	H	Priority and Matching Logic
RVP.3.680	3.7.1 (p.60)	R	PMP entries are statically prioritized. The lowest-numbered PMP entry that matches any byte of an access determines whether that access succeeds or fails.

ID	REFERENCE	TYPE	DEFINITION
RVP.3.681	3.7.1 (p.60)	R	The matching PMP entry must match all bytes of an access, or the access fails, irrespective of the L, R, W, and X bits.
RVP.3.682	3.7.1 (p.60)	I	For example, if a PMP entry is configured to match the four-byte range 0xC–0xF, then an 8-byte access to the range 0x8–0xF will fail, assuming that PMP entry is the highest-priority entry that matches those addresses.
RVP.3.683	3.7.1 (p.60)	R	If a PMP entry matches all bytes of an access, then the L, R, W, and X bits determine whether the access succeeds or fails.
RVP.3.684	3.7.1 (p.60)	R	If the L bit is clear and the privilege mode of the access is M, the access succeeds.
RVP.3.685	3.7.1 (p.60)	R	Otherwise, if the L bit is set or the privilege mode of the access is S or U, then the access succeeds only if the R, W, or X bit corresponding to the access type is set.
RVP.3.686	3.7.1 (p.60)	R	If no PMP entry matches an M-mode access, the access succeeds.
RVP.3.687	3.7.1 (p.60)	R	If no PMP entry matches an S-mode or U-mode access, but at least one PMP entry is implemented, the access fails.
RVP.3.688	3.7.1 (p.60)	C	If at least one PMP entry is implemented, but all PMP entries' A fields are set to OFF, then all S-mode and U-mode memory accesses will fail.
RVP.3.689	3.7.1 (p.60)	R	Failed accesses generate an instruction, load, or store access-fault exception.
RVP.3.690	3.7.1 (p.60)	R	Note that a single instruction may generate multiple accesses, which may not be mutually atomic. An access-fault exception is generated if at least one access generated by an instruction fails, though other accesses generated by that instruction may succeed with visible side effects. Notably, instructions that reference virtual memory are decomposed into multiple accesses.
RVP.3.691	3.7.1 (p.60)	R	On some implementations, misaligned loads, stores, and instruction fetches may also be decomposed into multiple accesses, some of which may succeed before an access-fault exception occurs.
RVP.3.692	3.7.1 (p.60, p.61)	R	In particular, a portion of a misaligned store that passes the PMP check may become visible, even if another portion fails the PMP check.
RVP.3.693	3.7.1 (p.61)	R	The same behavior may manifest for floating-point stores wider than XLEN bits (e.g., the FSD instruction in RV32D), even when the store address is naturally aligned.
RVP.3.694	3.7.2 (p.61)	H	Physical Memory Protection and Paging
RVP.3.695	3.7.2 (p.61)	R	The Physical Memory Protection mechanism is designed to compose with the page-based virtual memory systems described in Chapter 4.
RVP.3.696	3.7.2 (p.61)	R	When paging is enabled, instructions that access virtual memory may result in multiple physical-memory accesses, including implicit references to the page tables.
RVP.3.697	3.7.2 (p.61)	R	The PMP checks apply to all of these accesses.
RVP.3.698	3.7.2 (p.61)	R	The effective privilege mode for implicit page-table accesses is S.
RVP.3.699	3.7.2 (p.61)	R	Implementations with virtual memory are permitted to perform address translations speculatively and earlier than required by an explicit memory access, and are permitted to cache them in address translation cache structures—including possibly caching the identity mappings from effective address to physical address used in Bare translation modes and M-mode.

ID REFERENCE TYPE DEFINITION

- | | | | |
|-----------|--------------|---|---|
| RVP.3.700 | 3.7.2 (p.61) | R | The PMP settings for the resulting physical address may be checked (and possibly cached) at any point between the address translation and the explicit memory access. |
| RVP.3.701 | 3.7.2 (p.61) | R | Hence, when the PMP settings are modified, M-mode software must synchronize the PMP settings with the virtual memory system and any PMP or address-translation caches. This is accomplished by executing an SFENCE.VMA instruction with $rs1=x0$ and $rs2=x0$, after the PMP CSRs are written. |
| RVP.3.702 | 3.7.2 (p.61) | R | If page-based virtual memory is not implemented, memory accesses check the PMP settings synchronously, so no SFENCE.VMA is needed. |

CHAPTER 4 Supervisor-Level ISA

ID	REFERENCE	TYPE	DEFINITION
RVP.4.1	4.0 (p.63)	H	Supervisor-Level ISA
RVP.4.2	4.0 (p.63) preface (p.i)	I	Supervisor Level ISA extension version is 1.12 and status is ratified.
RVP.4.3	4.0 (p.63)	I	This chapter describes the RISC-V supervisor-level architecture, which contains a common core that is used with various supervisor-level address translation and protection schemes.
RVP.4.4	4.0 (p.63)	C	Supervisor mode is deliberately restricted in terms of interactions with underlying physical hardware, such as physical memory and device interrupts, to support clean virtualization. In this spirit, certain supervisor-level facilities, including requests for timer and interprocessor interrupts, are provided by implementation-specific mechanisms. In some systems, a supervisor execution environment (SEE) provides these facilities in a manner specified by a supervisor binary interface (SBI). Other systems supply these facilities directly, through some other implementation defined mechanism.
RVP.4.5	4.1 (p.63)	H	Supervisor CSRs
RVP.4.6	4.1 (p.63)	I	A number of CSRs are provided for the supervisor
RVP.4.7	4.1 (p.63)	C	The supervisor should only view CSR state that should be visible to a supervisor-level operating system. In particular, there is no information about the existence (or non-existence) of higher privilege levels (machine level or other) visible in the CSRs accessible by the supervisor.
RVP.4.8	4.1 (p.63)	C	Many supervisor CSRs are a subset of the equivalent machine-mode CSR, and the machinemode chapter should be read first to help understand the supervisor-level CSR descriptions.
RVP.4.9	4.1.1 (p.63)	H	Supervisor Status Register (<code>sstatus</code>)
RVP.4.10	4.1.1 (p.63)	R	The <code>sstatus</code> register is an SXLEN-bit read/write register
RVP.4.11	4.1.1 (p.63)	R	The <code>sstatus</code> register keeps track of the processor's current operating state.
RVP.4.12	4.1.1 (p.64) Figure 4.1	R	Supervisor-mode status register (<code>sstatus</code>) when SXLEN=32.

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
SD												MXR	SUM	WPRI

16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
XS	FS	WPRI	VS	SPP	WPRI	UBE	SPIE	WPRI	SIE	WPRI						

ID REFERENCE TYPE DEFINITION

RVP.4.13 4.1.1 (p.64) R supervisor-mode status register (`sstatus`) when SXLEN=64.
Figure 4.2

63	62	61	...	39	38	37	36	35	34	33	32
SD	WPRI									UXL	

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
WPRI									MXR	SUM	WPRI			

16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
XS	FS	WPRI	VS	SPP	WPRI	UBE	SPIE	WPRI	SIE	WPRI						

RVP.4.14 4.1.1 (p.63) R The SPP bit indicates the privilege level at which a hart was executing before entering supervisor mode.

RVP.4.15 4.1.1 (p.63) R When a trap is taken, SPP is set to 0 if the trap originated from user mode, or 1 otherwise.

RVP.4.16 4.1.1 (p.63, p.64) R When an SRET instruction (see Section 3.3.2) is executed to return from the trap handler, the privilege level is set to user mode if the SPP bit is 0, or supervisor mode if the SPP bit is 1; SPP is then set to 0.

RVP.4.17 4.1.1 (p.64) R The SIE bit enables or disables all interrupts in supervisor mode.

RVP.4.18 4.1.1 (p.64) R When SIE is clear, interrupts are not taken while in supervisor mode.

RVP.4.19 4.1.1 (p.64) R When the hart is running in user-mode, the value in SIE is ignored, and supervisor-level interrupts are enabled.

RVP.4.20 4.1.1 (p.64) R The supervisor can disable individual interrupt sources using the `sie` CSR.

RVP.4.21 4.1.1 (p.64) R The SPIE bit indicates whether supervisor interrupts were enabled prior to trapping into supervisor mode.

RVP.4.22 4.1.1 (p.64) R When a trap is taken into supervisor mode, SPIE is set to SIE, and SIE is set to 0.

RVP.4.23 4.1.1 (p.64) R When an SRET instruction is executed, SIE is set to SPIE, then SPIE is set to 1.

RVP.4.24 4.1.1 (p.64) I The `sstatus` register is a subset of the `mstatus` register.

RVP.4.25 4.1.1 (p.64) C In a straightforward implementation, reading or writing any field in `sstatus` is equivalent to reading or writing the homonymous field in `mstatus`.

RVP.4.26 4.1.1.1 (p.64) H Base ISA Control in `sstatus` Register

RVP.4.27 4.1.1.1 (p.64) R Table 3.1 The UXL field controls the value of XLEN for U-mode, termed UXLEN, which may differ from the value of XLEN for S-mode, termed SXLEN. The encoding of UXL is the same as that of the MXL field of `misa`.

UXL	UXLEN
1	32
2	64
3	128

RVP.4.28 4.1.1.1 (p.64) R When SXLEN=32, the UXL field does not exist, and UXLEN=32.

RVP.4.29 4.1.1.1 (p.64) R When SXLEN=64, it (UXL field) is a WARL field that encodes the current value of UXLEN.

ID	REFERENCE	TYPE	DEFINITION
RVP.4.30	4.1.1.1 (p.64)	R	In particular, an implementation may make UXL be a read-only field whose value always ensures that UXLEN=SXLEN.
RVP.4.31	4.1.1.1 (p.65)	R	If UXLEN ≠ SXLEN, instructions executed in the narrower mode must ignore source register operand bits above the configured XLEN, and must sign-extend results to fill the widest supported XLEN in the destination register.
RVP.4.32	4.1.1.1 (p.65)	R	If UXLEN < SXLEN, user-mode instruction-fetch addresses and load and store effective addresses are taken modulo 2^{UXLEN} . For example, when UXLEN=32 and SXLEN=64, user-mode memory accesses reference the lowest 4 GiB of the address space.
RVP.4.33	4.1.1.2 (p.65)	R	Memory Privilege in <code>sstatus</code> Register
RVP.4.34	4.1.1.2 (p.65)	R	The MXR (Make eXecutable Readable) bit modifies the privilege with which loads access virtual memory.
RVP.4.35	4.1.1.2 (p.65)	R	When MXR=0, only loads from pages marked readable (R=1 in RVP.4.234) will succeed.
RVP.4.36	4.1.1.2 (p.65)	R	When MXR=1, loads from pages marked either readable or executable (R=1 or X=1 in RVP.4.234) will succeed
RVP.4.37	4.1.1.2 (p.65)	R	MXR has no effect when page-based virtual memory is not in effect.
RVP.4.38	4.1.1.2 (p.65)	R	The SUM (permit Supervisor User Memory access) bit modifies the privilege with which S-mode loads and stores access virtual memory.
RVP.4.39	4.1.1.2 (p.65)	R	When SUM=0, S-mode memory accesses to pages that are accessible by U-mode (U=1 in RVP.4.234) will fault.
RVP.4.40	4.1.1.2 (p.65)	R	When SUM=1, these accesses (S-mode memory accesses to pages that are accessible by U-mode) are permitted.
RVP.4.41	4.1.1.2 (p.65)	R	SUM has no effect when page-based virtual memory is not in effect, nor when executing in U-mode.
RVP.4.42	4.1.1.2 (p.65)	R	Note that S-mode can never execute instructions from user pages, regardless of the state of SUM.
RVP.4.43	4.1.1.2 (p.65)	R	SUM is read-only 0 if satp.MODE is read-only 0.
RVP.4.44	4.1.1.2 (p.65)	C	The SUM mechanism prevents supervisor software from inadvertently accessing user memory. Operating systems can execute the majority of code with SUM clear; the few code segments that should access user memory can temporarily set SUM.
RVP.4.45	4.1.1.2 (p.65)	C	The SUM mechanism does not avail S-mode software of permission to execute instructions in user code pages. Legitimate uses cases for execution from user memory in supervisor context are rare in general and nonexistent in POSIX environments. However, bugs in supervisors that lead to arbitrary code execution are much easier to exploit if the supervisor exploit code can be stored in a user buffer at a virtual address chosen by an attacker.
RVP.4.46	4.1.1.2 (p.65)	C	Some non-POSIX single address space operating systems do allow certain privileged software to partially execute in supervisor mode, while most programs run in user mode, all in a shared address space. This use case can be realized by mapping the physical code pages at multiple virtual addresses with different permissions, possibly with the assistance of the instruction pagefault handler to direct supervisor software to use the alternate mapping.
RVP.4.47	4.1.1.3 (p.65)	H	Endianness Control in <code>sstatus</code> Register

ID REFERENCE TYPE DEFINITION

RVP.4.48	4.1.1.3 (p.65)	R	The UBE bit is aWARL field that controls the endianness of explicit memory accesses made from U-mode, which may differ from the endianness of memory accesses in S-mode.												
RVP.4.49	4.1.1.3 (p.65)	R	An implementation may make UBE be a read-only field that always specifies the same endianness as for S-mode.												
RVP.4.50	4.1.1.3 (p.65)	R	UBE controls whether explicit load and store memory accesses made from U-mode are little-endian (UBE=0) or big-endian (UBE=1).												
RVP.4.51	4.1.1.3 (p.65)	R	UBE has no effect on instruction fetches, which are implicit memory accesses that are always little-endian.												
RVP.4.52	4.1.1.3 (p.66)	R	For <i>implicit</i> accesses to supervisor-level memory management data structures, such as page tables, S-mode endianness always applies and UBE is ignored.												
RVP.4.53	4.1.1.3 (p.66)	C	Standard RISC-V ABIs are expected to be purely little-endian-only or big-endian-only, with no accommodation for mixing endianness. Nevertheless, endianness control has been defined so as to permit an OS of one endianness to execute user-mode programs of the opposite endianness.												
RVP.4.54	4.1.2 (p.66)	H	Supervisor Trap Vector Base Address Register (<code>stvec</code>)												
RVP.4.55	4.1.2 (p.66)	R	The <code>stvec</code> register is an SXLEN-bit read/write register that holds trap vector configuration, consisting of a vector base address (BASE) and a vector mode (MODE).												
RVP.4.56	4.1.2 (p.66) Figure 4.3	R	Supervisor trap vector base address register (<code>stvec</code>)												
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>SXLEN-1</td> <td>...</td> <td>2</td> <td>1</td> <td>0</td> </tr> <tr> <td colspan="3">BASE[SXLEN-1:2]</td> <td colspan="2">MODE</td> </tr> </table>	SXLEN-1	...	2	1	0	BASE[SXLEN-1:2]			MODE			
SXLEN-1	...	2	1	0											
BASE[SXLEN-1:2]			MODE												
RVP.4.57	4.1.2 (p.66)	R	The BASE field in <code>stvec</code> is a WARL field that can hold any valid virtual or physical address, subject to the following alignment constraints: the address must be 4-byte aligned, and MODE settings other than Direct might impose additional alignment constraints on the value in the BASE field.												
RVP.4.58	4.1.2 (p.66) Table 4.1	R	The encoding of the MODE field is shown in the table below.												
			<table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>VALUE</th> <th>NAME</th> <th>DESCRIPTION</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Direct</td> <td>All exceptions set pc to BASE.</td> </tr> <tr> <td>1</td> <td>Vectored</td> <td>Asynchronous interrupts set pc to BASE+4×cause.</td> </tr> <tr> <td>2, 3</td> <td>-</td> <td>Reserved</td> </tr> </tbody> </table>	VALUE	NAME	DESCRIPTION	0	Direct	All exceptions set pc to BASE.	1	Vectored	Asynchronous interrupts set pc to BASE+4×cause.	2, 3	-	Reserved
VALUE	NAME	DESCRIPTION													
0	Direct	All exceptions set pc to BASE.													
1	Vectored	Asynchronous interrupts set pc to BASE+4×cause.													
2, 3	-	Reserved													
RVP.4.59	4.1.2 (p.66)	R	When MODE=Direct, all traps into supervisor mode cause the pc to be set to the address in the BASE field.												
RVP.4.60	4.1.2 (p.66)	R	When MODE=Vectored, all synchronous exceptions into supervisor mode cause the pc to be set to the address in the BASE field, whereas interrupts cause the pc to be set to the address in the BASE field plus four times the interrupt cause number. For example, a supervisor-mode timer interrupt (see RVP.4.127) causes the pc to be set to BASE+0x14. Setting MODE=Vectored may impose a stricter alignment constraint on BASE.												
RVP.4.61	4.1.3 (p.66)	H	Supervisor Interrupt Registers (<code>sip</code> and <code>sie</code>)												
RVP.4.62	4.1.3 (p.66)	R	The <code>sip</code> (Supervisor interrupt-pending) register is an SXLEN-bit read/write register containing information on pending interrupts, ...												

ID	REFERENCE	TYPE	DEFINITION																																
RVP.4.63	4.1.3 (p.66)	R	... while <code>sie</code> (Supervisor interrupt-enable) register is the corresponding <code>SXLEN</code> -bit read/write register containing interrupt enable bits.																																
RVP.4.64	4.1.3 (p.66)	R	Interrupt cause number i (as reported in CSR <code>scause</code>) corresponds with bit i in both <code>sip</code> and <code>sie</code> .																																
RVP.4.65	4.1.3 (p.66) Figure 4.4	R	Supervisor Interrupt-Pending Register (<code>sip</code>).																																
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 2px;">SXLEN-1</td> <td style="padding: 2px;">...</td> <td style="padding: 2px;">0</td> </tr> <tr> <td colspan="2" style="padding: 2px;">Interrupts (WARL)</td> <td style="padding: 2px;"></td> </tr> </table>	SXLEN-1	...	0	Interrupts (WARL)																												
SXLEN-1	...	0																																	
Interrupts (WARL)																																			
RVP.4.66	4.1.3 (p.66) Figure 4.5	R	Supervisor Interrupt-Enable Register (<code>sie</code>).																																
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 2px;">SXLEN-1</td> <td style="padding: 2px;">...</td> <td style="padding: 2px;">0</td> </tr> <tr> <td colspan="2" style="padding: 2px;">Interrupts (WARL)</td> <td style="padding: 2px;"></td> </tr> </table>	SXLEN-1	...	0	Interrupts (WARL)																												
SXLEN-1	...	0																																	
Interrupts (WARL)																																			
RVP.4.67	4.1.3 (p.66)	R	Bits 15:0 are allocated to standard interrupt causes only, while bits 16 and above are designated for platform or custom use.																																
RVP.4.68	4.1.3 (p.67)	R	An interrupt i will trap to S-mode if both of the following are true: (a) either the current privilege mode is S and the SIE bit in the <code>sstatus</code> register is set, or the current privilege mode has less privilege than S-mode; and (b) bit i is set in both <code>sip</code> and <code>sie</code> .																																
RVP.4.69	4.1.3 (p.67)	R	These conditions for an interrupt trap to occur must be evaluated in a bounded amount of time from when an interrupt becomes, or ceases to be, pending in <code>sip</code> , and must also be evaluated immediately following the execution of an <code>SRET</code> instruction or an explicit write to a CSR on which these interrupt trap conditions expressly depend (including <code>sip</code> , <code>sie</code> and <code>sstatus</code>).																																
RVP.4.70	4.1.3 (p.67)	R	Interrupts to S-mode take priority over any interrupts to lower privilege modes.																																
RVP.4.71	4.1.3 (p.67)	R	Each individual bit in register <code>sip</code> may be writable or may be read-only.																																
RVP.4.72	4.1.3 (p.67)	R	When bit i in <code>sip</code> is writable, a pending interrupt i can be cleared by writing 0 to this bit.																																
RVP.4.73	4.1.3 (p.67)	R	If interrupt i can become pending but bit i in <code>sip</code> is read-only, the implementation must provide some other mechanism for clearing the pending interrupt (which may involve a call to the execution environment).																																
RVP.4.74	4.1.3 (p.67)	R	A bit in <code>sie</code> must be writable if the corresponding interrupt can ever become pending. Bits of <code>sie</code> that are not writable are read-only zero.																																
RVP.4.75	4.1.3 (p.67)	R	Bits of <code>sie</code> that are not writable are read-only zero.																																
RVP.4.76	4.1.3 (p.67) Figure 4.6	R	The standard portions (bits 15:0) of registers <code>sip</code> are formatted as																																
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 2px;">15</td><td style="padding: 2px;">14</td><td style="padding: 2px;">13</td><td style="padding: 2px;">12</td><td style="padding: 2px;">11</td><td style="padding: 2px;">10</td><td style="padding: 2px;">9</td><td style="padding: 2px;">8</td><td style="padding: 2px;">7</td><td style="padding: 2px;">6</td><td style="padding: 2px;">5</td><td style="padding: 2px;">4</td><td style="padding: 2px;">3</td><td style="padding: 2px;">2</td><td style="padding: 2px;">1</td><td style="padding: 2px;">0</td> </tr> <tr> <td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">SEIP</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">STIP</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">SSIP</td><td style="padding: 2px;">0</td> </tr> </table>	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	0	0	0	0	0	0	SEIP	0	0	0	STIP	0	0	0	SSIP	0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0																				
0	0	0	0	0	0	SEIP	0	0	0	STIP	0	0	0	SSIP	0																				
RVP.4.77	4.1.3 (p.67) Figure 4.7	R	The standard portions (bits 15:0) of registers <code>sie</code> are formatted as																																
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="padding: 2px;">15</td><td style="padding: 2px;">14</td><td style="padding: 2px;">13</td><td style="padding: 2px;">12</td><td style="padding: 2px;">11</td><td style="padding: 2px;">10</td><td style="padding: 2px;">9</td><td style="padding: 2px;">8</td><td style="padding: 2px;">7</td><td style="padding: 2px;">6</td><td style="padding: 2px;">5</td><td style="padding: 2px;">4</td><td style="padding: 2px;">3</td><td style="padding: 2px;">2</td><td style="padding: 2px;">1</td><td style="padding: 2px;">0</td> </tr> <tr> <td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">SEIE</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">STIE</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">0</td><td style="padding: 2px;">SSIE</td><td style="padding: 2px;">0</td> </tr> </table>	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	0	0	0	0	0	0	SEIE	0	0	0	STIE	0	0	0	SSIE	0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0																				
0	0	0	0	0	0	SEIE	0	0	0	STIE	0	0	0	SSIE	0																				
RVP.4.78	4.1.3 (p.67)	R	Bits <code>sip.SEIP</code> and <code>sie.SEIE</code> are the interrupt-pending and interrupt-enable bits for supervisor level external interrupts.																																

ID	REFERENCE	TYPE	DEFINITION
RVP.4.79	4.1.3 (p.67)	R	If implemented, SEIP is read-only in <code>sip</code> , and is set and cleared by the execution environment, typically through a platform-specific interrupt controller.
RVP.4.80	4.1.3 (p.68)	R	Bits <code>sip.STIP</code> and <code>sie.STIE</code> are the interrupt-pending and interrupt-enable bits for supervisor-level timer interrupts.
RVP.4.81	4.1.3 (p.68)	R	If implemented, STIP is read-only in <code>sip</code> , and is set and cleared by the execution environment.
RVP.4.82	4.1.3 (p.68)	R	Bits <code>sip.SSIP</code> and <code>sie.SSIE</code> are the interrupt-pending and interrupt-enable bits for supervisor-level software interrupts.
RVP.4.83	4.1.3 (p.68)	R	If implemented, SSIP is writable in <code>sip</code> and may also be set to 1 by a platform-specific interrupt controller.
RVP.4.84	4.1.3 (p.68)	C	Interprocessor interrupts are sent to other harts by implementation-specific means, which will ultimately cause the SSIP bit to be set in the recipient hart's <code>sip</code> register.
RVP.4.85	4.1.3 (p.68)	R	Each standard interrupt type (SEI, STI, or SSI) may not be implemented, in which case the corresponding interrupt-pending and interrupt-enable bits are read-only zeros.
RVP.4.86	4.1.3 (p.68)	R	All bits in <code>sip</code> and <code>sie</code> are WARL fields.
RVP.4.87	4.1.3 (p.68)	R	The implemented interrupts may be found by writing one to every bit location in <code>sie</code> , then reading back to see which bit positions hold a one.
RVP.4.88	4.1.3 (p.68)	C	The <code>sip</code> and <code>sie</code> registers are subsets of the <code>mip</code> and <code>mie</code> registers. Reading any implemented field, or writing any writable field, of <code>sip/sie</code> effects a read or write of the homonymous field of <code>mip/mie</code> .
RVP.4.89	4.1.3 (p.68)	C	Bits 3, 7, and 11 of <code>sip</code> and <code>sie</code> correspond to the machine-mode software, timer, and external interrupts, respectively. Since most platforms will choose not to make these interrupts delegatable from M-mode to S-mode, they are shown as 0 .
RVP.4.90	4.1.3 (p.68)	R	Multiple simultaneous interrupts destined for supervisor mode are handled in the following decreasing priority order: SEI, SSI, STI.
RVP.4.91	4.1.4 (p.68)	H	Supervisor Timers and Performance Counters
RVP.4.92	4.1.4 (p.68)	R	Supervisor software uses the same hardware performance monitoring facility as user-mode software, including the <code>time</code> , <code>cycle</code> , and <code>instret</code> CSRs.
RVP.4.93	4.1.4 (p.68)	R	The implementation should provide a mechanism to modify the counter values.
RVP.4.94	4.1.4 (p.68)	R	The implementation must provide a facility for scheduling timer interrupts in terms of the real-time counter, <code>time</code> .
RVP.4.95	4.1.5 (p.68)	H	Counter-Enable Register (<code>scounteren</code>)
RVP.4.96	4.1.5 (p.68)	R	The counter-enable register <code>scounteren</code> is a 32-bit register that controls the availability of the hardware performance monitoring counters to U-mode.
RVP.4.97	4.1.5 (p.68) Figure 4.8	R	Counter-enable register (<code>scounteren</code>)

31	30	29	...	5	4	3	2	1	0
HPM31	HPM30	HPM29	...	HPM5	HPM4	HPM3	IR	TM	CY

ID	REFERENCE	TYPE	DEFINITION						
RVP.4.98	4.1.5 (p.69)	R	When the CY, TM, IR, or HPM n bit in the scounteren register is clear, attempts to read the cycle, time, instret, or hpmcountern register while executing in U-mode will cause an illegal instruction exception. When one of these bits is set, access to the corresponding register is permitted.						
RVP.4.99	4.1.5 (p.69)	R	scounteren must be implemented. However, any of the bits may be read-only zero, indicating reads to the corresponding counter will cause an exception when executing in U-mode. Hence, they are effectively WARL fields.						
RVP.4.100	4.1.5 (p.69)	C	The setting of a bit in mcounteren does not affect whether the corresponding bit in scounteren is writable. However, U-mode may only access a counter if the corresponding bits in scounteren and mcounteren are both set.						
RVP.4.101	4.1.6 (p.69)	H	Supervisor Scratch Register (sscratch)						
RVP.4.102	4.1.6 (p.69)	R	The sscratch register is an SXLEN-bit read/write register, dedicated for use by the supervisor.						
RVP.4.103	4.1.6 (p.69)	R	Typically, sscratch is used to hold a pointer to the hart-local supervisor context while the hart is executing user code.						
RVP.4.104	4.1.6 (p.69)	R	At the beginning of a trap handler, sscratch is swapped with a user register to provide an initial working register.						
RVP.4.105	4.1.6 (p.69) Figure 4.9	R	Supervisor Scratch Register (sscratch).						
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>SXLEN-1</td> <td>...</td> <td>0</td> </tr> <tr> <td colspan="2"></td> <td>sscratch</td> </tr> </table>	SXLEN-1	...	0			sscratch
SXLEN-1	...	0							
		sscratch							
RVP.4.106	4.1.7 (p.69)	H	Supervisor Exception Program Counter (sepc)						
RVP.4.107	4.1.7 (p.69)	R	sepc is an SXLEN-bit read/write register						
RVP.4.108	4.1.7 (p.69)	R	The low bit of sepc (sepc[0]) is always zero.						
RVP.4.109	4.1.7 (p.69)	R	On implementations that support only IALIGN=32, the two low bits (sepc[1:0]) are always zero.						
RVP.4.110	4.1.7 (p.69)	R	If an implementation allows IALIGN to be either 16 or 32 (by changing CSR misa, for example), then, whenever IALIGN=32, bit sepc[1] is masked on reads so that it appears to be 0.						
RVP.4.111	4.1.7 (p.69)	R	This masking (sepc[1] appears to be 0) occurs also for the implicit read by the SRET instruction.						
RVP.4.112	4.1.7 (p.69)	R	Though masked, sepc[1] remains writable when IALIGN=32.						
RVP.4.113	4.1.7 (p.69)	R	sepc is a WARL register that must be able to hold all valid virtual addresses. It need not be capable of holding all possible invalid addresses.						
RVP.4.114	4.1.7 (p.69)	R	Prior to writing sepc, implementations may convert an invalid address into some other invalid address that sepc is capable of holding.						
RVP.4.115	4.1.7 (p.69)	R	When a trap is taken into S-mode, sepc is written with the virtual address of the instruction that was interrupted or that encountered the exception.						
RVP.4.116	4.1.7 (p.69)	R	Otherwise, sepc is never written by the implementation, though it may be explicitly written by software.						

ID REFERENCE TYPE DEFINITION

RVP.4.117 4.1.7 (p.70) R Supervisor exception program counter register (`sepc`).
 Figure 4.10

SXLEN-1	...	0
sepc		

RVP.4.118 4.1.8 (p.70) H Supervisor Cause Register (`scause`)

RVP.4.119 4.1.8 (p.70) R The `scause` register is an SXLEN-bit read-write register

RVP.4.120 4.1.8 (p.70)
 Figure 4.11 R Supervisor Cause Register (`scause`)

SXLEN-1	SXLEN-2	...	0
Interrupt	Exception Code		

RVP.4.121 4.1.8 (p.70) R When a trap is taken into S-mode, `scause` is written with a code indicating the event that caused the trap.

RVP.4.122 4.1.8 (p.70) R Otherwise, `scause` is never written by the implementation, though it may be explicitly written by software.

RVP.4.123 4.1.8 (p.70) R The Interrupt bit in the `scause` register is set if the trap was caused by an interrupt.

RVP.4.124 4.1.8 (p.70) R The Exception Code field contains a code identifying the last exception or interrupt.

RVP.4.125 4.1.8 (p.70) R The Exception Code is a WLRL field.

RVP.4.126 4.1.8 (p.70) R It (Exception Code) is required to hold the values 0–31 (i.e., bits 4–0 must be implemented), but otherwise it is only guaranteed to hold supported exception codes.

ID REFERENCE TYPE DEFINITION

RVP.4.127 4.1.8 (p.71) R Supervisor cause register (`scause`) values after trap (the possible exception codes for the current supervisor ISAs.).
 Table 4.2 Synchronous exception priorities are given by RVP.3.392.

Interrupt	Exception Code	Description
1	0	Reserved
1	1	Supervisor software interrupt
1	2-4	Reserved
1	5	Supervisor timer interrupt
1	6-8	Reserved
1	9	Supervisor external interrupt
1	10-15	Reserved
1	≥ 16	Designated for platform use
0	0	Instruction address misaligned
0	1	Instruction access fault
0	2	Illegal instruction
0	3	Breakpoint
0	4	Load address misaligned
0	5	Load access fault
0	6	Store/AMO address misaligned
0	7	Store/AMO access fault
0	8	Environment call from U-mode
0	9	Environment call from S-mode
0	10-11	Reserved
0	12	Instruction page fault
0	13	Load page fault
0	14	Reserved
0	15	Store/AMO page fault
0	16 - 23	Reserved
0	24 - 31	Designated for custom use
0	32 - 47	Reserved
0	48 - 63	Designated for custom use
0	≥ 64	Reserved

RVP.4.128 4.1.9 (p.70) H Supervisor Trap Value (`stval`) Register

RVP.4.129 4.1.9 (p.70) R The `stval` register is an SXLEN-bit read-write register

RVP.4.130 4.1.9 (p.70)
 Figure 4.12 R Supervisor Trap Value register (`stval`).

SXLEN-1	...	0
stval		

RVP.4.131 4.1.9 (p.70) R When a trap is taken into S-mode, `stval` is written with exception-specific information to assist software in handling the trap.

RVP.4.132 4.1.9 (p.70) R Otherwise, `stval` is never written by the implementation, though it may be explicitly written by software.

RVP.4.133 4.1.9 (p.70) R The hardware platform will specify which exceptions must set `stval` informatively and which may unconditionally set it to zero.

RVP.4.134 4.1.9 (p.70) R If `stval` is written with a nonzero value when a breakpoint, address-misaligned, access-fault, or page-fault exception occurs on an instruction fetch, load, or store, then `stval` will contain the faulting virtual address.

ID REFERENCE TYPE DEFINITION

- RVP.4.135 4.1.9 (p.70) R If `stval` is written with a nonzero value when a misaligned load or store causes an access-fault or page-fault exception, then `stval` will contain the virtual address of the portion of the access that caused the fault.
- RVP.4.136 4.1.9 (p.70, p.71) R If `stval` is written with a nonzero value when an instruction access-fault or page-fault exception occurs on a system with variable-length instructions, then `stval` will contain the virtual address of the portion of the instruction that caused the fault, while `sepc` will point to the beginning of the instruction.
- RVP.4.137 4.1.9 (p.71) R The `stval` register can optionally also be used to return the faulting instruction bits on an illegal instruction exception (`sepc` points to the faulting instruction in memory).
- RVP.4.138 4.1.9 (p.71) R If `stval` is written with a nonzero value when an illegal-instruction exception occurs, then `stval` will contain the shortest of:
 - the actual faulting instruction
 - the first ILEN bits of the faulting instruction
 - the first SXLEN bits of the faulting instruction
- RVP.4.139 4.1.9 (p.71) R The value loaded into `stval` on an illegal-instruction exception is right-justified and all unused upper bits are cleared to zero.
- RVP.4.140 4.1.9 (p.72) R For other traps, `stval` is set to zero, but a future standard may redefine `stval`'s setting for other traps.
- RVP.4.141 4.1.9 (p.72) R `stval` is a WARL register that must be able to hold all valid virtual addresses and the value 0. It need not be capable of holding all possible invalid addresses.
- RVP.4.142 4.1.9 (p.72) R Prior to writing `stval`, implementations may convert an invalid address into some other invalid address that `stval` is capable of holding.
- RVP.4.143 4.1.9 (p.72) R If the feature to return the faulting instruction bits is implemented, `stval` must also be able to hold all values less than 2^N , where N is the smaller of SXLEN and ILEN.
- RVP.4.144 4.1.10 (p.72) H Supervisor Environment Configuration Register (`senvcfg`)
- RVP.4.145 4.1.10 (p.72) R The `senvcfg` CSR is an SXLEN-bit read/write register that controls certain characteristics of the U-mode execution environment
- RVP.4.146 4.1.10 (p.72) R Supervisor environment configuration register (`senvcfg`)
Figure 4.13
- | | | | | | | | | | | |
|---------|-----|---|------|-------|------|------|---|---|------|---|
| SXLEN-1 | ... | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| WPRI | | | CBZE | CBCFE | CBIE | WPRI | | | FIOM | |
- RVP.4.147 4.1.10 (p.72) R If bit FIOM (Fence of I/O implies Memory) is set to one in `senvcfg`, FENCE instructions executed in U-mode are modified so the requirement to order accesses to device I/O implies also the requirement to order main memory accesses.
- RVP.4.148 4.1.10 (p.72) R Modified interpretation of FENCE instruction bits PI, PO, SI, and SO in U-mode when FIOM=1.
Table 4.3

Instruction Bit	Meaning when set
PI	Predecessor device input and memory reads (PR implied)
PO	Predecessor device output and memory writes (PW implied)
SI	Successor device input and memory reads (SR implied)
SO	Successor device output and memory writes (SW implied)

ID REFERENCE TYPE DEFINITION

- RVP.4.149 4.1.10 (p.72) R Similarly, for U-mode when FIOM=1, if an atomic instruction that accesses a region ordered as device I/O has its *aq* and/or *rl* bit set, then that instruction is ordered as though it accesses both device I/O and memory.
- RVP.4.150 4.1.10 (p.72) R If *satp.MODE* is read-only zero (always Bare), the implementation may make FIOM read-only zero.
- RVP.4.151 4.1.10 (p.72) C Bit FIOM exists for a specific circumstance when an I/O device is being emulated for U-mode and both of the following are true:
 (a) the emulated device has a memory buffer that should be I/O space but is actually mapped to main memory via address translation, and
 (b) multiple physical harts are involved in accessing this emulated device from U-mode.
- RVP.4.152 4.1.10 (p.72, p.73) C A hypervisor running in S-mode without the benefit of the hypervisor extension of Chapter 8 may need to emulate a device for U-mode if paravirtualization cannot be employed. If the same hypervisor provides a virtual machine (VM) with multiple virtual harts, mapped one-to-one to real harts, then multiple harts may concurrently access the emulated device, perhaps because:
 (a) the guest OS within the VM assigns device interrupt handling to one hart while the device is also accessed by a different hart outside of an interrupt handler, or
 (b) control of the device (or partial control) is being migrated from one hart to another, such as for interrupt load balancing within the VM. For such cases, guest software within the VM is expected to properly coordinate access to the (emulated) device across multiple harts using mutex locks and/or interprocessor interrupts as usual, which in part entails executing I/O fences. But those I/O fences may not be sufficient if some of the device "I/O" is actually main memory, unknown to the guest. Setting FIOM=1 modifies those fences (and all other I/O fences executed in U-mode) to include main memory, too.
- RVP.4.153 4.1.10 (p.73) C Software can always avoid the need to set FIOM by never using main memory to emulate a device memory buffer that should be I/O space. However, this choice usually requires trapping all U-mode accesses to the emulated buffer, which might have a noticeable impact on performance. The alternative offered by FIOM is sufficiently inexpensive to implement that we consider it worth supporting even if only rarely enabled.
- RVP.4.154 4.1.10 (p.73) R The definition of the CBZE field will be furnished by the forthcoming Zicboz extension. Its allocation within *senvcfg* may change prior to the ratification of that extension
- RVP.4.155 4.1.10 (p.73) R The definitions of the CBCFE and CBIE fields will be furnished by the forthcoming Zicbom extension. Their allocations within *senvcfg* may change prior to the ratification of that extension.
- RVP.4.156 4.1.11 (p.73) H Supervisor Address Translation and Protection (*satp*) Register
- RVP.4.157 4.1.11 (p.73) R The *satp* register is an SXLEN-bit read/write register which controls supervisor-mode address translation and protection
- RVP.4.158 4.1.11 (p.73) R Supervisor address translation and protection register *satp* when SXLEN=32
 Figure 4.14

31	30	...	22	21	...	0
MODE	ASID			PPN		

ID REFERENCE TYPE DEFINITION

- RVP.4.159 4.1.11 (p.73) R Supervisor address translation and protection register `satp` when SXLEN=64, for MODE values Bare, Sv39, Sv48, and Sv57.
- | | | | | | | | | |
|------|-----|----|----|------|----|----|-----|---|
| 63 | ... | 60 | 59 | ... | 44 | 43 | ... | 0 |
| MODE | | | | ASID | | | PPN | |
- RVP.4.160 4.1.11 (p.73) R This register holds the physical page number (PPN) of the root page table, i.e., its supervisor physical address divided by 4 KiB; an address space identifier (ASID), which facilitates address-translation fences on a per-address-space basis; and the MODE field, which selects the current address-translation scheme.
- RVP.4.161 4.1.11 (p.73) I Further details on the access to this register (`satp`) are described in Section 3.1.6.5.
- RVP.4.162 4.1.11 (p.73) C Storing a PPN in `satp`, rather than a physical address, supports a physical address space larger than 4 GiB for RV32. The `satp.PPN` field might not be capable of holding all physical page numbers. Some platform standards might place constraints on the values `satp.PPN` may assume, e.g., by requiring that all physical page numbers corresponding to main memory be representable.
- RVP.4.163 4.1.11 (p.74) C We store the ASID and the page table base address in the same CSR to allow the pair to be changed atomically on a context switch. Swapping them non-atomically could pollute the old virtual address space with new translations, or vice-versa. This approach also slightly reduces the cost of a context switch.
- RVP.4.164 4.1.11 (p.74) R Encoding of `satp` MODE field when SXLEN=32
- | Value | Name | Description |
|-------|------|--|
| 0 | Bare | No translation or protection |
| 1 | Sv32 | Page-based 32-bit virtual addressing (see Section 4.3) |
- RVP.4.165 4.1.11 (p.74) R Encoding of `satp` MODE field when SXLEN=64
- | Value | Name | Description |
|-------|------|--|
| 0 | Bare | No translation or protection |
| 1-7 | - | Reserved for standard use |
| 8 | Sv39 | Page-based 39-bit virtual addressing (see Section 4.4) |
| 9 | Sv48 | Page-based 48-bit virtual addressing (see Section 4.5) |
| 10 | Sv57 | Page-based 57-bit virtual addressing (see Section 4.6) |
| 11 | Sv64 | Sv64 Reserved for page-based 64-bit virtual addressing |
| 12-13 | - | Reserved for standard use |
| 14-15 | - | Designated for custom use |
- RVP.4.166 4.1.11 (p.74) R When MODE=Bare, supervisor virtual addresses are equal to supervisor physical addresses, and there is no additional memory protection beyond the physical memory protection scheme described in Section 3.7.
- RVP.4.167 4.1.11 (p.74) R To select MODE=Bare, software must write zero to the remaining fields of `satp` (bits 30–0 when SXLEN=32, or bits 59–0 when SXLEN=64).
- RVP.4.168 4.1.11 (p.74) R Attempting to select MODE=Bare with a nonzero pattern in the remaining fields has an UNSPECIFIED effect on the value that the remaining fields assume and an UNSPECIFIED effect on address translation and protection behavior.

ID	REFERENCE	TYPE	DEFINITION
RVP.4.169	4.1.11 (p.74)	R	When SXLEN=32, the <code>satp</code> encodings corresponding to MODE=Bare and ASID[8:7]=3 are designated for custom use, whereas the encodings corresponding to MODE=Bare and ASID[8:7]≠3 are reserved for future standard use.
RVP.4.170	4.1.11 (p.74)	R	When SXLEN=64, all <code>satp</code> encodings corresponding to MODE=Bare are reserved for future standard use.
RVP.4.171	4.1.11 (p.74)	R	When SXLEN=32, the only other valid setting for MODE is Sv32, a paged virtual-memory scheme described in Section 4.3.
RVP.4.172	4.1.11 (p.74)	R	When SXLEN=64, three paged virtual-memory schemes are defined: Sv39, Sv48, and Sv57, described in Sections 4.4, 4.5, and 4.6, respectively. One additional scheme, Sv64, will be defined in a later version of this specification.
RVP.4.173	4.1.11 (p.74)	R	The remaining MODE settings are reserved for future use and may define different interpretations of the other fields in <code>satp</code> .
RVP.4.174	4.1.11 (p.74)	R	Implementations are not required to support all MODE settings, and if <code>satp</code> is written with an unsupported MODE, the entire write has no effect; no fields in <code>satp</code> are modified.
RVP.4.175	4.1.11 (p.74)	R	The number of ASID bits is UNSPECIFIED and may be zero.
RVP.4.176	4.1.11 (p.74)	R	The number of implemented ASID bits, termed ASIDLEN, may be determined by writing one to every bit position in the ASID field, then reading back the value in <code>satp</code> to see which bit positions in the ASID field hold a one. The least-significant bits of ASID are implemented first: that is, if ASIDLEN > 0, ASID[ASIDLEN-1:0] is writable. The maximal value of ASIDLEN, termed ASIDMAX, is 9 for Sv32 or 16 for Sv39, Sv48, and Sv57.
RVP.4.177	4.1.11 (p.74)	C	For many applications, the choice of page size has a substantial performance impact. A large page size increases TLB reach and loosens the associativity constraints on virtually indexed, physically tagged caches. At the same time, large pages exacerbate internal fragmentation, wasting physical memory and possibly cache capacity.
RVP.4.178	4.1.11 (p.74, p.75)	C	After much deliberation, we have settled on a conventional page size of 4 KiB for both RV32 and RV64. We expect this decision to ease the porting of low-level runtime software and device drivers. The TLB reach problem is ameliorated by transparent superpage support in modern operating systems. Additionally, multi-level TLB hierarchies are quite inexpensive relative to the multi-level cache hierarchies whose address space they map.
RVP.4.179	4.1.11 (p.75)	R	The <code>satp</code> register is considered active when the effective privilege mode is S-mode or U-mode.
RVP.4.180	4.1.11 (p.75)	R	Executions of the address-translation algorithm may only begin using a given value of <code>satp</code> when <code>satp</code> is active.
RVP.4.181	4.1.11 (p.75)	C	Translations that began while <code>satp</code> was active are not required to complete or terminate when <code>satp</code> is no longer active, unless an SFENCE.VMA instruction matching the address and ASID is executed. The SFENCE.VMA instruction must be used to ensure that updates to the address-translation data structures are observed by subsequent implicit reads to those structures by a hart.
RVP.4.182	4.1.11 (p.75)	R	Note that writing <code>satp</code> does not imply any ordering constraints between page-table updates and subsequent address translations, nor does it imply any invalidation of address-translation caches.

ID REFERENCE TYPE DEFINITION

- RVP.4.183 4.1.11 (p.75) R If the new address space's page tables have been modified, or if an ASID is reused, it may be necessary to execute an SFENCE.VMA instruction (see Section 4.2.1) after, or in some cases before, writing satp.
- RVP.4.184 4.1.11 (p.75) C Not imposing upon implementations to flush address-translation caches upon satp writes reduces the cost of context switches, provided a sufficiently large ASID space.
- RVP.4.185 4.2 (p.75) H Supervisor Instructions
- RVP.4.186 4.2 (p.75) I In addition to the SRET instruction defined in Section 3.3.2, one new supervisor-level instruction is provided.
- RVP.4.187 4.2.1 (p.75) H Supervisor Memory-Management Fence Instruction
- RVP.4.188 4.2.1 (p.76)
9.0 (p.138) R SFENCE.VMA Instruction
Supervisor Memory-Management Fence Instruction

Encoding: R-Type

3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0									
SFENCE.VMA						rs2 / asid					rs1 / vaddr					PRIV			0			SYSTEM								
0	0	0	1	0	0	1					0	0	0	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1		

Valid Base: RV32, RV64, RV128

Task: –

Explanation: The supervisor memory-management fence instruction SFENCE.VMA is used to synchronize updates to in-memory memory-management data structures with current execution. Instruction execution causes implicit reads and writes to these data structures; however, these implicit references are ordinarily not ordered with respect to explicit loads and stores. Executing an SFENCE.VMA instruction guarantees that any previous stores already visible to the current RISC-V hart are ordered before certain implicit references by subsequent instructions in that hart to the memory management data structures..

Special Case: none

Exception: none

- RVP.4.189 4.2.1 (p.76) I The specific set of operations ordered by SFENCE.VMA is determined by rs1 and rs2, as described below.
- RVP.4.190 4.2.1 (p.76) I SFENCE.VMA is also used to invalidate entries in the address-translation cache associated with a hart (see Section 4.3.2). Further details on the behavior of this instruction are described in Section 3.1.6.5 and Section 3.7.2.
- RVP.4.191 4.2.1 (p.76) C The SFENCE.VMA is used to flush any local hardware caches related to address translation. It is specified as a fence rather than a TLB flush to provide cleaner semantics with respect to which instructions are affected by the flush operation and to support a wider variety of dynamic caching structures and memory-management schemes. SFENCE.VMA is also used by higher privilege levels to synchronize page table writes and the address translation hardware.
- RVP.4.192 4.2.1 (p.76) R SFENCE.VMA orders only the local hart's implicit references to the memory-management data structures.

ID REFERENCE TYPE DEFINITION

RVP.4.193	4.2.1 (p.76)	C	<p>Consequently, other harts must be notified separately when the memory-management data structures have been modified. One approach is to use</p> <ol style="list-style-type: none"> 1) a local data fence to ensure local writes are visible globally, then 2) an interprocessor interrupt to the other thread, then 3) a local SFENCE.VMA in the interrupt handler of the remote thread, and finally 4) signal back to originating thread that operation is complete. This is, of course, the RISC-V analog to a TLB shootdown.
RVP.4.194	4.2.1 (p.76)	R	<p>For the common case that the translation data structures have only been modified for a single address mapping (i.e., one page or superpage), $rs1$ can specify a virtual address within that mapping to effect a translation fence for that mapping only.</p>
RVP.4.195	4.2.1 (p.76)	R	<p>Furthermore, for the common case that the translation data structures have only been modified for a single address-space identifier, $rs2$ can specify the address space.</p>
RVP.4.196	4.2.1 (p.76)	R	<p>If $rs1=x0$ and $rs2=x0$, the fence orders all reads and writes made to any level of the page tables, for all address spaces. The fence also invalidates all address-translation cache entries, for all address spaces.</p>
RVP.4.197	4.2.1 (p.76)	R	<p>If $rs1=x0$ and $rs2\neq x0$, the fence orders all reads and writes made to any level of the page tables, but only for the address space identified by integer register $rs2$. Accesses to global mappings (see Section 4.3.1) are not ordered. The fence also invalidates all address-translation cache entries matching the address space identified by integer register $rs2$, except for entries containing global mappings.</p>
RVP.4.198	4.2.1 (p.77)	R	<p>If $rs1\neq x0$ and $rs2=x0$, the fence orders only reads and writes made to leaf page table entries corresponding to the virtual address in $rs1$, for all address spaces. The fence also invalidates all address-translation cache entries that contain leaf page table entries corresponding to the virtual address in $rs1$, for all address spaces.</p>
RVP.4.199	4.2.1 (p.77)	R	<p>If $rs1\neq x0$ and $rs2\neq x0$, the fence orders only reads and writes made to leaf page table entries corresponding to the virtual address in $rs1$, for the address space identified by integer register $rs2$. Accesses to global mappings are not ordered. The fence also invalidates all address translation cache entries that contain leaf page table entries corresponding to the virtual address in $rs1$ and that match the address space identified by integer register $rs2$, except for entries containing global mappings.</p>
RVP.4.200	4.2.1 (p.77)	R	<p>If the value held in $rs1$ is not a valid virtual address, then the SFENCE.VMA instruction has no effect. No exception is raised in this case.</p>
RVP.4.201	4.2.1 (p.77)	R	<p>When $rs2\neq x0$, bits SXLEN-1:ASIDMAX of the value held in $rs2$ are reserved for future standard use. Until their use is defined by a standard extension, they should be zeroed by software and ignored by current implementations.</p>
RVP.4.202	4.2.1 (p.77)	R	<p>Furthermore, if ASIDLEN < ASIDMAX, the implementation shall ignore bits ASIDMAX-1:ASIDLEN of the value held in $rs2$.</p>

ID	REFERENCE TYPE DEFINITION	
RVP.4.203 4.2.1 (p.77)	C	It is always legal to over-fence, e.g., by fencing only based on a subset of the bits in $rs1$ and/or $rs2$, and/or by simply treating all SFENCE.VMA instructions as having $rs1=x0$ and/or $rs2=x0$. For example, simpler implementations can ignore the virtual address in $rs1$ and the ASID value in $rs2$ and always perform a global fence. The choice not to raise an exception when an invalid virtual address is held in $rs1$ facilitates this type of simplification.
RVP.4.204 4.2.1 (p.77)	R	An implicit read of the memory-management data structures may return any translation for an address that was valid at any time since the most recent SFENCE.VMA that subsumes that address.
RVP.4.205 4.2.1 (p.77)	R	The ordering implied by SFENCE.VMA does not place implicit reads and writes to the memory management data structures into the global memory order in a way that interacts cleanly with the standard RVWMO ordering rules. In particular, even though an SFENCE.VMA orders prior explicit accesses before subsequent implicit accesses, and those implicit accesses are ordered before their associated explicit accesses, SFENCE.VMA does not necessarily place prior explicit accesses before subsequent explicit accesses in the global memory order. These implicit loads also need not otherwise obey normal program order semantics with respect to prior loads or stores to the same address.
RVP.4.206 4.2.1 (p.77)	C	A consequence of this specification is that an implementation may use any translation for an address that was valid at any time since the most recent SFENCE.VMA that subsumes that address. In particular, if a leaf PTE is modified but a subsuming SFENCE.VMA is not executed, either the old translation or the new translation will be used, but the choice is unpredictable. The behavior is otherwise well-defined.
RVP.4.207 4.2.1 (p.77)	C	In a conventional TLB design, it is possible for multiple entries to match a single address if, for example, a page is upgraded to a superpage without first clearing the original non-leaf PTE's valid bit and executing an SFENCE.VMA with $rs1=x0$. In this case, a similar remark applies: it is unpredictable whether the old non-leaf PTE or the new leaf PTE is used, but the behavior is otherwise well defined.
RVP.4.208 4.2.1 (p.77)	C	Another consequence of this specification is that it is generally unsafe to update a PTE using a set of stores of a width less than the width of the PTE, as it is legal for the implementation to read the PTE at any time, including when only some of the partial stores have taken effect.
RVP.4.209 4.2.1 (p.78)	C	This specification permits the caching of PTEs whose V (Valid) bit is clear. Operating systems must be written to cope with this possibility, but implementers are reminded that eagerly caching invalid PTEs will reduce performance by causing additional page faults.
RVP.4.210 4.2.1 (p.78)	R	Implementations must only perform implicit reads of the translation data structures pointed to by the current contents of the satp register or a subsequent valid (V=1) translation data structure entry, and must only raise exceptions for implicit accesses that are generated as a result of instruction execution, not those that are performed speculatively.
RVP.4.211 4.2.1 (p.78)	R	Changes to the sstatus fields SUM and MXR take effect immediately, without the need to execute an SFENCE.VMA instruction.
RVP.4.212 4.2.1 (p.78)	R	Changing satp.MODE from Bare to other modes and vice versa also takes effect immediately, without the need to execute an SFENCE.VMA instruction.
RVP.4.213 4.2.1 (p.78)	R	Likewise, changes to satp.ASID take effect immediately.

ID REFERENCE TYPE DEFINITION

RVP.4.214	4.2.1 (p.78)	C	<p>The following common situations typically require executing an SFENCE.VMA instruction:</p> <ul style="list-style-type: none"> When software recycles an ASID (i.e., reassociates it with a different page table), it should first change satp to point to the new page table using the recycled ASID, then execute SFENCE.VMA with $rs1=x0$ and $rs2$ set to the recycled ASID. Alternatively, software can execute the same SFENCE.VMA instruction while a different ASID is loaded into satp, provided the next time satp is loaded with the recycled ASID, it is simultaneously loaded with the new page table. If the implementation does not provide ASIDs, or software chooses to always use ASID 0, then after every satp write, software should execute SFENCE.VMA with $rs1=x0$. In the common case that no global translations have been modified, $rs2$ should be set to a register other than $x0$ but which contains the value zero, so that global translations are not flushed. If software modifies a non-leaf PTE, it should execute SFENCE.VMA with $rs1=x0$. If any PTE along the traversal path had its G bit set, $rs2$ must be $x0$; otherwise, $rs2$ should be set to the ASID for which the translation is being modified. If software modifies a leaf PTE, it should execute SFENCE.VMA with $rs1$ set to a virtual address within the page. If any PTE along the traversal path had its G bit set, $rs2$ must be $x0$; otherwise, $rs2$ should be set to the ASID for which the translation is being modified. For the special cases of increasing the permissions on a leaf PTE and changing an invalid PTE to a valid leaf, software may choose to execute the SFENCE.VMA lazily. After modifying the PTE but before executing SFENCE.VMA, either the new or old permissions will be used. In the latter case, a page-fault exception might occur, at which point software should execute SFENCE.VMA in accordance with the previous bullet point.
RVP.4.215	4.2.1 (p.78)	R	If a hart employs an address-translation cache, that cache must appear to be private to that hart. In particular, the meaning of an ASID is local to a hart; software may choose to use the same ASID to refer to different address spaces on different harts.
RVP.4.216	4.2.1 (p.78)	C	A future extension could redefine ASIDs to be global across the SEE, enabling such options as shared translation caches and hardware support for broadcast TLB shootdown. However, as OSes have evolved to significantly reduce the scope of TLB shootdowns using novel ASID-management techniques, we expect the local-ASID scheme to remain attractive for its simplicity and possibly better scalability.
RVP.4.217	4.2.1 (p.78)	R	For implementations that make satp.MODE read-only zero (always Bare), attempts to execute an SFENCE.VMA instruction might raise an illegal instruction exception.
RVP.4.218	4.3 (p.79)	H	Sv32: Page-Based 32-bit Virtual-Memory Systems
RVP.4.219	4.3 (p.79)	R	When Sv32 is written to the MODE field in the satp register (see Section 4.1.11), the supervisor operates in a 32-bit paged virtual-memory system.
RVP.4.220	4.3 (p.79)	R	In this mode, supervisor and user virtual addresses are translated into supervisor physical addresses by traversing a radix-tree page table.
RVP.4.221	4.3 (p.79)	R	Sv32 is supported when SXLEN=32 and is designed to include mechanisms sufficient for supporting modern Unix-based operating systems.

ID REFERENCE TYPE DEFINITION

- RVP.4.222 4.3 (p.79) C The initial RISC-V paged virtual-memory architectures have been designed as straightforward implementations to support existing operating systems. We have architected page table layouts to support a hardware page-table walker. Software TLB refills are a performance bottleneck on high-performance systems, and are especially troublesome with decoupled specialized coprocessors. An implementation can choose to implement software TLB refills using a machine-mode trap handler as an extension to M-mode.
- RVP.4.223 4.3 (p.79) C Some ISAs architecturally expose virtually indexed, physically tagged caches, in that accesses to the same physical address via different virtual addresses might not be coherent unless the virtual addresses lie within the same cache set. Implicitly, this specification does not permit such behavior to be architecturally exposed.
- RVP.4.224 4.3.1 (p.79) H Addressing and Memory Protection
- RVP.4.225 4.3.1 (p.79) R Sv32 implementations support a 32-bit virtual address space, divided into 4 KiB pages.
- RVP.4.226 4.3.1 (p.79)
Figure 4.16 R An Sv32 virtual address is partitioned into a virtual page number (VPN) and page offset, as shown below
- | | | | | | | | | |
|--------|-----|----|----|--------|----|----|-----|-------------|
| 31 | ... | 22 | 21 | ... | 12 | 11 | ... | 0 |
| VPN[1] | | | | VPN[0] | | | | Page offset |
- RVP.4.227 4.3.1 (p.79) R When Sv32 virtual memory mode is selected in the MODE field of the `satp` register, supervisor virtual addresses are translated into supervisor physical addresses via a two-level page table.
- RVP.4.228 4.3.1 (p.79)
Figure 4.17 R The 20-bit VPN is translated into a 22-bit physical page number (PPN), while the 12-bit page offset is untranslated.
- | | | | | | | | | |
|--------|-----|----|----|--------|----|----|-----|-------------|
| 33 | ... | 22 | 21 | ... | 12 | 11 | ... | 0 |
| PPN[1] | | | | PPN[0] | | | | Page offset |
- RVP.4.229 4.3.1 (p.79) R The resulting supervisor-level physical addresses are then checked using any physical memory protection structures (Sections 3.7), before being directly converted to machine-level physical addresses.
- RVP.4.230 4.3.1 (p.79) R If necessary, supervisor-level physical addresses are zero-extended to the number of physical address bits found in the implementation.
- RVP.4.231 4.3.1 (p.79) C For example, consider an RV32 system supporting 34 bits of physical address. When the value of `satp.MODE` is Sv32, a 34-bit physical address is produced directly, and therefore no zero extension is needed. When the value of `satp.MODE` is Bare, the 32-bit virtual address is translated (unmodified) into a 32-bit physical address, and then that physical address is zero-extended into a 34-bit machine-level physical address.
- RVP.4.232 4.3.1 (p.79) R Sv32 page tables consist of 2^{10} page-table entries (PTEs), each of four bytes. A page table is exactly the size of a page and must always be aligned to a page boundary.
- RVP.4.233 4.3.1 (p.79) R The physical page number of the root page table is stored in the `satp` register.
- RVP.4.234 4.3.1 (p.80)
Figure 4.18 R The PTE format for Sv32 is shown below
- | | | | | | | | | | | | | | | | | |
|--------|-----|----|----|--------|----|---|---|-----|---|---|---|---|---|---|---|---|
| 31 | ... | 20 | 19 | ... | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | |
| PPN[1] | | | | PPN[0] | | | | RSW | D | A | G | U | X | W | R | V |

ID REFERENCE TYPE DEFINITION

- RVP.4.235 4.3.1 (p.80) R The V bit indicates whether the PTE is valid; if it is 0, all other bits in the PTE are don't-cares and may be used freely by software.
- RVP.4.236 4.3.1 (p.80) R The permission bits, R, W, and X, indicate whether the page is readable, writable, and executable, respectively.
- RVP.4.237 4.3.1 (p.80) R When all three (R, W, X) are zero, the PTE is a pointer to the next level of the page table; otherwise, it is a leaf PTE.
- RVP.4.238 4.3.1 (p.80) R Writable pages must also be marked readable; the contrary combinations are reserved for future use.
- RVP.4.239 4.3.1 (p.80)
Table 4.5 R The encoding of the permission bits X, W, R in PTE format:
- | X | W | R | Meaning |
|---|---|---|-------------------------------------|
| 0 | 0 | 0 | Pointer to next level of page table |
| 0 | 0 | 1 | Read-only page |
| 0 | 1 | 0 | Reserved for future use |
| 0 | 1 | 1 | Read-write page |
| 1 | 0 | 0 | Execute-only page |
| 1 | 0 | 1 | Read-execute page |
| 1 | 1 | 0 | Reserved for future use |
| 1 | 1 | 1 | Read-write-execute page |
- RVP.4.240 4.3.1 (p.80) R Attempting to fetch an instruction from a page that does not have execute permissions raises a fetch page-fault exception.
- RVP.4.241 4.3.1 (p.80) R Attempting to execute a load or load-reserved instruction whose effective address lies within a page without read permissions raises a load page-fault exception.
- RVP.4.242 4.3.1 (p.80) R Attempting to execute a store, store-conditional, or AMO instruction whose effective address lies within a page without write permissions raises a store page-fault exception.
- RVP.4.243 4.3.1 (p.80) C AMOs never raise load page-fault exceptions. Since any unreadable page is also unwritable, attempting to perform an AMO on an unreadable page always raises a store page-fault exception
- RVP.4.244 4.3.1 (p.80) R The U bit indicates whether the page is accessible to user mode. U-mode software may only access the page when U=1.
- RVP.4.245 4.3.1 (p.80) R If the SUM bit in the `sstatus` register is set, supervisor mode software may also access pages with U=1. However, supervisor code normally operates with the SUM bit clear, in which case, supervisor code will fault on accesses to user-mode pages.
- RVP.4.246 4.3.1 (p.80) R Irrespective of SUM, the supervisor may not execute code on pages with U=1.
- RVP.4.247 4.3.1 (p.80) C An alternative PTE format would support different permissions for supervisor and user. We omitted this feature because it would be largely redundant with the SUM mechanism (see Section 4.1.1.2) and would require more encoding space in the PTE.
- RVP.4.248 4.3.1 (p.81) R The G bit designates a *global* mapping. Global mappings are those that exist in all address spaces.
- RVP.4.249 4.3.1 (p.81) R For non-leaf PTEs, the global setting implies that all mappings in the subsequent levels of the page table are global.

ID REFERENCE TYPE DEFINITION

RVP.4.250	4.3.1 (p.81)	R	Note that failing to mark a global mapping as global merely reduces performance, whereas marking a non-global mapping as global is a software bug that, after switching to an address space with a different non-global mapping for that address range, can unpredictably result in either mapping being used.
RVP.4.251	4.3.1 (p.81)	C	Global mappings need not be stored redundantly in address-translation caches for multiple ASIDs. Additionally, they need not be flushed from local address-translation caches when an SFENCE.VMA instruction is executed with rs2≠x0.
RVP.4.252	4.3.1 (p.81)	R	The RSW field is reserved for use by supervisor software; the implementation shall ignore this field.
RVP.4.253	4.3.1 (p.81)	R	Each leaf PTE contains an accessed (A) and dirty (D) bit.
RVP.4.254	4.3.1 (p.81)	R	The A bit indicates the virtual page has been read, written, or fetched from since the last time the A bit was cleared.
RVP.4.255	4.3.1 (p.81)	R	The D bit indicates the virtual page has been written since the last time the D bit was cleared.
RVP.4.256	4.3.1 (p.81)	R	Two schemes to manage the A and D bits are permitted: <ul style="list-style-type: none"> • When a virtual page is accessed and the A bit is clear, or is written and the D bit is clear, a page-fault exception is raised. • When a virtual page is accessed and the A bit is clear, or is written and the D bit is clear, the implementation sets the corresponding bit(s) in the PTE. The PTE update must be atomic with respect to other accesses to the PTE, and must atomically check that the PTE is valid and grants sufficient permissions. Updates of the A bit may be performed as a result of speculation, but updates to the D bit must be exact (i.e., not speculative), and observed in program order by the local hart. Furthermore, the PTE update must appear in the global memory order no later than the explicit memory access, or any subsequent explicit memory access to that virtual page by the local hart. The ordering on loads and stores provided by FENCE instructions and the acquire/release bits on atomic instructions also orders the PTE updates associated with those loads and stores as observed by remote harts. The PTE update is not required to be atomic with respect to the explicit memory access that caused the update, and the sequence is interruptible. However, the hart must not perform the explicit memory access before the PTE update is globally visible.
RVP.4.257	4.3.1 (p.81)	R	All harts in a system must employ the same PTE-update scheme as each other.
RVP.4.258	4.3.1 (p.81)	C	Prior versions of this specification required PTE A bit updates to be exact, but allowing the A bit to be updated as a result of speculation simplifies the implementation of address translation prefetchers. System software typically uses the A bit as a page replacement policy hint, but does not require exactness for functional correctness. On the other hand, D bit updates are still required to be exact and performed in program order, as the D bit affects the functional correctness of page eviction.
RVP.4.259	4.3.1 (p.81)	C	Implementations are of course still permitted to perform both A and D bit updates only in an exact manner.

ID REFERENCE TYPE DEFINITION

RVP.4.260	4.3.1 (p.81)	C	In both cases, requiring atomicity ensures that the PTE update will not be interrupted by other intervening writes to the page table, as such interruptions could lead to A/D bits being set on PTEs that have been reused for other purposes, on memory that has been reclaimed for other purposes, and so on. Simple implementations may instead generate page-fault exceptions.
RVP.4.261	4.3.1 (p.82)	C	The A and D bits are never cleared by the implementation. If the supervisor software does not rely on accessed and/or dirty bits, e.g. if it does not swap memory pages to secondary storage or if the pages are being used to map I/O space, it should always set them to 1 in the PTE to improve performance.
RVP.4.262	4.3.1 (p.82)	R	Any level of PTE may be a leaf PTE, so in addition to 4 KiB pages, Sv32 supports 4 MiB megapages.
RVP.4.263	4.3.1 (p.82)	R	A megapage must be virtually and physically aligned to a 4 MiB boundary; a page-fault exception is raised if the physical address is insufficiently aligned.
RVP.4.264	4.3.1 (p.82)	R	For non-leaf PTEs, the D, A, and U bits are reserved for future standard use.
RVP.4.265	4.3.1 (p.82)	R	Until their use is defined by a standard extension, they must be cleared by software for forward compatibility.
RVP.4.266	4.3.1 (p.82)	R	For implementations with both page-based virtual memory and the “A” standard extension, the LR/SC reservation set must lie completely within a single base page (i.e., a naturally aligned 4 KiB region).
RVP.4.267	4.3.2 (p.82)	H	Virtual Address Translation Process

ID REFERENCE TYPE DEFINITION

RVP.4.268	4.3.2 (p.82, p.83)	R	<p>A virtual address va is translated into a physical address pa as follows:</p> <ol style="list-style-type: none"> 1. Let a be $\text{satp}.ppn \times \text{PAGESIZE}$, and let $i = \text{LEVELS} - 1$. (For Sv32, $\text{PAGESIZE}=2^{12}$ and $\text{LEVELS}=2$.) The satp register must be active, i.e., the effective privilege mode must be S-mode or U-mode. 2. Let pte be the value of the PTE at address $a + va.\text{vpn}[i] \times \text{PTESIZE}$. (For Sv32, $\text{PTESIZE}=4$.) If accessing pte violates a PMA or PMP check, raise an access-fault exception corresponding to the original access type. 3. If $pte.v = 0$, or if $pte.r = 0$ and $pte.w = 1$, or if any bits or encodings that are reserved for future standard use are set within pte, stop and raise a page-fault exception corresponding to the original access type. 4. Otherwise, the PTE is valid. If $pte.r = 1$ or $pte.x = 1$, go to step 5. Otherwise, this PTE is a pointer to the next level of the page table. Let $i = i-1$. If $i < 0$, stop and raise a page-fault exception corresponding to the original access type. Otherwise, let $a = pte.ppn \times \text{PAGESIZE}$ and go to step 2. 5. A leaf PTE has been found. Determine if the requested memory access is allowed by the $pte.r$, $pte.w$, $pte.x$, and $pte.u$ bits, given the current privilege mode and the value of the SUM and MXR fields of the mstatus register. If not, stop and raise a page-fault exception corresponding to the original access type. 6. If $i > 0$ and $pte.ppn[i-1 : 0] \neq 0$, this is a misaligned superpage; stop and raise a page-fault exception corresponding to the original access type. 7. If $pte.a = 0$, or if the original memory access is a store and $pte.d = 0$, either raise a page-fault exception corresponding to the original access type, or: <ul style="list-style-type: none"> ▪ If a store to pte would violate a PMA or PMP check, raise an access-fault exception corresponding to the original access type. ▪ Perform the following steps atomically: <ul style="list-style-type: none"> – Compare pte to the value of the PTE at address $a + va.\text{vpn}[i] \times \text{PTESIZE}$. – If the values match, set $pte.a$ to 1 and, if the original memory access is a store, also set $pte.d$ to 1. – If the comparison fails, return to step 2 8. The translation is successful. The translated physical address is given as follows: <ul style="list-style-type: none"> ▪ $pa.\text{pgoff} = va.\text{pgoff}$. ▪ If $i > 0$, then this is a superpage translation and $pa.ppn[i-1 : 0] = va.\text{vpn}[i-1 : 0]$. ▪ $pa.ppn[\text{LEVELS} - 1 : i] = pte.ppn[\text{LEVELS} - 1 : i]$.
RVP.4.269	4.3.2 (p.83)	R	All implicit accesses to the address-translation data structures in this algorithm are performed using width PTESIZE.
RVP.4.270	4.3.2 (p.83)	C	This implies, for example, that an Sv48 implementation may not use two separate 4B reads to non-atomically access a single 8B PTE, and that A/D bit updates performed by the implementation are treated as atomically updating the entire PTE, rather than just the A and/or D bit alone (even though the PTE value does not otherwise change).

ID	REFERENCE	TYPE	DEFINITION
RVP.4.271	4.3.2 (p.83)	R	The results of implicit address-translation reads in step 2 may be held in a read-only, incoherent <i>address-translation cache</i> but not shared with other harts.
RVP.4.272	4.3.2 (p.83)	R	The address-translation cache may hold an arbitrary number of entries, including an arbitrary number of entries for the same address and ASID.
RVP.4.273	4.3.2 (p.83)	R	Entries in the address-translation cache may then satisfy subsequent step 2 reads if the ASID associated with the entry matches the ASID loaded in step 0 or if the entry is associated with a <i>global</i> mapping.
RVP.4.274	4.3.2 (p.83)	R	To ensure that implicit reads observe writes to the same memory locations, an SFENCE.VMA instruction must be executed after the writes to flush the relevant cached translations.
RVP.4.275	4.3.2 (p.83)	R	The address-translation cache cannot be used in step 7; accessed and dirty bits may only be updated in memory directly.
RVP.4.276	4.3.2 (p.83)	C	It is permitted for multiple address-translation cache entries to co-exist for the same address. This represents the fact that in a conventional TLB hierarchy, it is possible for multiple entries to match a single address if, for example, a page is upgraded to a superpage without first clearing the original non-leaf PTE's valid bit and executing an SFENCE.VMA with $rs1=x0$, or if multiple TLBs exist in parallel at a given level of the hierarchy. In this case, just as if an SFENCE.VMA is not executed between a write to the memory-management tables and subsequent implicit read of the same address: it is unpredictable whether the old non-leaf PTE or the new leaf PTE is used, but the behavior is otherwise well defined.
RVP.4.277	4.3.2 (p.83)	R	Implementations may also execute the address-translation algorithm speculatively at any time, for any virtual address, as long as <i>satp</i> is active (as defined in Section 4.1.11). Such speculative executions have the effect of pre-populating the address-translation cache.
RVP.4.278	4.3.2 (p.83)	R	Speculative executions of the address-translation algorithm behave as non-speculative executions of the algorithm do, except that they must not set the dirty bit for a PTE, they must not trigger an exception, and they must not create address-translation cache entries if those entries would have been invalidated by any SFENCE.VMA instruction executed by the hart since the speculative execution of the algorithm began.
RVP.4.279	4.3.2 (p.84)	C	For instance, it is illegal for both non-speculative and speculative executions of the translation algorithm to begin, read the level 2 page table, pause while the hart executes an SFENCE.VMA with $rs1=rs2=x0$, then resume using the now-stale level 2 PTE, as subsequent implicit reads could populate the address-translation cache with stale PTEs.
RVP.4.280	4.3.2 (p.84)	C	In many implementations, an SFENCE.VMA instruction with $rs1=x0$ will therefore either terminate all previously-launched speculative executions of the address-translation algorithm (for the specified ASID, if applicable), or simply wait for them to complete (in which case any address-translation cache entries created will be invalidated by the SFENCE.VMA as appropriate). Likewise, an SFENCE.VMA instruction with $rs1\neq x0$ generally must either ensure that previously-launched speculative executions of the address-translation algorithm (for the specified ASID, if applicable) are prevented from creating new address-translation cache entries mapping leaf PTEs, or wait for them to complete.

ID REFERENCE TYPE DEFINITION

- RVP.4.281 4.3.2 (p.84) C A consequence of implementations being permitted to read the translation data structures arbitrarily early and speculatively is that at any time, all page table entries reachable by executing the algorithm may be loaded into the address-translation cache.
- RVP.4.282 4.3.2 (p.84) C Although it would be uncommon to place page tables in non-idempotent memory, there is no explicit prohibition against doing so. Since the algorithm may only touch page tables reachable from the root page table indicated in `satp`, the range of addresses that an implementation's page table walker will touch is fully under supervisor control.
- RVP.4.283 4.3.2 (p.84) C The algorithm does not admit the possibility of ignoring high-order PPN bits for implementations with narrower physical addresses.
- RVP.4.284 4.4 (p.84) H Sv39: Page-Based 39-bit Virtual-Memory System
- RVP.4.285 4.4 (p.84) R Sv39 is a simple paged virtual-memory system for $SXLEN=64$, which supports 39-bit virtual address spaces.
- RVP.4.286 4.4 (p.84) R The design of Sv39 follows the overall scheme of Sv32, and this section details only the differences between the schemes.
- RVP.4.287 4.4 (p.84) C We specified multiple virtual memory systems for RV64 to relieve the tension between providing a large address space and minimizing address-translation cost. For many systems, 512 GiB of virtual-address space is ample, and so Sv39 suffices. Sv48 increases the virtual address space to 256 TiB, but increases the physical memory capacity dedicated to page tables, the latency of page-table traversals, and the size of hardware structures that store virtual addresses. Sv57 increases the virtual address space, page table capacity requirement, and translation latency even further.
- RVP.4.288 4.4.1 (p.84) H Addressing and Memory Protection
- RVP.4.289 4.4.1 (p.84) R Sv39 implementations support a 39-bit virtual address space, divided into 4 KiB pages.
- RVP.4.290 4.4.1 (p.84)
Figure 4.19 R An Sv39 address is partitioned as shown below
- | | | | | | | | | | | | |
|--------|--|--------|----|-----|--------|----|-----|-------------|----|-----|---|
| 38 | | 30 | 29 | ... | 21 | 20 | ... | 12 | 11 | ... | 0 |
| VPN[2] | | VPN[1] | | | VPN[0] | | | Page offset | | | |
- RVP.4.291 4.4.1 (p.84) R Instruction fetch addresses and load and store effective addresses, which are 64 bits, must have bits 63–39 all equal to bit 38, or else a page-fault exception will occur.
- RVP.4.292 4.4.1 (p.84)
Figure 4.20 R The 27-bit VPN is translated into a 44-bit PPN via a three-level page table, while the 12-bit page offset is untranslated.
- | | | | | | | | | | | | |
|--------|--|--------|----|-----|--------|----|-----|-------------|----|-----|---|
| 55 | | 30 | 29 | ... | 21 | 20 | ... | 12 | 11 | ... | 0 |
| PPN[2] | | PPN[1] | | | PPN[0] | | | Page offset | | | |
- RVP.4.293 4.4.1 (p.85) C When mapping between narrower and wider addresses, RISC-V zero-extends a narrower physical address to a wider size. The mapping between 64-bit virtual addresses and the 39-bit usable address space of Sv39 is not based on zero-extension but instead follows an entrenched convention that allows an OS to use one or a few of the most-significant bits of a full-size (64-bit) virtual address to quickly distinguish user and supervisor address regions.
- RVP.4.294 4.4.1 (p.85) R Sv39 page tables contain 2^9 page table entries (PTEs), eight bytes each.
- RVP.4.295 4.4.1 (p.85) R A page table is exactly the size of a page and must always be aligned to a page boundary.

ID REFERENCE TYPE DEFINITION

- RVP.4.296 4.4.1 (p.85) R The physical page number of the root page table is stored in the satp register's PPN field.
- RVP.4.297 4.4.1 (p.85) R The PTE format for Sv39 is shown below
- | | | | | | | | | | | | | | | | | | | | | | | | | |
|----|------|----------|----|-----|--------|----|--------|----|--------|-----|-----|----|-----|----|---|---|---|---|---|---|---|---|---|---|
| 63 | 62 | 61 | 60 | ... | 54 | 53 | .. | 28 | 27 | ... | 19 | 18 | ... | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| N | PBMT | Reserved | | | PPN[2] | | PPN[1] | | PPN[0] | | RSW | D | A | G | U | X | W | R | V | | | | | |
- RVP.4.298 4.4.1 (p.85) R Bits 9–0 have the same meaning as for Sv32.
- RVP.4.299 4.4.1 (p.85) R Bit 63 is reserved for use by the Svnapot extension in Chapter 5. If Svnapot is not implemented, bit 63 remains reserved and must be zeroed by software for forward compatibility, or else a page fault exception is raised.
- RVP.4.300 4.4.1 (p.85) R Bits 62–61 are reserved for use by the Svpbmt extension in Chapter 6. If Svpbmt is not implemented, bits 62–61 remain reserved and must be zeroed by software for forward compatibility, or else a page-fault exception is raised.
- RVP.4.301 4.4.1 (p.85) R Bits 60–54 are reserved for future standard use and, until their use is defined by some standard extension, must be zeroed by software for forward compatibility. If any of these bits are set, a page-fault exception is raised.
- RVP.4.302 4.4.1 (p.85) C We reserved several PTE bits for a possible extension that improves support for sparse address spaces by allowing page-table levels to be skipped, reducing memory usage and TLB refill latency. These reserved bits may also be used to facilitate research experimentation. The cost is reducing the physical address space, but 64 PiB is presently ample. When it no longer suffices, the reserved bits that remain unallocated could be used to expand the physical address space.
- RVP.4.303 4.4.1 (p.85) R Any level of PTE may be a leaf PTE, so in addition to 4 KiB pages, Sv39 supports 2 MiB *megapages* and 1 GiB *gigapages*, each of which must be virtually and physically aligned to a boundary equal to its size.
- RVP.4.304 4.4.1 (p.85) R A page-fault exception is raised if the physical address is insufficiently aligned.
- RVP.4.305 4.4.1 (p.85) R The algorithm for virtual-to-physical address translation is the same as in Section 4.3.2, except LEVELS equals 3 and PTESIZE equals 8.
- RVP.4.306 4.5 (p.86) H Sv48: Page-Based 48-bit Virtual-Memory System
- RVP.4.307 4.5 (p.86) R Sv48 is a simple paged virtual-memory system for SXLEN=64, which supports 48-bit virtual address spaces.
- RVP.4.308 4.5 (p.86) I Sv48 is intended for systems for which a 39-bit virtual address space is insufficient.
- RVP.4.309 4.5 (p.86) R It closely follows the design of Sv39, simply adding an additional level of page table, and so this chapter only details the differences between the two schemes.
- RVP.4.310 4.5 (p.86) R Implementations that support Sv48 must also support Sv39.
- RVP.4.311 4.5 (p.86) C Systems that support Sv48 can also support Sv39 at essentially no cost, and so should do so to maintain compatibility with supervisor software that assumes Sv39.
- RVP.4.312 4.5.1 (p.86) H Addressing and Memory Protection
- RVP.4.313 4.5.1 (p.86) R Sv48 implementations support a 48-bit virtual address space, divided into 4 KiB pages.

ID REFERENCE TYPE DEFINITION

RVP.4.314	4.5.1 (p.86) Figure 4.22	R	An Sv48 address is partitioned as shown below																																																																												
			<table border="1"> <tr> <td>47</td><td>...</td><td>39</td><td>38</td><td></td><td>30</td><td>29</td><td>...</td><td>21</td><td>20</td><td>...</td><td>12</td><td>11</td><td>...</td><td>0</td></tr> <tr> <td colspan="4">VPN[3]</td><td colspan="4">VPN[2]</td><td colspan="4">VPN[1]</td><td colspan="4">VPN[0]</td><td colspan="2">Page offset</td></tr> </table>	47	...	39	38		30	29	...	21	20	...	12	11	...	0	VPN[3]				VPN[2]				VPN[1]				VPN[0]				Page offset																																												
47	...	39	38		30	29	...	21	20	...	12	11	...	0																																																																	
VPN[3]				VPN[2]				VPN[1]				VPN[0]				Page offset																																																															
RVP.4.315	4.5.1 (p.86)	R	Instruction fetch addresses and load and store effective addresses, which are 64 bits, must have bits 63–48 all equal to bit 47, or else a page-fault exception will occur.																																																																												
RVP.4.316	4.5.1 (p.86) Figure 4.23	R	The 36-bit VPN is translated into a 44-bit PPN via a four-level page table, while the 12-bit page offset is untranslated.																																																																												
			<table border="1"> <tr> <td>55</td><td>...</td><td>39</td><td>38</td><td></td><td>30</td><td>29</td><td>...</td><td>21</td><td>20</td><td>...</td><td>12</td><td>11</td><td>...</td><td>0</td></tr> <tr> <td colspan="4">PPN[3]</td><td colspan="4">PPN[2]</td><td colspan="4">PPN[1]</td><td colspan="4">PPN[0]</td><td colspan="2">Page offset</td></tr> </table>	55	...	39	38		30	29	...	21	20	...	12	11	...	0	PPN[3]				PPN[2]				PPN[1]				PPN[0]				Page offset																																												
55	...	39	38		30	29	...	21	20	...	12	11	...	0																																																																	
PPN[3]				PPN[2]				PPN[1]				PPN[0]				Page offset																																																															
RVP.4.317	4.5.1 (p.86) Figure 4.24	R	The PTE format for Sv48 is shown below																																																																												
			<table border="1"> <tr> <td>6</td><td>6</td><td>6</td><td>6</td><td>...</td><td>5</td><td>5</td><td>3</td><td>3</td><td>2</td><td>2</td><td>1</td><td>1</td><td>...</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr> <td>3</td><td>2</td><td>1</td><td>0</td><td>...</td><td>4</td><td>3</td><td>7</td><td>6</td><td>8</td><td>7</td><td>9</td><td>8</td><td>...</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr> <td>N</td><td>PBMT</td><td>Reserved</td><td>PPN[3]</td><td>PPN[2]</td><td>PPN[1]</td><td>PPN[0]</td><td>RSW</td><td>D</td><td>A</td><td>G</td><td>U</td><td>X</td><td>W</td><td>R</td><td>V</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table>	6	6	6	6	...	5	5	3	3	2	2	1	1	...	1	9	8	7	6	5	4	3	2	1	0	3	2	1	0	...	4	3	7	6	8	7	9	8	...	0	9	8	7	6	5	4	3	2	1	0	N	PBMT	Reserved	PPN[3]	PPN[2]	PPN[1]	PPN[0]	RSW	D	A	G	U	X	W	R	V										
6	6	6	6	...	5	5	3	3	2	2	1	1	...	1	9	8	7	6	5	4	3	2	1	0																																																							
3	2	1	0	...	4	3	7	6	8	7	9	8	...	0	9	8	7	6	5	4	3	2	1	0																																																							
N	PBMT	Reserved	PPN[3]	PPN[2]	PPN[1]	PPN[0]	RSW	D	A	G	U	X	W	R	V																																																																
RVP.4.318	4.5.1 (p.86)	R	Bits 63–54 and 9–0 have the same meaning as for Sv39.																																																																												
RVP.4.319	4.5.1 (p.86)	R	Any level of PTE may be a leaf PTE, so in addition to 4 KiB pages, Sv48 supports 2 MiB <i>megapages</i> , 1 GiB <i>gigapages</i> , and 512 GiB <i>terapages</i> , each of which must be virtually and physically aligned to a boundary equal to its size.																																																																												
RVP.4.320	4.5.1 (p.86)	R	A page-fault exception is raised if the physical address is insufficiently aligned.																																																																												
RVP.4.321	4.5.1 (p.86)	R	The algorithm for virtual-to-physical address translation is the same as in Section 4.3.2, except LEVELS equals 4 and PTESIZE equals 8.																																																																												
RVP.4.322	4.6 (p.87)	H	Sv57: Page-Based 57-bit Virtual-Memory System																																																																												
RVP.4.323	4.6 (p.87)	R	Sv57 is a simple paged virtual-memory system designed for RV64 systems, which supports 57-bit virtual address spaces.																																																																												
RVP.4.324	4.6 (p.87)	R	Sv57 is intended for systems for which a 48-bit virtual address space is insufficient.																																																																												
RVP.4.325	4.6 (p.87)	R	It closely follows the design of Sv48, simply adding an additional level of page table, and so this chapter only details the differences between the two schemes.																																																																												
RVP.4.326	4.6 (p.87)	R	Implementations that support Sv57 must also support Sv48.																																																																												
RVP.4.327	4.6 (p.87)	C	Systems that support Sv57 can also support Sv48 at essentially no cost, and so should do so to maintain compatibility with supervisor software that assumes Sv48.																																																																												
RVP.4.328	4.6.1 (p.87)	H	Addressing and Memory Protection																																																																												
RVP.4.329	4.6.1 (p.87)	R	Sv57 implementations support a 57-bit virtual address space, divided into 4 KiB pages.																																																																												
RVP.4.330	4.6.1 (p.87) Figure 4.25	R	An Sv57 address is partitioned as shown below																																																																												
			<table border="1"> <tr> <td>56</td><td>...</td><td>48</td><td>47</td><td>...</td><td>39</td><td>38</td><td></td><td>30</td><td>29</td><td>...</td><td>21</td><td>20</td><td>...</td><td>12</td><td>11</td><td>...</td><td>0</td></tr> <tr> <td colspan="4">VPN[4]</td><td colspan="4">VPN[3]</td><td colspan="4">VPN[2]</td><td colspan="4">VPN[1]</td><td colspan="4">VPN[0]</td><td colspan="2">Page offset</td></tr> </table>	56	...	48	47	...	39	38		30	29	...	21	20	...	12	11	...	0	VPN[4]				VPN[3]				VPN[2]				VPN[1]				VPN[0]				Page offset																																					
56	...	48	47	...	39	38		30	29	...	21	20	...	12	11	...	0																																																														
VPN[4]				VPN[3]				VPN[2]				VPN[1]				VPN[0]				Page offset																																																											
RVP.4.331	4.6.1 (p.87)	R	Instruction fetch addresses and load and store effective addresses, which are 64 bits, must have bits 63–57 all equal to bit 56, or else a page-fault exception will occur.																																																																												

ID REFERENCE TYPE DEFINITION

- RVP.4.332 4.6.1 (p.87) R The 45-bit VPN is translated into a 44-bit PPN via a five-level page table, while the 12-bit page offset is untranslated
- | | | | | | | | | | | | | | | | | | |
|--------|-----|--------|----|--------|----|--------|--|--------|----|-------------|----|----|-----|----|----|-----|---|
| 55 | ... | 48 | 47 | ... | 39 | 38 | | 30 | 29 | ... | 21 | 20 | ... | 12 | 11 | ... | 0 |
| PPN[4] | | PPN[3] | | PPN[2] | | PPN[1] | | PPN[0] | | Page offset | | | | | | | |
- RVP.4.333 4.6.1 (p.87) R The PTE format for Sv57 is shown below
- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|------|---------|--------|--------|--------|--------|--------|---|---|-----|---|---|-----|---|---|-----|---|---|-----|---|-----|---|---|---|---|---|---|---|---|---|--|
| 6 | 6 | 6 | 6 | ... | 5 | 5 | ... | 4 | 4 | ... | 3 | 3 | ... | 2 | 2 | ... | 1 | 1 | ... | 1 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | |
| 3 | 2 | 1 | 0 | ... | 4 | 5 | ... | 6 | 5 | ... | 7 | 6 | .. | 8 | 7 | ... | 9 | 8 | ... | 0 | RSW | D | A | G | U | X | W | R | V | | |
| N | PBMT | Reserv. | PPN[4] | PPN[3] | PPN[2] | PPN[1] | PPN[0] | | | | | | | | | | | | | | | | | | | | | | | | |
- RVP.4.334 4.6.1 (p.87) R Bits 63–54 and 9–0 have the same meaning as for Sv39.
- RVP.4.335 4.6.1 (p.87) R Any level of PTE may be a leaf PTE, so in addition to 4 KiB pages, Sv57 supports 2 MiB *megapages*, 1 GiB *gigapages*, 512 GiB *terapages*, and 256 TiB *petapages*, each of which must be virtually and physically aligned to a boundary equal to its size.
- RVP.4.336 4.6.1 (p.87) R page-fault exception is raised if the physical address is insufficiently aligned.
- RVP.4.337 4.6.1 (p.87) R The algorithm for virtual-to-physical address translation is the same as in Section 4.3.2, except LEVELS equals 5 and PTESIZE equals 8.

CHAPTER 5 “Svnapot” Standard Extension for NAPOT Translation Contiguity

ID	REFERENCE	TYPE	DEFINITION																												
RVP.5.1	5.0 (p.89)	H	“Svnapot” Standard Extension for NAPOT Translation Contiguity																												
RVP.5.2	5.0 (p.89) preface (p.i)	I	“Svnapot” standard extension version is 1.0 and status is ratified.																												
RVP.5.3	5.0 (p.89)	R	In Sv39, Sv48, and Sv57, when a PTE has N=1, the PTE represents a translation that is part of a range of contiguous virtual-to-physical translations with the same values for PTE bits 5–0. Such ranges must be of a naturally aligned power-of-2 (NAPOT) granularity larger than the base page size.																												
RVP.5.4	5.0 (p.89)	R	The Svnapot extension depends on Sv39.																												
RVP.5.5	5.0 (p.89) Table 5.1	R	NAPOT PTEs behave identically to non-NAPOT PTEs within the address-translation algorithm in Section 4.3.2, except that: <ul style="list-style-type: none"> If the encoding in <i>pte</i> is valid according to the table below, then instead of returning the original value of <i>pte</i>, implicit reads of a NAPOT PTE return a copy of <i>pte</i> in which <i>pte.ppn[pte.napot bits – 1 : 0]</i> is replaced by <i>vpn[i][pte.napot bits – 1 : 0]</i>. If the encoding in <i>pte</i> is reserved according to the table below, then a page-fault exception must be raised. 																												
			<table border="1"> <thead> <tr> <th>i</th> <th>Wpte.ppn[i]</th> <th>Description</th> <th>pte.napot bits</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>x xxxx xxx1</td> <td>Reserved</td> <td>-</td> </tr> <tr> <td>0</td> <td>x xxxx xx1x</td> <td>Reserved</td> <td>-</td> </tr> <tr> <td>0</td> <td>x xxxx x1xx</td> <td>Reserved</td> <td>-</td> </tr> <tr> <td>0</td> <td>x xxxx 1000</td> <td>64 KiB contiguous region</td> <td>4</td> </tr> <tr> <td>0</td> <td>x xxxx 0xxx</td> <td>Reserved</td> <td>-</td> </tr> <tr> <td>≥1</td> <td>x xxxx xxxx</td> <td>Reserved</td> <td>-</td> </tr> </tbody> </table>	i	Wpte.ppn[i]	Description	pte.napot bits	0	x xxxx xxx1	Reserved	-	0	x xxxx xx1x	Reserved	-	0	x xxxx x1xx	Reserved	-	0	x xxxx 1000	64 KiB contiguous region	4	0	x xxxx 0xxx	Reserved	-	≥1	x xxxx xxxx	Reserved	-
i	Wpte.ppn[i]	Description	pte.napot bits																												
0	x xxxx xxx1	Reserved	-																												
0	x xxxx xx1x	Reserved	-																												
0	x xxxx x1xx	Reserved	-																												
0	x xxxx 1000	64 KiB contiguous region	4																												
0	x xxxx 0xxx	Reserved	-																												
≥1	x xxxx xxxx	Reserved	-																												
			<ul style="list-style-type: none"> Implicit reads of NAPOT page table entries may create address-translation cache entries mapping $a + va.vpn[j] \times \text{PTESIZE}$ to a copy of <i>pte</i> in which <i>pte.ppn[pte.napot bits – 1 : 0]</i> is replaced by <i>vpn[0][pte.napot bits – 1 : 0]</i>, for any or all <i>j</i> such that $j[8 : \text{napot bits}] = i[8 : \text{napot bits}]$, all for the address space identified in <i>satp</i> as loaded by step 0. 																												
RVP.5.6	5.0 (p.90)	C	The motivation for a NAPOT PTE is that it can be cached in a TLB as one or more entries representing the contiguous region as if it were a single (large) page covered by a single translation. This compaction can help relieve TLB pressure in some scenarios. The encoding is designed to fit within the pre-existing Sv39, Sv48, and Sv57 PTE formats so as not to disrupt existing implementations or designs that choose not to implement the scheme. It is also designed so as not to complicate the definition of the address-translation algorithm.																												
RVP.5.7	5.0 (p.90)	C	The address translation cache abstraction captures the behavior that would result from the creation of a single TLB entry covering the entire NAPOT region. It is also designed to be consistent with implementations that support NAPOT PTEs by splitting the NAPOT region into TLB entries covering any smaller power-of-two region sizes. For example, a 64 KiB NAPOT PTE might trigger the creation of 16 standard 4 KiB TLB entries, all with contents generated from the NAPOT PTE (even if the PTEs for the other 4 KiB regions have different contents).																												

ID REFERENCE TYPE DEFINITION

RVP.5.8

In typical usage scenarios, NAPOT PTEs in the same region will have the same attributes, same PPNs, and same values for bits 5–0. RSW remains reserved for supervisor software control. It is the responsibility of the OS and/or hypervisor to configure the page tables in such a way that there are no inconsistencies between NAPOT PTEs and other NAPOT or non-NAPOT PTEs that overlap the same address range. If an update needs to be made, the OS generally should first mark all of the PTEs invalid, then issue SFENCE.VMA instruction(s) covering all 4 KiB regions within the range (either via a single SFENCE.VMA with rs1=x0, or with multiple SFENCE.VMA instructions with rs1≠x0), then update the PTE(s), as described in Section 4.2.1, unless any inconsistencies are known to be benign. If any inconsistencies do exist, then the effect is the same as when SFENCE.VMA is used incorrectly: one of the translations will be chosen, but the choice is unpredictable.

RVP.5.9 5.0 (p.90)

C If an implementation chooses to use a NAPOT PTE (or cached version thereof), it might not consult the PTE directly specified by the algorithm in Section 4.3.2 at all. Therefore, the D and A bits may not be identical across all mappings of the same address range even in typical use cases. The operating system must query all NAPOT aliases of a page to determine whether that page has been accessed and/or is dirty. If the OS manually sets the A and/or D bits for a page, it is recommended that the OS also set the A and/or D bits for other NAPOT aliases as appropriate in order to avoid unnecessary traps.

RVP.5.10 5.0 (p.90)

C Just as with normal PTEs, TLBs are permitted to cache NAPOT PTEs whose V (Valid) bit is clear.

RVP.5.11 5.0 (p.90,
p.91)

C Depending on need, the NAPOT scheme may be extended to other intermediate page sizes and/or to other levels of the page table in the future. The encoding is designed to accommodate other NAPOT sizes should that need arise. For example:

<i>i</i>	<i>pte.ppn[i]</i>	Description	<i>pte.napot bits</i>
0	x xxxx xxx1	8 KiB contiguous region	1
0	x xxxx xx10	16 KiB contiguous region	2
0	x xxxx x100	32 KiB contiguous region	3
0	x xxxx 1000	64 KiB contiguous region	4
0	x xxx1 0000	128 KiB contiguous region	5
...
1	x xxxx xxx1	4 MiB contiguous region	1
1	x xxxx xx10	8 MiB contiguous region	2
...

In such a case, an implementation may or may not support all options. The discoverability mechanism for this extension would be extended to allow system software to determine which sizes are supported.

Other sizes may remain deliberately excluded, so that PPN bits not being used to indicate a valid NAPOT region size (e.g., the least-significant bit of *pte.ppn[i]*) may be repurposed for other uses in the future.

However, in case finer-grained intermediate page size support proves not to be useful, we have chosen to standardize only 64 KiB support as a first step.

CHAPTER 6 “Svpbmt” Standard Extension for Page-Based Memory Types

ID REFERENCE TYPE DEFINITION

RVP.6.1	6.0 (p.93)	H	“Svpbmt” Standard Extension for Page-Based Memory Types															
RVP.6.2	6.0 (p.93) preface (p.i)	I	“Svpbmt” Standard extension version is 1.0 and status is ratified.															
RVP.6.3	6.0 (p.93)	R	In Sv39, Sv48, and Sv57, bits 62–61 of a leaf page table entry indicate the use of page-based memory types that override the PMA(s) for the associated memory pages.															
RVP.6.4	6.0 (p.93) Table 6.1	R	Encodings for the PBMT field in Sv39, Sv48, and Sv57 PTEs. Attributes not mentioned are inherited from the PMA associated with the physical address															
			<table border="1"> <thead> <tr> <th>Mode</th> <th>Value</th> <th>Requested Memory Attributes</th> </tr> </thead> <tbody> <tr> <td>PMA</td> <td>0</td> <td>None</td> </tr> <tr> <td>NC</td> <td>1</td> <td>Non-cacheable, idempotent, weakly-ordered (RVWMO), main memory</td> </tr> <tr> <td>IO</td> <td>2</td> <td>Non-cacheable, non-idempotent, strongly-ordered (I/O ordering), I/O</td> </tr> <tr> <td>-</td> <td>3</td> <td>Reserved for future standard use</td> </tr> </tbody> </table>	Mode	Value	Requested Memory Attributes	PMA	0	None	NC	1	Non-cacheable, idempotent, weakly-ordered (RVWMO), main memory	IO	2	Non-cacheable, non-idempotent, strongly-ordered (I/O ordering), I/O	-	3	Reserved for future standard use
Mode	Value	Requested Memory Attributes																
PMA	0	None																
NC	1	Non-cacheable, idempotent, weakly-ordered (RVWMO), main memory																
IO	2	Non-cacheable, non-idempotent, strongly-ordered (I/O ordering), I/O																
-	3	Reserved for future standard use																
RVP.6.5	6.0 (p.93)	R	The Svpbmt extension depends on Sv39.															
RVP.6.6	6.0 (p.93)	C	Future extensions may provide more and/or finer-grained control over which PMAs can be overridden.															
RVP.6.7	6.0 (p.93)	R	For non-leaf PTEs, bits 62–61 are reserved for future standard use. Until their use is defined by a standard extension, they must be cleared by software for forward compatibility, or else a page-fault exception is raised.															
RVP.6.8	6.0 (p.93)	R	When PBMT settings override a main memory page into I/O or vice versa, memory accesses to such pages obey the memory ordering rules of the final effective attribute, as follows.															
RVP.6.9	6.0 (p.93)	R	If the underlying physical memory attribute for a page is I/O, and the page has PBMT=NC, then accesses to that page obey RVWMO. However, accesses to such pages are considered to be both I/O and main memory accesses for the purposes of FENCE, .aq, and .rl.															
RVP.6.10	6.0 (p.94)	R	If the underlying physical memory attribute for a page is main memory, and the page has PBMT=IO, then accesses to that page obey strong channel 0 I/O ordering rules with respect to other accesses to physical main memory and to other accesses to pages with PBMT=IO.															
RVP.6.11	6.0 (p.94)	R	However, accesses to such pages are considered to be both I/O and main memory accesses for the purposes of FENCE, .aq, and .rl.															
RVP.6.12	6.0 (p.94)	C	A device driver written to rely on I/O strong ordering rules will not operate correctly if the address range is mapped with PBMT=NC. As such, this configuration is discouraged.															
RVP.6.13	6.0 (p.94)	C	It will often still be useful to map physical I/O regions using PBMT=NC so that write combining and speculative accesses can be performed. Such optimizations will likely improve performance when applied with adequate care.															

ID	REFERENCE	TYPE	DEFINITION
RVP.6.14	6.0 (p.94)	R	When Svpbmt is used with non-zero PBMT encodings, it is possible for multiple virtual aliases of the same physical page to exist simultaneously with different memory attributes.
RVP.6.15	6.0 (p.94)	R	It is also possible for a U-mode or S-mode mapping through a PTE with Svpbmt enabled to observe different memory attributes for a given region of physical memory than a concurrent access to the same page performed by M-mode or when MODE=Bare. In such cases, the behaviors dictated by the attributes (including coherence, which is otherwise unaffected) may be violated.
RVP.6.16	6.0 (p.94)	R	Accessing the same location using different attributes that are both non-cacheable (e.g., NC and IO) does not cause loss of coherence, but might result in weaker memory ordering than the stricter attribute ordinarily guarantees. Executing a fence iorw, iorw instruction between such accesses suffices to prevent loss of memory ordering.
RVP.6.17	6.0 (p.94)	R	Accessing the same location using different cacheability attributes may cause loss of coherence. Executing the following sequence between such accesses prevents both loss of coherence and loss of memory ordering: fence iorw, iorw, followed by cbo.flush to an address of that location, followed by a fence iorw, iorw.
RVP.6.18	6.0 (p.94)	C	It follows that, if the same location might later be referenced using the original attributes, then this sequence must be repeated beforehand.
RVP.6.19	6.0 (p.94)	C	In certain cases, a weaker sequence might suffice to prevent loss of coherence. These situations will be detailed following the forthcoming formalization of the interaction of the RVWMO memory model with the instructions in the Zicbom extension.
RVP.6.20	6.0 (p.94)	R	When two-stage address translation is enabled within the H extension, the page-based memory types are also applied in two stages. First, if hgatp.MODE is not equal to zero, non-zero G-stage PTE PBMT bits override the attributes in the PMA to produce an intermediate set of attributes. Otherwise, the PMAs serve as the intermediate attributes. Second, if vsatp.MODE is not equal to zero, non-zero VS-stage PTE PBMT bits override the intermediate attributes to produce the final set of attributes used by accesses to the page in question. Otherwise, the intermediate attributes are used as the final set of attributes.

CHAPTER 7 “Svinval” Standard Extension for Fine-Grained Address-Translation Cache Invalidation

ID REFERENCE TYPE DEFINITION

RVP.7.1 7.0 (p.95) H “Svinval” Standard Extension for Fine-Grained Address-Translation Cache Invalidation

RVP.7.2 7.0 (p.95) preface (p.i) I “Svinval” standard extension version is 1.0 and status is ratified.

RVP.7.3 7.0 (p.95) R The Svinval extension splits SFENCE.VMA, HFENCE.VVMA, and HFENCE.GVMA instructions into finer-grained invalidation and ordering operations that can be more efficiently batched or pipelined on certain classes of high-performance implementation.

RVP.7.4 7.0 (p.95)
9.0 (p.138) R SINVAL.VMA Instruction
Invalidates address-translation cache entries
Encoding: R-Type

3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0										
SINVAL.VMA					rs2 / asid					rs1 / vaddr					PRIV			0			SYSTEM										
0	0	0	1	0	1	1				0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	1			

Valid Base: RV32, RV64, RV128

Task: –

Explanation: The SINVAL.VMA instruction invalidates any address-translation cache entries that an SFENCE.VMA instruction with the same values of rs1 and rs2 would invalidate.

However, unlike SFENCE.VMA, SINVAL.VMA instructions are only ordered with respect to SFENCE.VMA, SFENCE.W.INVAL, and SFENCE.INVAL.IR instructions

Special Case: none

Exception: none

RVP.7.5 7.0 (p.95)
9.0 (p.138) R SFENCE.W.INVAL Instruction

Encoding: R-Type

3	3	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0										
SINVAL.VMA					0					PRIV			0			SYSTEM						1	1	1	0	0	1	1			
0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	1			

Valid Base: RV32, RV64, RV128

Task: –

Explanation: The SFENCE.W.INVAL instruction guarantees that any previous stores already visible to the current RISC-V hart are ordered before subsequent SINVAL.VMA instructions executed by the same hart.

Special Case: none

Exception: none

ID REFERENCE TYPE DEFINITION

RVP.7.6	7.0 (p.95, p.96) 9.0 (p.138)	R	SFENCE.INVAL.IR: Instruction Encoding: R-Type																																																																																																															
			<table border="1"> <tbody> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td colspan="12">SFENCE.INVAL.IR</td><td>0</td><td colspan="3">PRIV</td><td>0</td><td colspan="5">SYSTEM</td></tr> <tr> <td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td></td><td></td><td></td><td>0</td><td>0</td><td>0</td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td></td> </tr> </tbody> </table>	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0								SFENCE.INVAL.IR												0	PRIV			0	SYSTEM					0	0	0	1	1	0	0	0	0	0	0	1				0	0	0				1	1	1	0	0	1	1			
3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																						
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																													
SFENCE.INVAL.IR												0	PRIV			0	SYSTEM																																																																																																	
0	0	0	1	1	0	0	0	0	0	0	1				0	0	0				1	1	1	0	0	1	1																																																																																							
			Valid Base: RV32, RV64, RV128																																																																																																															
			Task: –																																																																																																															
			Explanation: The SFENCE.INVAL.IR instruction guarantees that any previous SINVAL.VMA instructions executed by the current hart are ordered before subsequent implicit references by that hart to the memory-management data structures.																																																																																																															
			Special Case: none																																																																																																															
			Exception: none																																																																																																															
RVP.7.7	7.0 (p.96)	R	When executed in order (but not necessarily consecutively) by a single hart, the sequence SFENCE.W.INVAL, SINVAL.VMA, and SFENCE.INVAL.IR has the same effect as a hypothetical SFENCE.VMA instruction in which: <ul style="list-style-type: none"> the values of rs1 and rs2 for the SFENCE.VMA are the same as those used in the SINVAL.VMA, reads and writes prior to the SFENCE.W.INVAL are considered to be those prior to the SFENCE.VMA, and reads and writes following the SFENCE.INVAL.IR are considered to be those subsequent to the SFENCE.VMA. 																																																																																																															
RVP.7.8	7.0 (p.96)	R	If the hypervisor extension is implemented, the Svinval extension also provides two additional instructions: HINVAL.VVMA and HINVAL.GVMA. These have the same semantics as SINVAL.VMA, except that they combine with SFENCE.W.INVAL and SFENCE.INVAL.IR to replace HFENCE.VVMA and HFENCE.GVMA, respectively, instead of SFENCE.VMA. In addition, HINVAL.GVMA uses VMIDs instead of ASIDs.																																																																																																															
RVP.7.9	7.0 (p.96) 9.0 (p.138)	R	HINVAL.VVMA Instruction Encoding: R-Type																																																																																																															
			<table border="1"> <tbody> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td colspan="12">HINVAL.VVMA</td><td>rs2 / asid</td><td>rs1 / vaddr</td><td>PRIV</td><td>0</td><td colspan="5">SYSTEM</td></tr> <tr> <td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td></td> </tr> </tbody> </table>	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0								HINVAL.VVMA												rs2 / asid	rs1 / vaddr	PRIV	0	SYSTEM					0	0	1	0	0	1	1						0	0	0							1	1	1	0	0	1	1		
3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																				
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																													
HINVAL.VVMA												rs2 / asid	rs1 / vaddr	PRIV	0	SYSTEM																																																																																																		
0	0	1	0	0	1	1						0	0	0							1	1	1	0	0	1	1																																																																																							
			Valid Base: RV32, RV64, RV128																																																																																																															
			Task: –																																																																																																															
			Explanation: See SINVAL.VMA and RVP.7.8																																																																																																															
			Special Case: none																																																																																																															
			Exception: none																																																																																																															
RVP.7.10	7.0 (p.96) 9.0 (p.138)	R	HINVAL.GVMA Instruction Encoding: R-Type																																																																																																															
			<table border="1"> <tbody> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td colspan="12">HINVAL.GVMA</td><td>rs2 / vmid</td><td>rs1 / gaddr</td><td>PRIV</td><td>0</td><td colspan="5">SYSTEM</td></tr> <tr> <td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td></td> </tr> </tbody> </table>	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0								HINVAL.GVMA												rs2 / vmid	rs1 / gaddr	PRIV	0	SYSTEM					0	1	1	0	0	1	1						0	0	0							1	1	1	0	0	1	1	
3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																			
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																													
HINVAL.GVMA												rs2 / vmid	rs1 / gaddr	PRIV	0	SYSTEM																																																																																																		
0	1	1	0	0	1	1						0	0	0							1	1	1	0	0	1	1																																																																																							
			Valid Base: RV32, RV64, RV128																																																																																																															
			Task: –																																																																																																															
			Explanation: See SINVAL.VMA and RVP.7.8																																																																																																															
			Special Case: none																																																																																																															
			Exception: none																																																																																																															

ID	REFERENCE	TYPE	DEFINITION
RVP.7.11	7.0 (p.96)	R	SINVAL.VMA, HINVAL.VVMA, and HINVAL.GVMA require the same permissions and raise the same exceptions as SFENCE.VMA, HFENCE.VVMA, and HFENCE.GVMA, respectively.
RVP.7.12	7.0 (p.96)	R	In particular, an attempt to execute any of these instructions in U-mode always raises an illegal instruction exception.
RVP.7.13	7.0 (p.96)	R	And an attempt to execute SINVAL.VMA or HINVAL.GVMA in S-mode or HS-mode when mstatus.TVM=1 also raises an illegal instruction exception.
RVP.7.14	7.0 (p.96)	R	An attempt to execute HINVAL.VVMA or HINVAL.GVMA in VS-mode or VU-mode, or to execute SINVAL.VMA in VU-mode, raises a virtual instruction exception.
RVP.7.15	7.0 (p.96)	R	When hstatus.VTVM=1, an attempt to execute SINVAL.VMA in VS-mode also raises a virtual instruction exception.
RVP.7.16	7.0 (p.96)	C	SFENCE.W.INVAL and SFENCE.INVAL.IR instructions do not need to be trapped when mstatus.TVM=1 or when hstatus.VTVM=1, as they only have ordering effects but no visible side effects. Trapping of the SINVAL.VMA instruction is sufficient to enable emulation of the intended overall TLB maintenance functionality.
RVP.7.17	7.0 (p.96)	C	In typical usage, software will invalidate a range of virtual addresses in the address-translation caches by executing an SFENCE.W.INVAL instruction, executing a series of SINVAL.VMA, HINVAL.VVMA, or HINVAL.GVMA instructions to the addresses (and optionally ASIDs or VMIDs) in question, and then executing an SFENCE.INVAL.IR instruction.
RVP.7.18	7.0 (p.96)	C	High-performance implementations will be able to pipeline the address-translation cache invalidation operations, and will defer any pipeline stalls or other memory ordering enforcement until an SFENCE.W.INVAL, SFENCE.INVAL.IR, SFENCE.VMA, HFENCE.GVMA, or HFENCE.VVMA instruction is executed.
RVP.7.19	7.0 (p.96)	C	Simpler implementations may implement SINVAL.VMA, HINVAL.VVMA, and HINVAL.GVMA identically to SFENCE.VMA, HFENCE.VVMA, and HFENCE.GVMA, respectively, while implementing SFENCE.W.INVAL and SFENCE.INVAL.IR instructions as no-ops.

CHAPTER 8 Hypervisor Extension

ID	REFERENCE	TYPE	DEFINITION
RVP.8.1	8.0 (p.99)	H	Hypervisor Extension
RVP.8.2	8.0 (p.99) preface (p.i)	I	Hypervisor extension version is 1.0 and status is ratified.
RVP.8.3	8.0 (p.99)	I	This chapter describes the RISC-V hypervisor extension, which virtualizes the supervisor-level architecture to support the efficient hosting of guest operating systems atop a type-1 or type-2 hypervisor.
RVP.8.4	8.0 (p.99)	R	The hypervisor extension changes supervisor mode into <i>hypervisor-extended supervisor mode</i> (HS-mode, or hypervisor mode for short), where a hypervisor or a hosting-capable operating system runs.
RVP.8.5	8.0 (p.99)	R	The hypervisor extension also adds another stage of address translation, from <i>guest physical addresses</i> to supervisor physical addresses, to virtualize the memory and memory-mapped I/O subsystems for a guest operating system.
RVP.8.6	8.0 (p.99)	R	HS-mode acts the same as S-mode, but with additional instructions and CSRs that control the new stage of address translation and support hosting a guest OS in virtual S-mode (VS-mode).
RVP.8.7	8.0 (p.99)	R	Regular S-mode operating systems can execute without modification either in HS-mode or as VS-mode guests.
RVP.8.8	8.0 (p.99)	R	In HS-mode, an OS or hypervisor interacts with the machine through the same SBI as an OS normally does from S-mode.
RVP.8.9	8.0 (p.99)	R	An HS-mode hypervisor is expected to implement the SBI for its VS-mode guest.
RVP.8.10	8.0 (p.99)	R	The hypervisor extension depends on an “I” base integer ISA with 32 x registers (RV32I or RV64I), not RV32E, which has only 16 x registers.
RVP.8.11	8.0 (p.99)	R	CSR <code>mtval</code> must not be read-only zero, and standard page-based address translation must be supported, either Sv32 for RV32, or a minimum of Sv39 for RV64.
RVP.8.12	8.0 (p.99)	R	The hypervisor extension is enabled by setting bit 7 in the <code>misa</code> CSR, which corresponds to the letter H. RISC-V harts that implement the hypervisor extension are encouraged not to hardwire <code>misa[7]</code> , so that the extension may be disabled.
RVP.8.13	8.0 (p.99)	C	The baseline privileged architecture is designed to simplify the use of classic virtualization techniques, where a guest OS is run at user-level, as the few privileged instructions can be easily detected and trapped. The hypervisor extension improves virtualization performance by reducing the frequency of these traps.
RVP.8.14	8.0 (p.99)	C	The hypervisor extension has been designed to be efficiently emulable on platforms that do not implement the extension, by running the hypervisor in S-mode and trapping into M-mode for hypervisor CSR accesses and to maintain shadow page tables. The majority of CSR accesses for type-2 hypervisors are valid S-mode accesses so need not be trapped. Hypervisors can support nested virtualization analogously.
RVP.8.15	8.1 (p.100)	H	Privilege Modes
RVP.8.16	8.1 (p.100)	R	The current <i>virtualization mode</i> , denoted V, indicates whether the hart is currently executing in a guest.

ID	REFERENCE	TYPE	DEFINITION																														
RVP.8.17	8.1 (p.100)	R	When $V=1$, the hart is either in virtual S-mode (VS-mode), or in virtual U-mode (VU-mode) atop a guest OS running in VS-mode.																														
RVP.8.18	8.1 (p.100)	R	When $V=0$, the hart is either in M-mode, in HS-mode, or in U-mode atop an OS running in HS-mode.																														
RVP.8.19	8.1 (p.100)	R	The virtualization mode also indicates whether two-stage address translation is active ($V=1$) or inactive ($V=0$).																														
RVP.8.20	8.1 (p.100) Table 8.1	R	The table below lists the possible privilege modes of a RISC-V hart with the hypervisor extension.																														
			<table border="1"> <thead> <tr> <th>Virtualization Mode (V)</th> <th>Nominal Privilege</th> <th>Abbreviation</th> <th>Name</th> <th>Two-Stage Translation</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>U</td> <td>U-mode</td> <td>User mode</td> <td>off</td> </tr> <tr> <td>0</td> <td>S</td> <td>HS-mode</td> <td>Hypervisor-extended supervisor mode</td> <td>off</td> </tr> <tr> <td>0</td> <td>M</td> <td>M-mode</td> <td>Machine mode</td> <td>off</td> </tr> <tr> <td>1</td> <td>U</td> <td>VU-mode</td> <td>Virtual user mode</td> <td>on</td> </tr> <tr> <td>1</td> <td>S</td> <td>VS-mode</td> <td>Virtual supervisor mode</td> <td>on</td> </tr> </tbody> </table>	Virtualization Mode (V)	Nominal Privilege	Abbreviation	Name	Two-Stage Translation	0	U	U-mode	User mode	off	0	S	HS-mode	Hypervisor-extended supervisor mode	off	0	M	M-mode	Machine mode	off	1	U	VU-mode	Virtual user mode	on	1	S	VS-mode	Virtual supervisor mode	on
Virtualization Mode (V)	Nominal Privilege	Abbreviation	Name	Two-Stage Translation																													
0	U	U-mode	User mode	off																													
0	S	HS-mode	Hypervisor-extended supervisor mode	off																													
0	M	M-mode	Machine mode	off																													
1	U	VU-mode	Virtual user mode	on																													
1	S	VS-mode	Virtual supervisor mode	on																													
RVP.8.21	8.1 (p.100)	R	For privilege modes U and VU, the <i>nominal privilege mode</i> is U, ...																														
RVP.8.22	8.1 (p.100)	R	... and for privilege modes HS and VS, the nominal privilege mode is S.																														
RVP.8.23	8.1 (p.100)	R	HS-mode is more privileged than VS-mode, and VS-mode is more privileged than VU-mode.																														
RVP.8.24	8.1 (p.100)	R	VS-mode interrupts are globally disabled when executing in U-mode.																														
RVP.8.25	8.1 (p.100)	C	This description does not consider the possibility of U-mode or VU-mode interrupts and will be revised if an extension for user-level interrupts is adopted.																														
RVP.8.26	8.2 (p.100)	H	Hypervisor and Virtual Supervisor CSRs																														
RVP.8.27	8.2 (p.100)	R	An OS or hypervisor running in HS-mode uses the supervisor CSRs to interact with the exception, interrupt, and address-translation subsystems.																														
RVP.8.28	8.2 (p.100)	R	Additional CSRs are provided to HS-mode, but not to VS-mode, to manage two-stage address translation and to control the behavior of a VS mode guest: hstatus, hdeleg, hideleg, hvip, hip, hie, hgeip, hgeie, henvcfg, henvcfgfgh, hcounteren, htimedelta, htimedeltah, htval, htinst, and hgatp.																														
RVP.8.29	8.2 (p.100)	R	Furthermore, several <i>virtual supervisor</i> CSRs (VS CSRs) are replicas of the normal supervisor CSRs. For example, vsstatus is the VS CSR that duplicates the usual sstatus CSR.																														
RVP.8.30	8.2 (p.100)	R	When $V=1$, the VS CSRs substitute for the corresponding supervisor CSRs, taking over all functions of the usual supervisor CSRs except as specified otherwise. Instructions that normally read or modify a supervisor CSR shall instead access the corresponding VS CSR.																														
RVP.8.31	8.2 (p.100)	R	When $V=1$, an attempt to read or write a VS CSR directly by its own separate CSR address causes a virtual instruction exception.																														
RVP.8.32	8.2 (p.100)	R	(Attempts from U-mode cause an illegal instruction exception as usual.)																														
RVP.8.33	8.2 (p.100)	R	The VS CSRs can be accessed as themselves only from M-mode or HS-mode.																														

Virtualization Mode (V)	Nominal Privilege	Abbreviation	Name	Two-Stage Translation
0	U	U-mode	User mode	off
0	S	HS-mode	Hypervisor-extended supervisor mode	off
0	M	M-mode	Machine mode	off
1	U	VU-mode	Virtual user mode	on
1	S	VS-mode	Virtual supervisor mode	on

- RVP.8.21 8.1 (p.100) R For privilege modes U and VU, the *nominal privilege mode* is U, ...
- RVP.8.22 8.1 (p.100) R ... and for privilege modes HS and VS, the nominal privilege mode is S.
- RVP.8.23 8.1 (p.100) R HS-mode is more privileged than VS-mode, and VS-mode is more privileged than VU-mode.
- RVP.8.24 8.1 (p.100) R VS-mode interrupts are globally disabled when executing in U-mode.
- RVP.8.25 8.1 (p.100) C This description does not consider the possibility of U-mode or VU-mode interrupts and will be revised if an extension for user-level interrupts is adopted.
- RVP.8.26 8.2 (p.100) H Hypervisor and Virtual Supervisor CSRs
- RVP.8.27 8.2 (p.100) R An OS or hypervisor running in HS-mode uses the supervisor CSRs to interact with the exception, interrupt, and address-translation subsystems.
- RVP.8.28 8.2 (p.100) R Additional CSRs are provided to HS-mode, but not to VS-mode, to manage two-stage address translation and to control the behavior of a VS mode guest: hstatus, hdeleg, hideleg, hvip, hip, hie, hgeip, hgeie, henvcfg, henvcfgfgh, hcounteren, htimedelta, htimedeltah, htval, htinst, and hgatp.
- RVP.8.29 8.2 (p.100) R Furthermore, several *virtual supervisor* CSRs (VS CSRs) are replicas of the normal supervisor CSRs. For example, vsstatus is the VS CSR that duplicates the usual sstatus CSR.
- RVP.8.30 8.2 (p.100) R When $V=1$, the VS CSRs substitute for the corresponding supervisor CSRs, taking over all functions of the usual supervisor CSRs except as specified otherwise. Instructions that normally read or modify a supervisor CSR shall instead access the corresponding VS CSR.
- RVP.8.31 8.2 (p.100) R When $V=1$, an attempt to read or write a VS CSR directly by its own separate CSR address causes a virtual instruction exception.
- RVP.8.32 8.2 (p.100) R (Attempts from U-mode cause an illegal instruction exception as usual.)
- RVP.8.33 8.2 (p.100) R The VS CSRs can be accessed as themselves only from M-mode or HS-mode.

ID REFERENCE TYPE DEFINITION

- RVP.8.34 8.2 (p.101) R While V=1, the normal HS-level supervisor CSRs that are replaced by VS CSRs retain their values but do not affect the behavior of the machine unless specifically documented to do so.
- RVP.8.35 8.2 (p.101) R Conversely, when V=0, the VS CSRs do not ordinarily affect the behavior of the machine other than being readable and writable by CSR instructions.
- RVP.8.36 8.2 (p.101) R Some standard supervisor CSRs (`sevcfg`, `scounteren`, and `scontext`, possibly others) have no matching VS CSR. These supervisor CSRs continue to have their usual function and accessibility even when V=1, except with VS-mode and VU-mode substituting for HS-mode and U-mode.
- RVP.8.37 8.2 (p.101) R Hypervisor software is expected to manually swap the contents of these registers as needed.
- RVP.8.38 8.2 (p.101) C Matching VS CSRs exist only for the supervisor CSRs that must be duplicated, which are mainly those that get automatically written by traps or that impact instruction execution immediately after trap entry and/or right before SRET, when software alone is unable to swap a CSR at exactly the right moment. Currently, most supervisor CSRs fall into this category, but future ones might not.
- RVP.8.39 8.2 (p.101) I In this chapter, we use the term HSXLEN to refer to the effective XLEN when executing in HS-mode, and VSXLEN to refer to the effective XLEN when executing in VS-mode.
- RVP.8.40 8.2.1 (p.101) H Hypervisor Status Register (`hstatus`)
- RVP.8.41 8.2.1 (p.101) R The `hstatus` register is an HSXLEN-bit read/write register.
- RVP.8.42 8.2.1 (p.101) R Hypervisor status register (`hstatus`) when SXLEN=32.
Figure 8.1
- | | | | | | | | |
|------|-----|----|------|-----|------|------|----|
| 31 | ... | 23 | 22 | 21 | 20 | 19 | 18 |
| WPRI | | | VTSR | VTW | VTVM | WPRI | |
-
- | | | | | | | | | | | | | |
|------------|-----|----|------|----|------|-----|-----|------|------|---|-----|---|
| 17 | ... | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | ... | 0 |
| VGEIN[5:0] | | | WPRI | HU | SPVP | SPV | GVA | VSBE | WPRI | | | |
-
- RVP.8.43 8.2.1 (p.101) R Hypervisor status register (`hstatus`) when SXLEN=64.
Figure 8.2
- | | | | | | | | | | | | | |
|----------|-----|----|------|----|------|-----|----|------|-----|------|------|----|
| HSXLEN-1 | ... | 34 | 33 | 32 | 31 | ... | 23 | 22 | 21 | 20 | 19 | 18 |
| WPRI | | | VSXL | | WPRI | | | VTSR | VTW | VTVM | WPRI | |
-
- | | | | | | | | | | | | | |
|------------|-----|----|------|----|------|-----|-----|------|------|---|-----|---|
| 17 | ... | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | ... | 0 |
| VGEIN[5:0] | | | WPRI | HU | SPVP | SPV | GVA | VSBE | WPRI | | | |
-
- RVP.8.44 8.2.1 (p.101) R The `hstatus` register provides facilities analogous to the `mstatus` register for tracking and controlling the exception behavior of a VS-mode guest.
- RVP.8.45 8.2.1 (p.101) R The VSXL field controls the effective XLEN for VS-mode (known as VSXLEN), which may differ from the XLEN for HS-mode (HSXLEN).
- RVP.8.46 8.2.1 (p.101) R When HSXLEN=32, the VSXL field does not exist, and VSXLEN=32.

ID REFERENCE TYPE DEFINITION

- RVP.8.47 8.2.1 (p.101) R When HSXLEN=64, VSXL is a WARL field that is encoded the same as the MXL field of misa
- | VSXL | VSXLEN |
|-------------|---------------|
| 1 | 32 |
| 2 | 64 |
| 3 | 128 |
- RVP.8.48 8.2.1 (p.101) R In particular, an implementation may make VSXL be a read-only field whose value always ensures that VSXLEN=HSXLEN.
- RVP.8.49 8.2.1 (p.102) R If HSXLEN is changed from 32 to a wider width, and if field VSXL is not restricted to a single value, it gets the value corresponding to the widest supported width not wider than the new HSXLEN.
- RVP.8.50 8.2.1 (p.102) R The `hstatus` fields VTSR, VTW, and VTVM are defined analogously to the `mstatus` fields TSR, TW, and TVM, but affect execution only in VS-mode, and cause virtual instruction exceptions instead of illegal instruction exceptions.
- RVP.8.51 8.2.1 (p.102) R When VTSR=1, an attempt in VS-mode to execute SRET raises a virtual instruction exception.
- RVP.8.52 8.2.1 (p.102) R When VTW=1 (and assuming mstatus.TW=0), an attempt in VS-mode to execute WFI raises a virtual instruction exception if the WFI does not complete within an implementation-specific, bounded time limit.
- RVP.8.53 8.2.1 (p.102) R When VTVM=1, an attempt in VS-mode to execute SFENCE.VMA or SINVAL.VMA or to access CSR satp raises a virtual instruction exception.
- RVP.8.54 8.2.1 (p.102) R The VGEIN (Virtual Guest External Interrupt Number) field selects a guest external interrupt source for VS-level external interrupts.
- RVP.8.55 8.2.1 (p.102) R VGEIN is a WLRL field that must be able to hold values between zero and the maximum guest external interrupt number (known as GEILEN), inclusive.
- RVP.8.56 8.2.1 (p.102) R When VGEIN=0, no guest external interrupt source is selected for VS-level external interrupts.
- RVP.8.57 8.2.1 (p.102) R GEILEN may be zero, in which case VGEIN may be read-only zero.
- RVP.8.58 8.2.1 (p.102) I Guest external interrupts are explained in Section 8.2.4, and the use of VGEIN is covered further in Section 8.2.3.
- RVP.8.59 8.2.1 (p.102) R Field HU (Hypervisor in U-mode) controls whether the virtual-machine load/store instructions, HLV, HLvx, and HSV, can be used also in U-mode.
- RVP.8.60 8.2.1 (p.102) R When HU=1, these instructions can be executed in U-mode the same as in HS-mode.
- RVP.8.61 8.2.1 (p.102) R When HU=0, all hypervisor instructions cause an illegal instruction trap in U-mode.
- RVP.8.62 8.2.1 (p.102) C The HU bit allows a portion of a hypervisor to be run in U-mode for greater protection against software bugs, while still retaining access to a virtual machine's memory.
- RVP.8.63 8.2.1 (p.102) R The SPV bit (Supervisor Previous Virtualization mode) is written by the implementation whenever a trap is taken into HS-mode.

ID	REFERENCE	TYPE	DEFINITION						
RVP.8.64	8.2.1 (p.102)	R	Just as the SPP bit in sstatus is set to the (nominal) privilege mode at the time of the trap, the SPV bit in hstatus is set to the value of the virtualization mode V at the time of the trap.						
RVP.8.65	8.2.1 (p.102)	R	When an SRET instruction is executed when V=0, V is set to SPV.						
RVP.8.66	8.2.1 (p.102)	R	When V=1 and a trap is taken into HS-mode, bit SPVP (Supervisor Previous Virtual Privilege) is set to the nominal privilege mode at the time of the trap, the same as sstatus.SPP.						
RVP.8.67	8.2.1 (p.102)	R	But if V=0 before a trap, SPVP is left unchanged on trap entry. SPVP controls the effective privilege of explicit memory accesses made by the virtual-machine load/store instructions, HLV, HLVX, and HSV.						
RVP.8.68	8.2.1 (p.102)	C	Without SPVP, if instructions HLV, HLVX, and HSV looked instead to sstatus.SPP for the effective privilege of their memory accesses, then, even with HU=1, U-mode could not access virtual machine memory at VS-level, because to enter U-mode using SRET always leaves SPP=0. Unlike SPP, field SPVP is untouched by transitions back-and-forth between HS-mode and Umode.						
RVP.8.69	8.2.1 (p.102)	R	Field GVA (Guest Virtual Address) is written by the implementation whenever a trap is taken into HS-mode. For any trap (breakpoint, address misaligned, access fault, page fault, or guest page fault) that writes a guest virtual address to stval, GVA is set to 1. For any other trap into HS-mode, GVA is set to 0.						
RVP.8.70	8.2.1 (p.103)	C	For breakpoint and memory access traps that write a nonzero value to stval, GVA is redundant with field SPV (the two bits are set the same) except when the explicit memory access of an HLV, HLVX, or HSV instruction causes a fault. In that case, SPV=0 but GVA=1.						
RVP.8.71	8.2.1 (p.103)	R	The VSBE bit is a WARL field that controls the endianness of explicit memory accesses made from VS-mode. If VSBE=0, explicit load and store memory accesses made from VS-mode are little endian, and if VSBE=1, they are big-endian.						
RVP.8.72	8.2.1 (p.103)	R	VSBE also controls the endianness of all implicit accesses to VS-level memory management data structures, such as page tables.						
RVP.8.73	8.2.1 (p.103)	R	An implementation may make VSBE a read-only field that always specifies the same endianness as HS-mode.						
RVP.8.74	8.2.2 (p.103)	H	Hypervisor Trap Delegation Registers (<code>hedeleg</code> and <code>hideleg</code>)						
RVP.8.75	8.2.2 (p.103)	R	Register <code>hedeleg</code> (Hypervisor exception delegation register) is HSXLEN-bit read/write WARL register						
RVP.8.76	8.2.2 (p.103) Figure 8.3	R	Hypervisor exception delegation register (<code>hedeleg</code>).						
			<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">HSXLEN-1</td> <td style="padding: 2px;">...</td> <td style="padding: 2px;">0</td> </tr> <tr> <td colspan="3" style="padding: 2px;">Synchronous Exceptions (WARL)</td> </tr> </table>	HSXLEN-1	...	0	Synchronous Exceptions (WARL)		
HSXLEN-1	...	0							
Synchronous Exceptions (WARL)									
RVP.8.77	8.2.2 (p.103)	R	Register <code>hideleg</code> (Hypervisor interrupt delegation register) is HSXLEN-bit read/write WARL register						
RVP.8.78	8.2.2 (p.103) Figure 8.4	R	Hypervisor interrupt delegation register (<code>hideleg</code>).						
			<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">HSXLEN-1</td> <td style="padding: 2px;">...</td> <td style="padding: 2px;">0</td> </tr> <tr> <td colspan="3" style="padding: 2px;">Interrupts (WARL)</td> </tr> </table>	HSXLEN-1	...	0	Interrupts (WARL)		
HSXLEN-1	...	0							
Interrupts (WARL)									
RVP.8.79	8.2.2 (p.103)	R	By default, all traps at any privilege level are handled in M-mode, though M-mode usually uses the <code>medeleg</code> and <code>mideleg</code> CSRs to delegate some traps to HS-mode						

ID	REFERENCE	TYPE	DEFINITION																																																												
RVP.8.80	8.2.2 (p.103)	R	The <code>hedeleg</code> and <code>hideleg</code> CSRs allow these traps to be further delegated to a VS-mode guest; their layout is the same as <code>medeleg</code> and <code>mideleg</code> .																																																												
RVP.8.81	8.2.2 (p.103)	R	A synchronous trap that has been delegated to HS-mode (using <code>medeleg</code>) is further delegated to VS-mode if V=1 before the trap and the corresponding <code>hedeleg</code> bit is set.																																																												
RVP.8.82	8.2.2 (p.103)	R	Each bit of <code>hedeleg</code> shall be either writable or read-only zero.																																																												
RVP.8.83	8.2.2 (p.103) Table 8.2	R	Many bits of <code>hedeleg</code> are required specifically to be writable or zero, as enumerated in the table below																																																												
			<table border="1"> <thead> <tr> <th>Bit</th> <th>Attribute</th> <th>Corresponding exception</th> </tr> </thead> <tbody> <tr><td>0</td><td>Writable if IALIGN=32</td><td>Instruction address misaligned</td></tr> <tr><td>1</td><td>Writable</td><td>Instruction access fault</td></tr> <tr><td>2</td><td>Writable</td><td>Illegal instruction</td></tr> <tr><td>3</td><td>Writable</td><td>Breakpoint</td></tr> <tr><td>4</td><td>Writable</td><td>Load address misaligned</td></tr> <tr><td>5</td><td>Writable</td><td>Load access fault</td></tr> <tr><td>6</td><td>Writable</td><td>Store/AMO address misaligned</td></tr> <tr><td>7</td><td>Writable</td><td>Store/AMO access fault</td></tr> <tr><td>8</td><td>Writable</td><td>Environment call from U-mode or VU-mode</td></tr> <tr><td>9</td><td>Read-only 0</td><td>Environment call from HS-mode</td></tr> <tr><td>10</td><td>Read-only 0</td><td>Environment call from VS-mode</td></tr> <tr><td>11</td><td>Read-only 0</td><td>Environment call from M-mode</td></tr> <tr><td>12</td><td>Writable</td><td>Instruction page fault</td></tr> <tr><td>13</td><td>Writable</td><td>Load page fault</td></tr> <tr><td>15</td><td>Writable</td><td>Store/AMO page fault</td></tr> <tr><td>20</td><td>Read-only 0</td><td>Instruction guest-page fault</td></tr> <tr><td>21</td><td>Read-only 0</td><td>Load guest-page fault</td></tr> <tr><td>22</td><td>Read-only 0</td><td>Virtual instruction</td></tr> <tr><td>23</td><td>Read-only 0</td><td>Store/AMO guest-page fault</td></tr> </tbody> </table>	Bit	Attribute	Corresponding exception	0	Writable if IALIGN=32	Instruction address misaligned	1	Writable	Instruction access fault	2	Writable	Illegal instruction	3	Writable	Breakpoint	4	Writable	Load address misaligned	5	Writable	Load access fault	6	Writable	Store/AMO address misaligned	7	Writable	Store/AMO access fault	8	Writable	Environment call from U-mode or VU-mode	9	Read-only 0	Environment call from HS-mode	10	Read-only 0	Environment call from VS-mode	11	Read-only 0	Environment call from M-mode	12	Writable	Instruction page fault	13	Writable	Load page fault	15	Writable	Store/AMO page fault	20	Read-only 0	Instruction guest-page fault	21	Read-only 0	Load guest-page fault	22	Read-only 0	Virtual instruction	23	Read-only 0	Store/AMO guest-page fault
Bit	Attribute	Corresponding exception																																																													
0	Writable if IALIGN=32	Instruction address misaligned																																																													
1	Writable	Instruction access fault																																																													
2	Writable	Illegal instruction																																																													
3	Writable	Breakpoint																																																													
4	Writable	Load address misaligned																																																													
5	Writable	Load access fault																																																													
6	Writable	Store/AMO address misaligned																																																													
7	Writable	Store/AMO access fault																																																													
8	Writable	Environment call from U-mode or VU-mode																																																													
9	Read-only 0	Environment call from HS-mode																																																													
10	Read-only 0	Environment call from VS-mode																																																													
11	Read-only 0	Environment call from M-mode																																																													
12	Writable	Instruction page fault																																																													
13	Writable	Load page fault																																																													
15	Writable	Store/AMO page fault																																																													
20	Read-only 0	Instruction guest-page fault																																																													
21	Read-only 0	Load guest-page fault																																																													
22	Read-only 0	Virtual instruction																																																													
23	Read-only 0	Store/AMO guest-page fault																																																													
RVP.8.84	8.2.2 (p.103)	R	Bit 0, corresponding to instruction address misaligned exceptions, must be writable if IALIGN=32.																																																												
RVP.8.85	8.2.2 (p.103)	C	Requiring that certain bits of <code>hedeleg</code> be writable reduces some of the burden on a hypervisor to handle variations of implementation.																																																												
RVP.8.86	8.2.2 (p.103)	R	An interrupt that has been delegated to HS-mode (using <code>mideleg</code>) is further delegated to VS-mode if the corresponding <code>hideleg</code> bit is set.																																																												
RVP.8.87	8.2.2 (p.103)	R	Among bits 15:0 of <code>hideleg</code> , bits 10, 6, and 2 (corresponding to the standard VS-level interrupts) are writable, and bits 12, 9, 5, and 1 (corresponding to the standard S-level interrupts) are read-only zeros.																																																												
RVP.8.88	8.2.2 (p.103)	R	When a virtual supervisor external interrupt (code 10) is delegated to VS-mode, it is automatically translated by the machine into a supervisor external interrupt (code 9) for VS-mode, including the value written to <code>vscause</code> on an interrupt trap.																																																												
RVP.8.89	8.2.2 (p.103, p.104)	R	Likewise, a virtual supervisor timer interrupt (6) is translated into a supervisor timer interrupt (5) for VS-mode, and a virtual supervisor software interrupt (2) is translated into a supervisor software interrupt (1) for VS-mode.																																																												
RVP.8.90	8.2.2 (p.104)	R	Similar translations may or may not be done for platform or custom interrupt causes (codes 16 and above).																																																												

Bit	Attribute	Corresponding exception
0	Writable if IALIGN=32	Instruction address misaligned
1	Writable	Instruction access fault
2	Writable	Illegal instruction
3	Writable	Breakpoint
4	Writable	Load address misaligned
5	Writable	Load access fault
6	Writable	Store/AMO address misaligned
7	Writable	Store/AMO access fault
8	Writable	Environment call from U-mode or VU-mode
9	Read-only 0	Environment call from HS-mode
10	Read-only 0	Environment call from VS-mode
11	Read-only 0	Environment call from M-mode
12	Writable	Instruction page fault
13	Writable	Load page fault
15	Writable	Store/AMO page fault
20	Read-only 0	Instruction guest-page fault
21	Read-only 0	Load guest-page fault
22	Read-only 0	Virtual instruction
23	Read-only 0	Store/AMO guest-page fault

- RVP.8.84 8.2.2 (p.103) R Bit 0, corresponding to instruction address misaligned exceptions, must be writable if IALIGN=32.
- RVP.8.85 8.2.2 (p.103) C Requiring that certain bits of `hedeleg` be writable reduces some of the burden on a hypervisor to handle variations of implementation.
- RVP.8.86 8.2.2 (p.103) R An interrupt that has been delegated to HS-mode (using `mideleg`) is further delegated to VS-mode if the corresponding `hideleg` bit is set.
- RVP.8.87 8.2.2 (p.103) R Among bits 15:0 of `hideleg`, bits 10, 6, and 2 (corresponding to the standard VS-level interrupts) are writable, and bits 12, 9, 5, and 1 (corresponding to the standard S-level interrupts) are read-only zeros.
- RVP.8.88 8.2.2 (p.103) R When a virtual supervisor external interrupt (code 10) is delegated to VS-mode, it is automatically translated by the machine into a supervisor external interrupt (code 9) for VS-mode, including the value written to `vscause` on an interrupt trap.
- RVP.8.89 8.2.2 (p.103, p.104) R Likewise, a virtual supervisor timer interrupt (6) is translated into a supervisor timer interrupt (5) for VS-mode, and a virtual supervisor software interrupt (2) is translated into a supervisor software interrupt (1) for VS-mode.
- RVP.8.90 8.2.2 (p.104) R Similar translations may or may not be done for platform or custom interrupt causes (codes 16 and above).

ID	REFERENCE	TYPE	DEFINITION																												
RVP.8.91	8.2.3 (p.104)	H	Hypervisor Interrupt Registers (<code>hvip</code> , <code>hip</code> , and <code>hie</code>)																												
RVP.8.92	8.2.3 (p.104)	R	Register <code>hvip</code> (Hypervisor virtual-interrupt-pending register) is an HSXLEN-bit read/write WARL register that a hypervisor can write to indicate virtual interrupts intended for VS-mode.																												
RVP.8.93	8.2.3 (p.104) Figure 8.5	R	Hypervisor virtual-interrupt-pending register (<code>hvip</code>). <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>HSXLEN-1</td> <td>...</td> <td>0</td> </tr> <tr> <td colspan="3">Virtual Interrupts (WARL)</td> </tr> </table>	HSXLEN-1	...	0	Virtual Interrupts (WARL)																								
HSXLEN-1	...	0																													
Virtual Interrupts (WARL)																															
RVP.8.94	8.2.3 (p.104)	R	Bits of <code>hvip</code> that are not writable are read-only zeros.																												
RVP.8.95	8.2.3 (p.104) Figure 8.6	R	The standard portion (bits 15:0) of <code>hvip</code> is formatted as shown <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>15</td> <td>...</td> <td>11</td> <td>10</td> <td>9</td> <td>8</td> <td>7</td> <td>6</td> <td>5</td> <td>4</td> <td>3</td> <td>2</td> <td>1</td> <td>0</td> </tr> <tr> <td>0</td> <td></td> <td>VSEIP</td> <td>0</td> <td>VSTIP</td> <td>0</td> <td>VSSIP</td> <td>0</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	15	...	11	10	9	8	7	6	5	4	3	2	1	0	0		VSEIP	0	VSTIP	0	VSSIP	0						
15	...	11	10	9	8	7	6	5	4	3	2	1	0																		
0		VSEIP	0	VSTIP	0	VSSIP	0																								
RVP.8.96	8.2.3 (p.104)	R	Bits VSEIP, VSTIP, and VSSIP of <code>hvip</code> are writable.																												
RVP.8.97	8.2.3 (p.104)	R	Setting VSEIP=1 in <code>hvip</code> asserts a VS-level external interrupt; setting VSTIP asserts a VS-level timer interrupt; and setting VSSIP asserts a VS-level software interrupt.																												
RVP.8.98	8.2.3 (p.105)	R	Register <code>hip</code> (Hypervisor interrupt-pending register) is HSXLEN-bit read/write register that supplements HS-level's <code>sip</code> register.																												
RVP.8.99	8.2.3 (p.105) Figure 8.7	R	Hypervisor interrupt-pending register (<code>hip</code>). <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>HSXLEN-1</td> <td>...</td> <td>0</td> </tr> <tr> <td colspan="3">Interrupts (WARL)</td> </tr> </table>	HSXLEN-1	...	0	Interrupts (WARL)																								
HSXLEN-1	...	0																													
Interrupts (WARL)																															
RVP.8.100	8.2.3 (p.105)	R	Register <code>hie</code> (Hypervisor interrupt-enable register) is HSXLEN-bit read/write register that supplements HS-level's <code>sie</code> register.																												
RVP.8.101	8.2.3 (p.105) Figure 8.8	R	Hypervisor interrupt-enable register (<code>hie</code>). <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>HSXLEN-1</td> <td>...</td> <td>0</td> </tr> <tr> <td colspan="3">Interrupts (WARL)</td> </tr> </table>	HSXLEN-1	...	0	Interrupts (WARL)																								
HSXLEN-1	...	0																													
Interrupts (WARL)																															
RVP.8.102	8.2.3 (p.105)	R	Hence, the nonzero bits in <code>sie</code> and <code>hie</code> are always mutually exclusive, and likewise for <code>sip</code> and <code>hip</code> .																												
RVP.8.103	8.2.3 (p.105)	C	The active bits of <code>hip</code> and <code>hie</code> cannot be placed in HS-level's <code>sip</code> and <code>sie</code> because doing so would make it impossible for software to emulate the hypervisor extension on platforms that do not implement it in hardware.																												
RVP.8.104	8.2.3 (p.105)	R	An interrupt i will trap to HS-mode whenever all of the following are true: (a) either the current operating mode is HS-mode and the SIE bit in the sstatus register is set, or the current operating mode has less privilege than HS-mode; (b) bit i is set in both <code>sip</code> and <code>sie</code> , or in both <code>hip</code> and <code>hie</code> ; and (c) bit i is not set in <code>hidleg</code> .																												
RVP.8.105	8.2.3 (p.105)	R	If bit i of <code>sie</code> is read-only zero, the same bit in register <code>hip</code> may be writable or may be read-only.																												
RVP.8.106	8.2.3 (p.105)	R	When bit i in <code>hip</code> is writable, a pending interrupt i can be cleared by writing 0 to this bit.																												

ID REFERENCE TYPE DEFINITION

RVP.8.107	8.2.3 (p.105)	R	If interrupt <i>i</i> can become pending in <code>hip</code> but bit <i>i</i> in <code>hip</code> is read-only, then either the interrupt can be cleared by clearing bit <i>i</i> of <code>hvip</code> , or the implementation must provide some other mechanism for clearing the pending interrupt (which may involve a call to the execution environment).																																
RVP.8.108	8.2.3 (p.105)	R	A bit in <code>hie</code> shall be writable if the corresponding interrupt can ever become pending in <code>hip</code> .																																
RVP.8.109	8.2.3 (p.105)	R	Bits of <code>hie</code> that are not writable shall be read-only zero.																																
RVP.8.110	8.2.3 (p.105) Figure 8.9	R	The standard portions (bits 15:0) of register <code>hip</code> are formatted as:																																
			<table border="1" style="margin-left: auto; margin-right: auto;"><tr><td>15</td><td>14</td><td>13</td><td>12</td><td>11</td><td>10</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr><tr><td>0</td><td>SGEIP</td><td>0</td><td>VSEIP</td><td>0</td><td>VSTIP</td><td>0</td><td>VSSIP</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	0	SGEIP	0	VSEIP	0	VSTIP	0	VSSIP	0							
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0																				
0	SGEIP	0	VSEIP	0	VSTIP	0	VSSIP	0																											
RVP.8.111	8.2.3 (p.105) Figure 8.10	R	The standard portions (bits 15:0) of register <code>hie</code> are formatted as:																																
			<table border="1" style="margin-left: auto; margin-right: auto;"><tr><td>15</td><td>14</td><td>13</td><td>12</td><td>11</td><td>10</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr><tr><td>0</td><td>SGEIE</td><td>0</td><td>VSEIE</td><td>0</td><td>VSTIE</td><td>0</td><td>VSSIE</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	0	SGEIE	0	VSEIE	0	VSTIE	0	VSSIE	0							
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0																				
0	SGEIE	0	VSEIE	0	VSTIE	0	VSSIE	0																											
RVP.8.112	8.2.3 (p.105)	R	Bits <code>hip.SGEIP</code> and <code>hie.SGEIE</code> are the interrupt-pending and interrupt-enable bits for guest external interrupts at supervisor level (HS-level).																																
RVP.8.113	8.2.3 (p.105)	R	<code>SGEIP</code> is read-only in <code>hip</code> , and is 1 if and only if the bitwise logical-AND of CSRs <code>hgeip</code> and <code>hgeie</code> is nonzero in any bit. (See Section 8.2.4.)																																
RVP.8.114	8.2.3 (p.106)	R	Bits <code>hip.VSEIP</code> and <code>hie.VSEIE</code> are the interrupt-pending and interrupt-enable bits for VS-level external interrupts.																																
RVP.8.115	8.2.3 (p.106)	R	<code>VSEIP</code> is read-only in <code>hip</code> , and is the logical-OR of these interrupt sources: <ul style="list-style-type: none">• bit <code>VSEIP</code> of <code>hvip</code>;• the bit of <code>hgeip</code> selected by <code>hstatus.VGEIN</code>; and• any other platform-specific external interrupt signal directed to VS-level.																																
RVP.8.116	8.2.3 (p.106)	R	Bits <code>hip.VSTIP</code> and <code>hie.VSTIE</code> are the interrupt-pending and interrupt-enable bits for VS-level timer interrupts.																																
RVP.8.117	8.2.3 (p.106)	R	<code>VSTIP</code> is read-only in <code>hip</code> , and is the logical-OR of <code>hvip.VSTIP</code> and any other platform-specific timer interrupt signal directed to VS-level.																																
RVP.8.118	8.2.3 (p.106)	R	Bits <code>hip.VSSIP</code> and <code>hie.VSSIE</code> are the interrupt-pending and interrupt-enable bits for VS-level software interrupts.																																
RVP.8.119	8.2.3 (p.106)	R	<code>VSSIP</code> in <code>hip</code> is an alias (writable) of the same bit in <code>hvip</code> .																																
RVP.8.120	8.2.3 (p.106)	R	Multiple simultaneous interrupts destined for HS-mode are handled in the following decreasing priority order: SEI, SSI, STI, SGEI, VSEI, VSSI, VSTI.																																
RVP.8.121	8.2.4 (p.106)	H	Hypervisor Guest External Interrupt Registers (<code>hgeip</code> and <code>hgeie</code>)																																
RVP.8.122	8.2.4 (p.106)	R	The <code>hgeip</code> (Hypervisor guest external interrupt-pending) register is an HSXLEN-bit read-only register that indicates pending guest external interrupts for this hart.																																
RVP.8.123	8.2.4 (p.106) Figure 8.11	R	Hypervisor guest external interrupt-pending register (<code>hgeip</code>).																																

HSXLEN-1	...	1	0
Guest External Interrupts			0

ID	REFERENCE	TYPE	DEFINITION								
RVP.8.124	8.2.4 (p.106)	R	The <code>hgeie</code> (Hypervisor guest external interrupt-enable) register is an HSXLEN-bit read/write WARL register that contains enable bits for the guest external interrupts at this hart.								
RVP.8.125	8.2.4 (p.106) Figure 8.12	R	Hypervisor guest external interrupt-enable register (<code>hgeie</code>).								
			<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">HSXLEN-1</td> <td style="padding: 2px;">...</td> <td style="padding: 2px; text-align: center;">1</td> <td style="padding: 2px; text-align: center;">0</td> </tr> <tr> <td colspan="2"></td> <td colspan="2" style="text-align: center;">Guest External Interrupts (WARL)</td> </tr> </table>	HSXLEN-1	...	1	0			Guest External Interrupts (WARL)	
HSXLEN-1	...	1	0								
		Guest External Interrupts (WARL)									
RVP.8.126	8.2.4 (p.106)	R	Guest external interrupt number i corresponds with bit i in both <code>hgeip</code> and <code>hgeie</code> .								
RVP.8.127	8.2.4 (p.106)	R	Guest external interrupts represent interrupts directed to individual virtual machines at VS-level.								
RVP.8.128	8.2.4 (p.106)	R	If a RISC-V platform supports placing a physical device under the direct control of a guest OS with minimal hypervisor intervention (known as <i>pass-through</i> or <i>direct assignment</i> between a virtual machine and the physical device), then, in such circumstance, interrupts from the device are intended for a specific virtual machine.								
RVP.8.129	8.2.4 (p.106, p.107)	R	Each bit of <code>hgeip</code> summarizes all pending interrupts directed to one virtual hart, as collected and reported by an interrupt controller. To distinguish specific pending interrupts from multiple devices, software must query the interrupt controller.								
RVP.8.130	8.2.4 (p.107)	C	Support for guest external interrupts requires an interrupt controller that can collect virtual-machine-directed interrupts separately from other interrupts.								
RVP.8.131	8.2.4 (p.107)	R	The number of bits implemented in <code>hgeip</code> and <code>hgeie</code> for guest external interrupts is UNSPECIFIED and may be zero.								
RVP.8.132	8.2.4 (p.107)	I	This number (of bits implemented in <code>hgeip</code> and <code>hgeie</code>) is known as GEILEN.								
RVP.8.133	8.2.4 (p.107)	R	The least-significant bits are implemented first, apart from bit 0. Hence, if GEILEN is nonzero, bits GEILEN:1 shall be writable in <code>hgeie</code> , and all other bit positions shall be read-only zeros in both <code>hgeip</code> and <code>hgeie</code> .								
RVP.8.134	8.2.4 (p.107)	C	The set of guest external interrupts received and handled at one physical hart may differ from those received at other harts. Guest external interrupt number i at one physical hart is typically expected not to be the same as guest external interrupt i at any other hart. For any one physical hart, the maximum number of virtual harts that may directly receive guest external interrupts is limited by GEILEN. The maximum this number can be for any implementation is 31 for RV32 and 63 for RV64, per physical hart.								
RVP.8.135	8.2.4 (p.107)	C	A hypervisor is always free to emulate devices for any number of virtual harts without being limited by GEILEN. Only direct pass-through (direct assignment) of interrupts is affected by the GEILEN limit, and the limit is on the number of virtual harts receiving such interrupts, not the number of distinct interrupts received. The number of distinct interrupts a single virtual hart may receive is determined by the interrupt controller.								
RVP.8.136	8.2.4 (p.107)	R	Register <code>hgeie</code> selects the subset of guest external interrupts that cause a supervisor-level (HS-level) guest external interrupt.								
RVP.8.137	8.2.4 (p.107)	R	The enable bits in <code>hgeie</code> do not affect the VS-level external interrupt signal selected from <code>hgeip</code> by <code>hstatus.VGEIN</code> .								

ID REFERENCE TYPE DEFINITION

RVP.8.138	8.2.5 (p.107)	H	Hypervisor Environment Configuration Registers (<code>henvcfg</code> and <code>henvcfgh</code>)																										
RVP.8.139	8.2.5 (p.107)	R	The <code>henvcfg</code> (Hypervisor environment configuration register) CSR is an HSXLEN-bit read/write register that controls certain characteristics of the execution environment when virtualization mode V=1.																										
RVP.8.140	8.2.5 (p.107) Figure 8.13	R	Hypervisor environment configuration register (<code>henvcfg</code>) for HSXLEN=64.																										
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>63</td><td>62</td><td>61</td><td>...</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>VSTCE</td><td>PBMTE</td><td>WPRI</td><td></td><td>CBZE</td><td>CBCFE</td><td>CBIE</td><td></td><td>WPRI</td><td></td><td></td><td></td><td>FIOM</td> </tr> </table>	63	62	61	...	8	7	6	5	4	3	2	1	0	VSTCE	PBMTE	WPRI		CBZE	CBCFE	CBIE		WPRI				FIOM
63	62	61	...	8	7	6	5	4	3	2	1	0																	
VSTCE	PBMTE	WPRI		CBZE	CBCFE	CBIE		WPRI				FIOM																	
RVP.8.141	8.2.5 (p.107)	R	If bit FIOM (Fence of I/O implies Memory) is set to one in <code>henvcfg</code> , FENCE instructions executed when V=1 are modified so the requirement to order accesses to device I/O implies also the requirement to order main memory accesses.																										
RVP.8.142	8.2.5 (p.107) Table 8.3	R	The table below details the modified interpretation of FENCE instruction bits PI, PO, SI, and SO when FIOM=1 and V=1.																										
			<table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Instruction bit</th><th>Meaning when set</th></tr> </thead> <tbody> <tr> <td>PI</td><td>Predecessor device input and memory reads (PR implied)</td></tr> <tr> <td>PO</td><td>Predecessor device output and memory writes (PW implied)</td></tr> <tr> <td>SI</td><td>Successor device input and memory reads (SR implied)</td></tr> <tr> <td>SO</td><td>Successor device output and memory writes (SW implied)</td></tr> </tbody> </table>	Instruction bit	Meaning when set	PI	Predecessor device input and memory reads (PR implied)	PO	Predecessor device output and memory writes (PW implied)	SI	Successor device input and memory reads (SR implied)	SO	Successor device output and memory writes (SW implied)																
Instruction bit	Meaning when set																												
PI	Predecessor device input and memory reads (PR implied)																												
PO	Predecessor device output and memory writes (PW implied)																												
SI	Successor device input and memory reads (SR implied)																												
SO	Successor device output and memory writes (SW implied)																												
RVP.8.143	8.2.5 (p.107)	R	Similarly, when FIOM=1 and V=1, if an atomic instruction that accesses a region ordered as device I/O has its <i>aq</i> and/or <i>rl</i> bit set, then that instruction is ordered as though it accesses both device I/O and memory.																										
RVP.8.144	8.2.5 (p.108)	R	The PBMTE bit controls whether the Svpbmt extension is available for use in VS-stage address translation.																										
RVP.8.145	8.2.5 (p.108)	R	When PBMTE=1, Svpbmt is available for VS-stage address translation.																										
RVP.8.146	8.2.5 (p.108)	R	When PBMTE=0, the implementation behaves as though Svpbmt were not implemented for VS-stage address translation.																										
RVP.8.147	8.2.5 (p.108)	R	If Svpbmt is not implemented, PBMTE is read-only zero.																										
RVP.8.148	8.2.5 (p.108)	R	The definition of the VSTCE field will be furnished by the forthcoming Sstc extension. Its allocation within <code>henvcfg</code> may change prior to the ratification of that extension.																										
RVP.8.149	8.2.5 (p.108)	R	The definition of the CBZE field will be furnished by the forthcoming Zicboz extension. Its allocation within <code>henvcfg</code> may change prior to the ratification of that extension																										
RVP.8.150	8.2.5 (p.108)	R	The definitions of the CBCFE and CBIE fields will be furnished by the forthcoming Zicbom extension. Their allocations within <code>henvcfg</code> may change prior to the ratification of that extension.																										
RVP.8.151	8.2.5 (p.108)	R	When HSXLEN=32, <code>henvcfg</code> contains the same fields as bits 31:0 of <code>henvcfg</code> when HSXLEN=64.																										
RVP.8.152	8.2.5 (p.108)	R	Additionally, when HSXLEN=32, <code>henvcfgh</code> is a 32-bit read/write register that contains the same fields as bits 63:32 of <code>henvcfg</code> when HSXLEN=64.																										
RVP.8.153	8.2.5 (p.108)	R	Register <code>henvcfgh</code> does not exist when HSXLEN=64.																										
RVP.8.154	8.2.6 (p.108)	H	Hypervisor Counter-Enable Register (<code>hcounteren</code>)																										

ID REFERENCE TYPE DEFINITION

RVP.8.155 8.2.6 (p.108) R Hypervisor counter-enable register `hcounteren` is a 32-bit register that controls the availability of the hardware performance monitoring counters to the guest virtual machine.

RVP.8.156 8.2.6 (p.108) R Hypervisor counter-enable register (`hcounteren`).

31	30	29	...	5	4	3	2	1	0
HPM31	HPM30	HPM29	...	HPM5	HPM4	HPM3	IR	TM	CY

RVP.8.157 8.2.6 (p.108) R When the CY, TM, IR, or HPM_n bit in the `hcounteren` register is clear, attempts to read the `cycle`, `time`, `instret`, or `hpmcounter` register while V=1 will cause a virtual instruction exception if the same bit in `mcounteren` is 1.

RVP.8.158 8.2.6 (p.108) R When one of these bits is set, access to the corresponding register is permitted when V=1, unless prevented for some other reason.

RVP.8.159 8.2.6 (p.108) R In VU-mode, a counter is not readable unless the applicable bits are set in both `hcounteren` and `scounteren`.

RVP.8.160 8.2.6 (p.108) R `hcounteren` must be implemented.

RVP.8.161 8.2.6 (p.108) R However, any of the bits (of `hcounteren`) may be read-only zero, indicating reads to the corresponding counter will cause an exception when V=1.

RVP.8.162 8.2.6 (p.108) R Hence, they (bits in `hcounteren`) are effectively WARL fields.

RVP.8.163 8.2.7 (p.109) H Hypervisor Time Delta Registers (`htimedelta`, `htimedeltah`)

RVP.8.164 8.2.7 (p.109) R The `htimedelta` (Hypervisor Time Delta Register) CSR is a read/write register that contains the delta between the value of the time CSR and the value returned in VS-mode or VU-mode.

RVP.8.165 8.2.7 (p.109) R Hypervisor time delta register, HSXLEN=64
Figure 8.15

63	...	0
htimedelta		

RVP.8.166 8.2.7 (p.109) R That is, reading the time CSR in VS or VU mode returns the sum of the contents of `htimedelta` and the actual value of `time`.

RVP.8.167 8.2.7 (p.109) C Because overflow is ignored when summing `htimedelta` and `time`, large values of `htimedelta` may be used to represent negative time offsets.

RVP.8.168 8.2.7 (p.109) R For HSXLEN=32 only, `htimedelta` holds the lower 32 bits of the delta, and `htimedeltah` holds the upper 32 bits of the delta.

RVP.8.169 8.2.7 (p.109) R Hypervisor time delta registers, HSXLEN=32.
Figure 8.16

31	...	0
htimedelta		
htimedeltah		

RVP.8.170 8.2.8 (p.109) H Hypervisor Trap Value Register (`htval`)

RVP.8.171 8.2.8 (p.109) R The `htval` register is an HSXLEN-bit read/write register.

RVP.8.172 8.2.8 (p.109) R Hypervisor trap value register (`htval`).
Figure 8.17

HSXLEN-1	...	0
htval		

ID	REFERENCE	TYPE	DEFINITION
RVP.8.173	8.2.8 (p.109)	R	When a trap is taken into HS-mode, <code>htval</code> is written with additional exception-specific information, alongside <code>stval</code> , to assist software in handling the trap.
RVP.8.174	8.2.8 (p.109)	R	When a guest-page-fault trap is taken into HS-mode, <code>htval</code> is written with either zero or the guest physical address that faulted, shifted right by 2 bits.
RVP.8.175	8.2.8 (p.109)	R	For other traps, <code>htval</code> is set to zero, but a future standard or extension may redefine <code>htval</code> 's setting for other traps.
RVP.8.176	8.2.8 (p.109)	R	A guest-page fault may arise due to an implicit memory access during first-stage (VS-stage) address translation, in which case a guest physical address written to <code>htval</code> is that of the implicit memory access that faulted—for example, the address of a VS-level page table entry that could not be read. (The guest physical address corresponding to the original virtual address is unknown when VS-stage translation fails to complete.)
RVP.8.177	8.2.8 (p.109)	R	Additional information is provided in CSR <code>htinst</code> to disambiguate such situations.
RVP.8.178	8.2.8 (p.109)	R	Otherwise, for misaligned loads and stores that cause guest-page faults, a nonzero guest physical address in <code>htval</code> corresponds to the faulting portion of the access as indicated by the virtual address in <code>stval</code> .
RVP.8.179	8.2.8 (p.110)	R	For instruction guest-page faults on systems with variable-length instructions, a nonzero <code>htval</code> corresponds to the faulting portion of the instruction as indicated by the virtual address in <code>stval</code> .
RVP.8.180	8.2.8 (p.110)	C	A guest physical address written to <code>htval</code> is shifted right by 2 bits to accommodate addresses wider than the current XLEN. For RV32, the hypervisor extension permits guest physical addresses as wide as 34 bits, and <code>htval</code> reports bits 33:2 of the address. This shift-by-2 encoding of guest physical addresses matches the encoding of physical addresses in PMP address registers (Section 3.7) and in page table entries (Sections 4.3, 4.4, 4.5, and 4.6).
RVP.8.181	8.2.8 (p.110)	C	If the least-significant two bits of a faulting guest physical address are needed, these bits are ordinarily the same as the least-significant two bits of the faulting virtual address in <code>stval</code> . For faults due to implicit memory accesses for VS-stage address translation, the least-significant two bits are instead zeros. These cases can be distinguished using the value provided in register <code>htinst</code> .
RVP.8.182	8.2.8 (p.110)	R	<code>htval</code> is a WARL register that must be able to hold zero and may be capable of holding only an arbitrary subset of other 2-bit-shifted guest physical addresses, if any.
RVP.8.183	8.2.8 (p.110)	C	Unless it has reason to assume otherwise (such as a platform standard), software that writes a value to <code>htval</code> should read back from <code>htval</code> to confirm the stored value.
RVP.8.184	8.2.9 (p.110)	R	Hypervisor Trap Instruction Register (<code>htinst</code>)
RVP.8.185	8.2.9 (p.110)	R	The <code>htinst</code> register is an HSXLEN-bit read/write register
RVP.8.186	8.2.9 (p.110)	R	Hypervisor trap instruction register (<code>htinst</code>). Figure 8.18

- RVP.8.173 8.2.8 (p.109) R When a trap is taken into HS-mode, `htval` is written with additional exception-specific information, alongside `stval`, to assist software in handling the trap.
- RVP.8.174 8.2.8 (p.109) R When a guest-page-fault trap is taken into HS-mode, `htval` is written with either zero or the guest physical address that faulted, shifted right by 2 bits.
- RVP.8.175 8.2.8 (p.109) R For other traps, `htval` is set to zero, but a future standard or extension may redefine `htval`'s setting for other traps.
- RVP.8.176 8.2.8 (p.109) R A guest-page fault may arise due to an implicit memory access during first-stage (VS-stage) address translation, in which case a guest physical address written to `htval` is that of the implicit memory access that faulted—for example, the address of a VS-level page table entry that could not be read. (The guest physical address corresponding to the original virtual address is unknown when VS-stage translation fails to complete.)
- RVP.8.177 8.2.8 (p.109) R Additional information is provided in CSR `htinst` to disambiguate such situations.
- RVP.8.178 8.2.8 (p.109) R Otherwise, for misaligned loads and stores that cause guest-page faults, a nonzero guest physical address in `htval` corresponds to the faulting portion of the access as indicated by the virtual address in `stval`.
- RVP.8.179 8.2.8 (p.110) R For instruction guest-page faults on systems with variable-length instructions, a nonzero `htval` corresponds to the faulting portion of the instruction as indicated by the virtual address in `stval`.
- RVP.8.180 8.2.8 (p.110) C A guest physical address written to `htval` is shifted right by 2 bits to accommodate addresses wider than the current XLEN. For RV32, the hypervisor extension permits guest physical addresses as wide as 34 bits, and `htval` reports bits 33:2 of the address. This shift-by-2 encoding of guest physical addresses matches the encoding of physical addresses in PMP address registers (Section 3.7) and in page table entries (Sections 4.3, 4.4, 4.5, and 4.6).
- RVP.8.181 8.2.8 (p.110) C If the least-significant two bits of a faulting guest physical address are needed, these bits are ordinarily the same as the least-significant two bits of the faulting virtual address in `stval`. For faults due to implicit memory accesses for VS-stage address translation, the least-significant two bits are instead zeros. These cases can be distinguished using the value provided in register `htinst`.
- RVP.8.182 8.2.8 (p.110) R `htval` is a WARL register that must be able to hold zero and may be capable of holding only an arbitrary subset of other 2-bit-shifted guest physical addresses, if any.
- RVP.8.183 8.2.8 (p.110) C Unless it has reason to assume otherwise (such as a platform standard), software that writes a value to `htval` should read back from `htval` to confirm the stored value.
- RVP.8.184 8.2.9 (p.110) R Hypervisor Trap Instruction Register (`htinst`)
- RVP.8.185 8.2.9 (p.110) R The `htinst` register is an HSXLEN-bit read/write register
- RVP.8.186 8.2.9 (p.110) R Hypervisor trap instruction register (`htinst`).
Figure 8.18

HSXLEN-1	...	0
htinst		

ID REFERENCE TYPE DEFINITION

RVP.8.187 8.2.9 (p.110) R When a trap is taken into HS-mode, htinst is written with a value that, if nonzero, provides information about the instruction that trapped, to assist software in handling the trap.

RVP.8.188 8.2.9 (p.110) I The values that may be written to htinst on a trap are documented in Section 8.6.3.

RVP.8.189 8.2.9 (p.110) R htinst is a WARL register that need only be able to hold the values that the implementation may automatically write to it on a trap.

RVP.8.190 8.2.10 (p.110) H Hypervisor Guest Address Translation and Protection Register (hgatp)

RVP.8.191 8.2.10 (p.110) R The hgatp register is an HSXLEN-bit read/write register which controls G-stage address translation and protection, the second stage of two-stage translation for guest virtual addresses (see Section 8.5).

RVP.8.192 8.2.10 (p.111) R Hypervisor guest address translation and protection register hgatp when HSXLEN=32

31	30	29	28	...	22	21	...	0
MODE	0	0		VMID			PPN	

RVP.8.193 8.2.10 (p.111) R Hypervisor guest address translation and protection register hgatp when HSXLEN=64, for MODE values Bare, Sv39x4, Sv48x4, and Sv57x4.

63	...	60	59	58	57	...	44	43	...	0
MODE	0	0		VMID			PPN			

RVP.8.194 8.2.10 (p.110) R Similar to CSR satp, this register holds the physical page number (PPN) of the guest-physical root page table; a virtual machine identifier (VMID), which facilitates address-translations fences on a per-virtual-machine basis; and the MODE field, which selects the address-translations scheme for guest physical addresses.

RVP.8.195 8.2.10 (p.110) R When mstatus.TVM=1, attempts to read or write hgatp while executing in HS-mode will raise an illegal instruction exception.

RVP.8.196 8.2.10 (p.111) R Table below shows the encodings of hgatp MODE field when HSXLEN=32

Value	Name	Description
0	Bare	No translation or protection.
1	Sv32x4	Page-based 34-bit virtual addressing (2-bit extension of Sv32)

RVP.8.197 8.2.10 (p.111) R Table below shows the encodings of hgatp MODE field when HSXLEN=64

Value	Name	Description
0	Bare	No translation or protection.
1-7	-	Reserved
8	Sv39x4	Page-based 41-bit virtual addressing (2-bit extension of Sv39)
9	Sv48x4	Page-based 50-bit virtual addressing (2-bit extension of Sv48)
10	Sv57x4	Page-based 59-bit virtual addressing (2-bit extension of Sv57)
11-15	-	Reserved

RVP.8.198 8.2.10 (p.111) R When MODE=Bare, guest physical addresses are equal to supervisor physical addresses, and there is no further memory protection for a guest virtual machine beyond the physical memory protection scheme described in Section 3.7.

ID	REFERENCE	TYPE	DEFINITION
RVP.8.199	8.2.10 (p.111)	R	In this case (MODE=Bare), the remaining fields in <code>hgatp</code> must be set to zeros.
RVP.8.200	8.2.10 (p.111)	R	When HSXLEN=32, the only other valid setting for MODE is Sv32x4, which is a modification of the usual Sv32 paged virtual-memory scheme, extended to support 34-bit guest physical addresses.
RVP.8.201	8.2.10 (p.111)	R	When HSXLEN=64, modes Sv39x4, Sv48x4, and Sv57x4 are defined as modifications of the Sv39, Sv48, and Sv57 paged virtual-memory schemes.
RVP.8.202	8.2.10 (p.111)	I	All of these paged virtual-memory schemes are described in Section 8.5.1.
RVP.8.203	8.2.10 (p.111)	R	The remaining MODE settings when HSXLEN=64 are reserved for future use and may define different interpretations of the other fields in <code>hgatp</code> .
RVP.8.204	8.2.10 (p.111)	R	Implementations are not required to support all defined MODE settings when HSXLEN=64.
RVP.8.205	8.2.10 (p.111)	R	A write to <code>hgatp</code> with an unsupported MODE value is not ignored as it is for <code>satp</code> . Instead, the fields of <code>hgatp</code> are WARL in the normal way, when so indicated.
RVP.8.206	8.2.10 (p.111, p.112)	R	As explained in Section 8.5.1, for the paged virtual-memory schemes (Sv32x4, Sv39x4, Sv48x4, and Sv57x4), the root page table is 16 KiB and must be aligned to a 16-KiB boundary. In these modes, the lowest two bits of the physical page number (PPN) in <code>hgatp</code> always read as zeros.
RVP.8.207	8.2.10 (p.112)	R	An implementation that supports only the defined paged virtual-memory schemes and/or Bare may make PPN[1:0] read-only zero.
RVP.8.208	8.2.10 (p.112)	R	The number of VMID bits is UNSPECIFIED and may be zero.
RVP.8.209	8.2.10 (p.112)	R	The number of implemented VMID bits, termed VMIDLEN, may be determined by writing one to every bit position in the VMID field, then reading back the value in <code>hgatp</code> to see which bit positions in the VMID field hold a one.
RVP.8.210	8.2.10 (p.112)	R	The least-significant bits of VMID are implemented first: that is, if VMIDLEN > 0, VMID[VMIDLEN-1:0] is writable.
RVP.8.211	8.2.10 (p.112)	R	The maximal value of VMIDLEN, termed VMIDMAX, is 7 for Sv32x4 or 14 for Sv39x4, Sv48x4, and Sv57x4.
RVP.8.212	8.2.10 (p.112)	R	The <code>hgatp</code> register is considered active for the purposes of the address-translation algorithm unless the effective privilege mode is U and <code>hstatus.HU=0</code> .
RVP.8.213	8.2.10 (p.112)	C	This definition simplifies the implementation of speculative execution of HLV, HLVX, and HSV instructions.
RVP.8.214	8.2.10 (p.112)	R	Note that writing <code>hgatp</code> does not imply any ordering constraints between page-table updates and subsequent G-stage address translations.
RVP.8.215	8.2.10 (p.112)	R	If the new virtual machine's guest physical page tables have been modified, or if a VMID is reused, it may be necessary to execute an HFENCE.GVMA instruction (see Section 8.3.2) before or after writing <code>hgatp</code> .
RVP.8.216	8.2.11 (p.112)	H	Virtual Supervisor Status Register (<code>vsstatus</code>)
RVP.8.217	8.2.11 (p.112)	R	The <code>vsstatus</code> register is a VSXLEN-bit read/write register that is VS-mode's version of supervisor register <code>sstatus</code>

ID REFERENCE TYPE DEFINITION

RVP.8.218 8.2.11 (p.112) R Virtual supervisor status register (`vsstatus`) when VSXLEN=32

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
SD												MXR	SUM	WPRI

16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
XS	FS	WPRI	VS	SPP	WPRI	UBE	SPIE		WPRI	SIE	WPRI					

RVP.8.219 8.2.11 (p.112) R Virtual supervisor status register (`vsstatus`) when VSXLEN=64

63	62	...	34	33	32	31	...	20	19	18	17
SD			WPRI		UXL		WPRI		MXR	SUM	WPRI

16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
XS	FS	WPRI	VS	SPP	WPRI	UBE	SPIE		WPRI	SIE	WPRI					

RVP.8.220 8.2.11 (p.112) R When V=1, `vsstatus` substitutes for the usual `sstatus`, so instructions that normally read or modify `sstatus` actually access `vsstatus` instead.

RVP.8.221 8.2.11 (p.113) R The UXL field controls the effective XLEN for VU-mode, which may differ from the XLEN for VSmode (VSXLEN).

RVP.8.222 8.2.11 (p.113) R When VSXLEN=32, the UXL field does not exist, and VU-mode XLEN=32

RVP.8.223 8.2.11 (p.113) R When VSXLEN=64, UXL is a WARL field that is encoded the same as the MXL field of `misa`

UXL	XLEN
1	32
2	64
3	128

RVP.8.224 8.2.11 (p.113) R In particular, an implementation may make UXL be a read-only copy of field VSXL of `hstatus`, forcing VU-mode XLEN=VSXLEN.

RVP.8.225 8.2.11 (p.113) R If VSXLEN is changed from 32 to a wider width, and if field UXL is not restricted to a single value, it gets the value corresponding to the widest supported width not wider than the new VSXLEN.

RVP.8.226 8.2.11 (p.113) R When V=1, both `vsstatus.FS` and the HS-level `sstatus.FS` are in effect.

RVP.8.227 8.2.11 (p.113) R Attempts to execute a floating-point instruction when either field is 0 (Off) raise an illegal-instruction exception.

RVP.8.228 8.2.11 (p.113) R Modifying the floating-point state when V=1 causes both fields to be set to 3 (Dirty).

ID REFERENCE TYPE DEFINITION

- RVP.8.229 8.2.11 (p.113) C For a hypervisor to benefit from the extension context status, it must have its own copy in the HS-level `sstatus`, maintained independently of a guest OS running in VS-mode. While a version of the extension context status obviously must exist in `vsstatus` for VS-mode, a hypervisor cannot rely on this version being maintained correctly, given that VS-level software can change `vsstatus.FS` arbitrarily. If the HS-level `sstatus.FS` were not independently active and maintained by the hardware in parallel with `vsstatus.FS` while $V=1$, hypervisors would always be forced to conservatively swap all floating-point state when context-switching between virtual machines.
- RVP.8.230 8.2.11 (p.113) R Similarly, when $V=1$, both `vsstatus.VS` and the HS-level `sstatus.VS` are in effect.
- RVP.8.231 8.2.11 (p.113) R Attempts to execute a vector instruction when either field is 0 (Off) raise an illegal-instruction exception.
- RVP.8.232 8.2.11 (p.113) R Modifying the vector state when $V=1$ causes both fields to be set to 3 (Dirty).
- RVP.8.233 8.2.11 (p.113) R Read-only fields SD and XS summarize the extension context status as it is visible to VS-mode only. For example, the value of the HS-level `sstatus.FS` does not affect `vsstatus.SD`.
- RVP.8.234 8.2.11 (p.113) R An implementation may make field UBE be a read-only copy of `hstatus.VSBE`.
- RVP.8.235 8.2.11 (p.113) R When $V=0$, `vsstatus` does not directly affect the behavior of the machine, unless a virtual-machine load/store (HLV, HLVX, or HSV) or the MPRV feature in the `mstatus` register is used to execute a load or store as though $V=1$.
- RVP.8.236 8.2.12 (p.113) H Virtual Supervisor Interrupt Registers (`vsip` and `vsie`)
- RVP.8.237 8.2.12 (p.113) R The `vsip` (Virtual supervisor interrupt-pending) register is VSXLEN-bit read/write WARL register that is VS-mode's versions of supervisor CSRs `sip` register
- RVP.8.238 8.2.12 (p.113) R Virtual supervisor interrupt-pending register (`vsip`).
Figure 8.23
- | | | |
|-------------------|-----|---|
| VSXLEN-1 | ... | 0 |
| Interrupts (WARL) | | |
- RVP.8.239 8.2.12 (p.113) R The `vsie` (Virtual supervisor interrupt-enable) register is VSXLEN-bit read/write WARL register that is VS-mode's versions of supervisor CSRs `sie` register
- RVP.8.240 8.2.12 (p.113) R Virtual supervisor interrupt-enable register (`vsie`).
Figure 8.24
- | | | |
|-------------------|-----|---|
| VSXLEN-1 | ... | 0 |
| Interrupts (WARL) | | |
- RVP.8.241 8.2.12 (p.113) R When $V=1$, `vsip` and `vsie` substitute for the usual `sip` and `sie`, so instructions that normally read or modify `sip/sie` actually access `vsip/vsie` instead.
- RVP.8.242 8.2.12 (p.113) R However, interrupts directed to HS-level continue to be indicated in the HS-level `sip` register, not in `vsip`, when $V=1$.

ID REFERENCE TYPE DEFINITION

RVP.8.243 8.2.12 (p.114) R
Figure 8.25

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0						SEIP	0		STIP	0		SSIP	0		

RVP.8.244 8.2.12 (p.114) R
Figure 8.26

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0						SEIE	0		STIE	0		SSIE	0		

RVP.8.245 8.2.12 (p.114) R

When bit 10 of `hideleg` is zero, `vsip.SEIP` and `vsie.SEIE` are read-only zeros. Else, `vsip.SEIP` and `vsie.SEIE` are aliases of `hip.VSEIP` and `hie.VSEIE`.

RVP.8.246 8.2.12 (p.114) R

When bit 6 of `hideleg` is zero, `vsip.STIP` and `vsie.STIE` are read-only zeros. Else, `vsip.STIP` and `vsie.STIE` are aliases of `hip.VSTIP` and `hie.VSTIE`.

RVP.8.247 8.2.12 (p.114) R

When bit 2 of `hideleg` is zero, `vsip.SSIP` and `vsie.SSIE` are read-only zeros. Else, `vsip.SSIP` and `vsie.SSIE` are aliases of `hip.VSSIP` and `hie.VSSIE`.

RVP.8.248 8.2.13 (p.114) H

RVP.8.249 8.2.13 (p.114) R

The `vstvec` register is a VSXLEN-bit read/write register that is VS-mode's version of supervisor register `stvec`

RVP.8.250 8.2.13 (p.114) R
Figure 8.27

VSXLEN-1	...	2	1	0
BASE[VSXLEN-1:2] (WARL)				MODE (WARL)

RVP.8.251 8.2.13 (p.114) R

When `V=1`, `vstvec` substitutes for the usual `stvec`, so instructions that normally read or modify `stvec` actually access `vstvec` instead.

RVP.8.252 8.2.13 (p.114) R

When `V=0`, `vstvec` does not directly affect the behavior of the machine.

RVP.8.253 8.2.14 (p.114) H

RVP.8.254 8.2.14 (p.114) R

The `vsscratch` (Virtual Supervisor Scratch) register is a VSXLEN-bit read/write register that is VS-mode's version of supervisor register `sscratch`,

RVP.8.255 8.2.14 (p.114) R
Figure 8.28

VSXLEN-1	...	0
vsscratch		

RVP.8.256 8.2.14 (p.114) R

When `V=1`, `vsscratch` substitutes for the usual `sscratch`, so instructions that normally read or modify `sscratch` actually access `vsscratch` instead.

RVP.8.257 8.2.14 (p.114) R

The contents of `vsscratch` never directly affect the behavior of the machine.

RVP.8.258 8.2.15 (p.115) H

RVP.8.259 8.2.15 (p.115) R

The `vsepc` register is a VSXLEN-bit read/write register that is VS-mode's version of supervisor register `sepc`

ID REFERENCE TYPE DEFINITION

RVP.8.260 8.2.15 (p.115) R
Figure 8.29

VSXLEN-1	...	0
vsepc		

RVP.8.261 8.2.15 (p.115) R

When V=1, vsepc substitutes for the usual sepc, so instructions that normally read or modify sepc actually access vsepc instead.

RVP.8.262 8.2.15 (p.115) R

V=0, vsepc does not directly affect the behavior of the machine.

RVP.8.263 8.2.15 (p.115) R

vsepc is a WARL register that must be able to hold the same set of values that sepc can hold.

RVP.8.264 8.2.16 (p.115) H

Virtual Supervisor Cause Register (vscause)

RVP.8.265 8.2.16 (p.115) R

The vscause register is a VSXLEN-bit read/write register that is VS-mode's version of supervisor register scause

RVP.8.266 8.2.16 (p.115) R

Figure 8.30

Virtual supervisor cause register (vscause).

VSXLEN-1	VSXLEN-2	...	0
Interrupt	Exception Code		

RVP.8.267 8.2.16 (p.115) R

When V=1, vscause substitutes for the usual scause, so instructions that normally read or modify scause actually access vscause instead.

RVP.8.268 8.2.16 (p.115) R

When V=0, vscause does not directly affect the behavior of the machine.

RVP.8.269 8.2.16 (p.115) R

vscause is a WLRL register that must be able to hold the same set of values that scause can hold.

RVP.8.270 8.2.17 (p.115) H

Virtual Supervisor Trap Value Register (vstval)

RVP.8.271 8.2.17 (p.115) R

The vstval register is a VSXLEN-bit read/write register that is VS-mode's version of supervisor register stval

RVP.8.272 8.2.17 (p.115) R

Figure 8.31

Virtual supervisor trap value register (vstval).

VSXLEN-1	...	0
vstval		

RVP.8.273 8.2.17 (p.115) R

When V=1, vstval substitutes for the usual stval, so instructions that normally read or modify stval actually access vstval instead.

RVP.8.274 8.2.17 (p.115) R

When V=0, vstval does not directly affect the behavior of the machine.

RVP.8.275 8.2.17 (p.115) R

vstval is a WARL register that must be able to hold the same set of values that stval can hold.

RVP.8.276 8.2.18 (p.116) R

Virtual Supervisor Address Translation and Protection Register (vsatp)

RVP.8.277 8.2.18 (p.116) R

The vsatp register is a VSXLEN-bit read/write register that is VS-mode's version of supervisor register satp,

RVP.8.278 8.2.18 (p.116) R

Figure 8.32

Virtual supervisor address translation and protection register vsatp when VSXLEN=32.

31	30	...	22	21	...	0
MODE	ASID			PPN		

ID REFERENCE TYPE DEFINITION

RVP.8.279	8.2.18 (p.116)	R	Virtual supervisor address translation and protection register vsatp when VSXLEN=64, for MODE values Bare, Sv39, Sv48, and Sv57																																																																																																																																									
	Figure 8.33																																																																																																																																											
			<table border="1"> <tr> <td>63</td><td>...</td><td>60</td><td>59</td><td>...</td><td>44</td><td>43</td><td>...</td><td>0</td></tr> <tr> <td colspan="4">MODE</td><td colspan="3">ASID</td><td colspan="2">PPN</td></tr> </table>	63	...	60	59	...	44	43	...	0	MODE				ASID			PPN																																																																																																																								
63	...	60	59	...	44	43	...	0																																																																																																																																				
MODE				ASID			PPN																																																																																																																																					
RVP.8.280	8.2.18 (p.116)	R	The vsatp register is considered active for the purposes of the address-translation algorithm unless the effective privilege mode is U and hstatus.HU=0.																																																																																																																																									
RVP.8.281	8.2.18 (p.116)	R	However, even when vsatp is active, VS-stage page-table entries' A bits must not be set as a result of speculative execution, unless the effective privilege mode is VS or VU.																																																																																																																																									
RVP.8.282	8.2.18 (p.116)	C	In particular, virtual-machine load/store (HLV, HLVX, or HSV) instructions that are misspeculatively executed must not cause VS-stage A bits to be set.																																																																																																																																									
RVP.8.283	8.2.18 (p.116)	R	When V=0, a write to vsatp with an unsupported MODE value is not ignored as it is for satp. Instead, the fields of vsatp are WARL in the normal way.																																																																																																																																									
RVP.8.284	8.2.18 (p.116)	R	When V=0, vsatp does not directly affect the behavior of the machine, unless a virtual-machine load/store (HLV, HLVX, or HSV) or the MPRV feature in the mstatus register is used to execute a load or store as though V=1.																																																																																																																																									
RVP.8.285	8.3 (p.116)	H	Hypervisor Instructions																																																																																																																																									
RVP.8.286	8.3 (p.116)	I	The hypervisor extension adds virtual-machine load and store instructions and two privileged fence instructions.																																																																																																																																									
RVP.8.287	8.3.1 (p.117) 9.0 (p.138)	R	<p>HLV.B Instruction Encoding: R-Type</p> <table border="1"> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td colspan="12">HLV.B</td><td colspan="4">rs1 / addr</td><td colspan="2">PRIVM</td><td colspan="4">rd</td><td colspan="8">SYSTEM</td></tr> <tr> <td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr> </table> <p>Valid Base: RV32, RV64, RV128 Task: – Explanation: See RVP.8.300 through RVP.8.316 Special Case: none Exception: none</p>	3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0												HLV.B												rs1 / addr				PRIVM		rd				SYSTEM								0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1						
3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																																												
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																																							
HLV.B												rs1 / addr				PRIVM		rd				SYSTEM																																																																																																																						
0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1																																																																																																										
RVP.8.288	8.3.1 (p.117) 9.0 (p.138)	R	<p>HLV.BU Instruction Encoding: R-Type</p> <table border="1"> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td colspan="12">HLV.BU</td><td colspan="4">rs1 / addr</td><td colspan="2">PRIVM</td><td colspan="4">rd</td><td colspan="8">SYSTEM</td></tr> <tr> <td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr> </table> <p>Valid Base: RV32, RV64, RV128 Task: – Explanation: See RVP.8.300 through RVP.8.316 Special Case: none Exception: none</p>	3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0													HLV.BU												rs1 / addr				PRIVM		rd				SYSTEM								0	1	1	0	0	0	0	0	0	0	0	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1
3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																																									
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																																							
HLV.BU												rs1 / addr				PRIVM		rd				SYSTEM																																																																																																																						
0	1	1	0	0	0	0	0	0	0	0	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1																																																																																																								

ID REFERENCE TYPE DEFINITION

RVP.8.289 8.3.1 (p.117) R
9.0 (p.138)

HLV.H Instruction

Encoding: R-Type

3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0								
HLV.H										rs1 / addr		PRIVM		rd		SYSTEM													
0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	1	1	1	0	0	1	1		

Valid Base: RV32, RV64, RV128

Task: –

Explanation: See RVP.8.300 through RVP.8.316

Special Case: none

Exception: none

RVP.8.290 8.3.1 (p.117) R
9.0 (p.138)

HLV.HU Instruction

Encoding: R-Type

3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0									
HLV.HU										rs1 / addr		PRIVM		rd		SYSTEM														
0	1	1	0	0	1	0	0	0	0	1	1	0	0	0	0	1	0	0	1	0	1	1	1	0	0	1	1			

Valid Base: RV32, RV64, RV128

Task: –

Explanation: See RVP.8.300 through RVP.8.316

Special Case: none

Exception: none

RVP.8.291 8.3.1 (p.117) R
9.0 (p.138)

HLVX.HU Instruction

Encoding: R-Type

3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0									
HLVX.HU										rs1 / addr		PRIVM		rd		SYSTEM														
0	1	1	0	0	1	0	0	0	0	1	1	0	0	0	0	1	0	0	1	0	1	1	1	0	0	1	1			

Valid Base: RV32, RV64, RV128

Task: –

Explanation: See RVP.8.300 through RVP.8.316

Special Case: none

Exception: none

RVP.8.292 8.3.1 (p.117) R
9.0 (p.138)

HLV.W Instruction

Encoding: R-Type

3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0									
HLV.W										rs1 / addr		PRIVM		rd		SYSTEM														
0	1	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1	0	1	1	1	0	0	1	1		

Valid Base: RV32, RV64, RV128

Task: –

Explanation: See RVP.8.300 through RVP.8.316

Special Case: none

Exception: none

ID REFERENCE TYPE DEFINITION

RVP.8.293	8.3.1 (p.117) 9.0 (p.138)	R	HLVX.WU Instruction Encoding: R-Type																																																																																																																											
			<table border="1"> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td colspan="12">HLVX.WU</td><td colspan="2">rs1 / addr</td><td colspan="2">PRIVM</td><td colspan="2">rd</td><td colspan="8">SYSTEM</td></tr> <tr> <td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr> </table>	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0										HLVX.WU												rs1 / addr		PRIVM		rd		SYSTEM								0	1	1	0	1	0	0	0	0	0	1	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1					
3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																																	
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																									
HLVX.WU												rs1 / addr		PRIVM		rd		SYSTEM																																																																																																												
0	1	1	0	1	0	0	0	0	0	1	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1																																																																																																
			Valid Base: RV32, RV64, RV128																																																																																																																											
			Task: –																																																																																																																											
			Explanation: See RVP.8.300 through RVP.8.316																																																																																																																											
			Special Case: none																																																																																																																											
			Exception: none																																																																																																																											
RVP.8.294	8.3.1 (p.117) 9.0 (p.138)	R	HSV.B Instruction Encoding: R-Type																																																																																																																											
			<table border="1"> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td colspan="12">HSV.B</td><td colspan="2">rs2 / src</td><td colspan="2">rs1 / addr</td><td colspan="2">PRIVM</td><td colspan="2">0</td><td colspan="8">SYSTEM</td></tr> <tr> <td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr> </table>	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0										HSV.B												rs2 / src		rs1 / addr		PRIVM		0		SYSTEM								0	1	1	0	0	0	1	1	0	0	0	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1	
3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																															
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																									
HSV.B												rs2 / src		rs1 / addr		PRIVM		0		SYSTEM																																																																																																										
0	1	1	0	0	0	1	1	0	0	0	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1																																																																																																
			Valid Base: RV32, RV64, RV128																																																																																																																											
			Task: –																																																																																																																											
			Explanation: See RVP.8.300 through RVP.8.316																																																																																																																											
			Special Case: none																																																																																																																											
			Exception: none																																																																																																																											
RVP.8.295	8.3.1 (p.117) 9.0 (p.138)	R	HSV.H Instruction Encoding: R-Type																																																																																																																											
			<table border="1"> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td colspan="12">HSV.H</td><td colspan="2">rs2 / src</td><td colspan="2">rs1 / addr</td><td colspan="2">PRIVM</td><td colspan="2">0</td><td colspan="8">SYSTEM</td></tr> <tr> <td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr> </table>	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0										HSV.H												rs2 / src		rs1 / addr		PRIVM		0		SYSTEM								0	1	1	0	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1	
3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																														
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																									
HSV.H												rs2 / src		rs1 / addr		PRIVM		0		SYSTEM																																																																																																										
0	1	1	0	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1																																																																																																	
			Valid Base: RV32, RV64, RV128																																																																																																																											
			Task: –																																																																																																																											
			Explanation: See RVP.8.300 through RVP.8.316																																																																																																																											
			Special Case: none																																																																																																																											
			Exception: none																																																																																																																											
RVP.8.296	8.3.1 (p.117) 9.0 (p.138)	R	HSV.W Instruction Encoding: R-Type																																																																																																																											
			<table border="1"> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td colspan="12">HSV.W</td><td colspan="2">rs2 / src</td><td colspan="2">rs1 / addr</td><td colspan="2">PRIVM</td><td colspan="2">0</td><td colspan="8">SYSTEM</td></tr> <tr> <td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr> </table>	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0										HSV.W												rs2 / src		rs1 / addr		PRIVM		0		SYSTEM								0	1	1	0	1	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1
3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																														
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																									
HSV.W												rs2 / src		rs1 / addr		PRIVM		0		SYSTEM																																																																																																										
0	1	1	0	1	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1																																																																																																
			Valid Base: RV32, RV64, RV128																																																																																																																											
			Task: –																																																																																																																											
			Explanation: See RVP.8.300 through RVP.8.316																																																																																																																											
			Special Case: none																																																																																																																											
			Exception: none																																																																																																																											

ID **REFERENCE TYPE DEFINITION**

RVP.8.297	8.3.1 (p.117) 9.0 (p.138)	R	HLV.WU Instruction Encoding: R-Type																																																																																																																												
			<table border="1"> <tr><td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td colspan="12">HLV.WU</td><td colspan="2">rs1 / addr</td><td colspan="2">PRIVM</td><td colspan="2">rd</td><td colspan="8">SYSTEM</td></tr> <tr> <td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td></td><td></td><td></td><td></td><td>1</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr> </table>	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0										HLV.WU												rs1 / addr		PRIVM		rd		SYSTEM								0	1	1	0	1	0	0	0	0	0	0	1					1	0	0							1	1	1	0	0	1	1					
3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																																		
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																										
HLV.WU												rs1 / addr		PRIVM		rd		SYSTEM																																																																																																													
0	1	1	0	1	0	0	0	0	0	0	1					1	0	0							1	1	1	0	0	1	1																																																																																																
			Valid Base: RV64, RV128																																																																																																																												
			Task: –																																																																																																																												
			Explanation: See RVP.8.300 through RVP.8.316																																																																																																																												
			Special Case: none																																																																																																																												
			Exception: none																																																																																																																												
RVP.8.298	8.3.1 (p.117) 9.0 (p.138)	R	HLV.D Instruction Encoding: R-Type																																																																																																																												
			<table border="1"> <tr><td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td colspan="12">HLV.D</td><td colspan="2">rs1 / addr</td><td colspan="2">PRIVM</td><td colspan="2">rd</td><td colspan="8">SYSTEM</td></tr> <tr> <td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td>1</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr> </table>	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0										HLV.D												rs1 / addr		PRIVM		rd		SYSTEM								0	1	1	0	1	1	0	0	0	0	0	0					1	0	0							1	1	1	0	0	1	1			
3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																																
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																										
HLV.D												rs1 / addr		PRIVM		rd		SYSTEM																																																																																																													
0	1	1	0	1	1	0	0	0	0	0	0					1	0	0							1	1	1	0	0	1	1																																																																																																
			Valid Base: RV64, RV128																																																																																																																												
			Task: –																																																																																																																												
			Explanation: See RVP.8.300 through RVP.8.316																																																																																																																												
			Special Case: none																																																																																																																												
			Exception: none																																																																																																																												
RVP.8.299	8.3.1 (p.117) 9.0 (p.138)	R	HSV.D Instruction Encoding: R-Type																																																																																																																												
			<table border="1"> <tr><td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td colspan="12">HSV.D</td><td colspan="2">rs2 / src</td><td colspan="2">rs1 / addr</td><td colspan="2">PRIVM</td><td colspan="2">0</td><td colspan="8">SYSTEM</td></tr> <tr> <td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr> </table>	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0										HSV.D												rs2 / src		rs1 / addr		PRIVM		0		SYSTEM								0	1	1	0	1	1	1										1	0	0							1	1	1	0	0	1	1
3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																															
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																										
HSV.D												rs2 / src		rs1 / addr		PRIVM		0		SYSTEM																																																																																																											
0	1	1	0	1	1	1										1	0	0							1	1	1	0	0	1	1																																																																																																
			Valid Base: RV64, RV128																																																																																																																												
			Task: –																																																																																																																												
			Explanation: See RVP.8.300 through RVP.8.316																																																																																																																												
			Special Case: none																																																																																																																												
			Exception: none																																																																																																																												
RVP.8.300	8.3.1 (p.117)	R	The hypervisor virtual-machine load and store instructions are valid only in M-mode or HS-mode, or in U-mode when <code>hstatus.HU=1</code> .																																																																																																																												
RVP.8.301	8.3.1 (p.117)	R	Each instruction (HLV.* , HLVX.* , HSV.*) performs an explicit memory access as though V=1; i.e., with the address translation and protection, and the endianness, that apply to memory accesses in either VS-mode or VU-mode.																																																																																																																												
RVP.8.302	8.3.1 (p.117)	R	Field SPVP of <code>hstatus</code> controls the privilege level of the access.																																																																																																																												
RVP.8.303	8.3.1 (p.117)	R	The explicit memory access is done as though in VU-mode when SPVP=0, and as though in VS-mode when SPVP=1.																																																																																																																												
RVP.8.304	8.3.1 (p.117)	R	As usual when V=1, two-stage address translation is applied, and the HS-level <code>sstatus.SUM</code> is ignored.																																																																																																																												
RVP.8.305	8.3.1 (p.117)	R	HS-level <code>sstatus.MXR</code> makes execute-only pages readable for both stages of address translation (VS-stage and G-stage), whereas <code>vssstatus.MXR</code> affects only the first translation stage (VS-stage).																																																																																																																												
RVP.8.306	8.3.1 (p.117)	R	For every RV32I or RV64I load instruction, LB, LBU, LH, LHU, LW, LWU, and LD, there is a corresponding virtual-machine load instruction: HLV.B, HLV.BU, HLV.H, HLV.HU, HLV.W, HLV.WU, and HLV.D.																																																																																																																												

ID REFERENCE TYPE DEFINITION

RVP.8.307	8.3.1 (p.117)	R	For every RV32I or RV64I store instruction, SB, SH, SW, and SD, there is a corresponding virtual-machine store instruction: HSV.B, HSV.H, HSV.W, and HSV.D.																																																																																																																									
RVP.8.308	8.3.1 (p.117)	R	Instructions HLV.WU, HLV.D, and HSV.D are not valid for RV32, of course.																																																																																																																									
RVP.8.309	8.3.1 (p.117)	R	Instructions HLVX.HU and HLVX.WU are the same as HLV.HU and HLV.WU, except that execute permission takes the place of read permission during address translation.																																																																																																																									
RVP.8.310	8.3.1 (p.117)	R	That is, the memory being read must be executable in both stages of address translation, but read permission is not required.																																																																																																																									
RVP.8.311	8.3.1 (p.117)	R	For the supervisor physical address that results from address translation, the supervisor physical memory attributes must grant both execute and read permissions.																																																																																																																									
RVP.8.312	8.3.1 (p.117)	I	(<i>The supervisor physical memory attributes</i> are the machine's physical memory attributes as modified by physical memory protection, Section 3.7, for supervisor level.)																																																																																																																									
RVP.8.313	8.3.1 (p.117)	C	HLVX cannot override machine-level physical memory protection (PMP), so attempting to read memory that PMP designates as execute-only still results in an access-fault exception.																																																																																																																									
RVP.8.314	8.3.1 (p.117)	R	HLVX.WU is valid for RV32, even though LWU and HLV.WU are not. (For RV32, HLVX.WU can be considered a variant of HLV.W, as sign extension is irrelevant for 32-bit values.)																																																																																																																									
RVP.8.315	8.3.1 (p.117)	R	Attempts to execute a virtual-machine load/store instruction (HLV, HLVX, or HSV) when V=1 cause a virtual instruction trap.																																																																																																																									
RVP.8.316	8.3.1 (p.117)	R	Attempts to execute one of these same instructions from U-mode when hstatus.HU=0 cause an illegal instruction trap.																																																																																																																									
RVP.8.317	8.3.2 (p.118)	H	Hypervisor Memory-Management Fence Instructions																																																																																																																									
RVP.8.318	8.3.2 (p.118) 9.0 (p.138)	R	HFENCE.VVMA Instruction Encoding: R-Type <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td colspan="4">HFENCE.VVMA</td><td colspan="4">rs2 / asid</td><td colspan="4">rs1 / vaddr</td><td colspan="4">PRIV</td><td colspan="4">0</td><td colspan="4">SYSTEM</td> </tr> <tr> <td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td></td><td></td><td></td> </tr> </table> Valid Base: RV32, RV64, RV128 Task: – Explanation: See RVP.8.320 through RVP.8.341 Special Case: none Exception: none	3	3	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0											HFENCE.VVMA				rs2 / asid				rs1 / vaddr				PRIV				0				SYSTEM				0	0	1	0	0	0	1						0	0	0								1	1	1	0	0	1	1				
3	3	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																													
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																							
HFENCE.VVMA				rs2 / asid				rs1 / vaddr				PRIV				0				SYSTEM																																																																																																								
0	0	1	0	0	0	1						0	0	0								1	1	1	0	0	1	1																																																																																																
RVP.8.319	8.3.2 (p.118) 9.0 (p.138)	R	HFENCE.GVMA Instruction Encoding: R-Type <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>3</td><td>3</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td> </tr> <tr> <td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td colspan="4">HFENCE.GVMA</td><td colspan="4">rs2 / vmid</td><td colspan="4">rs1 / gaddr</td><td colspan="4">PRIV</td><td colspan="4">0</td><td colspan="4">SYSTEM</td> </tr> <tr> <td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td></td><td></td><td></td> </tr> </table> Valid Base: RV32, RV64, RV128 Task: – Explanation: See RVP.8.320 through RVP.8.341 Special Case: none Exception: none	3	3	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0											HFENCE.GVMA				rs2 / vmid				rs1 / gaddr				PRIV				0				SYSTEM				0	1	1	0	0	0	1						0	0	0								1	1	1	0	0	1	1			
3	3	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0																																																																																												
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0																																																																																																							
HFENCE.GVMA				rs2 / vmid				rs1 / gaddr				PRIV				0				SYSTEM																																																																																																								
0	1	1	0	0	0	1						0	0	0								1	1	1	0	0	1	1																																																																																																

ID REFERENCE TYPE DEFINITION

RVP.8.320	8.3.2 (p.118)	R	The hypervisor memory-management fence instructions, HFENCE.VVMA and HFENCE.GVMA, perform a function similar to SFENCE.VMA (Section 4.2.1), except applying to the VS-level memory-management data structures controlled by CSR <code>vsatp</code> (HFENCE.VVMA) or the guest-physical memory-management data structures controlled by CSR <code>hgatp</code> (HFENCE.GVMA).
RVP.8.321	8.3.2 (p.118)	R	Instruction SFENCE.VMA applies only to the memory-management data structures controlled by the current <code>satp</code> (either the HS-level <code>satp</code> when <code>V=0</code> or <code>vsatp</code> when <code>V=1</code>).
RVP.8.322	8.3.2 (p.118)	R	HFENCE.VVMA is valid only in M-mode or HS-mode. Its effect is much the same as temporarily entering VS-mode and executing SFENCE.VMA.
RVP.8.323	8.3.2 (p.118)	R	Executing an HFENCE.VVMA guarantees that any previous stores already visible to the current hart are ordered before all subsequent implicit reads by that hart of the VS-level memory-management data structures, when those implicit reads are for instructions that <ul style="list-style-type: none"> • are subsequent to the HFENCE.VVMA, and • execute when <code>hgatp.VMID</code> has the same setting as it did when HFENCE.VVMA executed.
RVP.8.324	8.3.2 (p.118)	R	Implicit reads need not be ordered when <code>hgatp.VMID</code> is different than at the time HFENCE.VVMA executed.
RVP.8.325	8.3.2 (p.118)	R	If operand <code>rs1</code> \neq x0, it specifies a single guest virtual address, and if operand <code>rs2</code> \neq x0, it specifies a single guest address-space identifier (ASID).
RVP.8.326	8.3.2 (p.118)	C	An HFENCE.VVMA instruction applies only to a single virtual machine, identified by the setting of <code>hgatp.VMID</code> when HFENCE.VVMA executes
RVP.8.327	8.3.2 (p.118)	R	When <code>rs2</code> \neq x0, bits XLEN-1:ASIDMAX of the value held in <code>rs2</code> are reserved for future standard use.
RVP.8.328	8.3.2 (p.118)	R	Until their use is defined by a standard extension, they should be zeroed by software and ignored by current implementations.
RVP.8.329	8.3.2 (p.118)	R	Furthermore, if ASIDLEN < ASIDMAX, the implementation shall ignore bits ASIDMAX-1:ASIDLEN of the value held in <code>rs2</code> .
RVP.8.330	8.3.2 (p.118)	C	Simpler implementations of HFENCE.VVMA can ignore the guest virtual address in <code>rs1</code> and the guest ASID value in <code>rs2</code> , as well as <code>hgatp.VMID</code> , and always perform a global fence for the VS-level memory management of all virtual machines, or even a global fence for all memory management data structures.
RVP.8.331	8.3.2 (p.118)	R	Neither <code>mstatus.TVM</code> nor <code>hstatus.VTVM</code> causes HFENCE.VVMA to trap.
RVP.8.332	8.3.2 (p.118)	R	HFENCE.GVMA is valid only in HS-mode when <code>mstatus.TVM=0</code> , or in M-mode (irrespective of <code>mstatus.TVM</code>).
RVP.8.333	8.3.2 (p.118)	R	Executing an HFENCE.GVMA instruction guarantees that any previous stores already visible to the current hart are ordered before all subsequent implicit reads by that hart of guest-physical memory-management data structures done for instructions that follow the HFENCE.GVMA.
RVP.8.334	8.3.2 (p.118)	R	If operand <code>rs1</code> \neq x0, it specifies a single guest physical address, shifted right by 2 bits, and if operand <code>rs2</code> \neq x0, it specifies a single virtual machine identifier (VMID).

ID REFERENCE TYPE DEFINITION

- RVP.8.335 8.3.2 (p.119) C Like for a guest physical address written to htval on a trap, a guest physical address specified in *rs1* is shifted right by 2 bits to accommodate addresses wider than the current XLEN.
- RVP.8.336 8.3.2 (p.119) R When *rs2*≠*x0*, bits XLEN-1:VMIDMAX of the value held in *rs2* are reserved for future standard use. Until their use is defined by a standard extension, they should be zeroed by software and ignored by current implementations.
- RVP.8.337 8.3.2 (p.119) R Furthermore, if VMIDLEN < VMIDMAX, the implementation shall ignore bits VMIDMAX-1:VMIDLEN of the value held in *rs2*.
- RVP.8.338 8.3.2 (p.119) C Simpler implementations of HFENCE.GVMA can ignore the guest physical address in *rs1* and the VMID value in *rs2* and always perform a global fence for the guest-physical memory management of all virtual machines, or even a global fence for all memory-management data structures.
- RVP.8.339 8.3.2 (p.119) R If hgatp.MODE is changed for a given VMID, an HFENCE.GVMA with *rs1*=*x0* (and *rs2* set to either *x0* or the VMID) must be executed to order subsequent guest translations with the MODE change—even if the old MODE or new MODE is Bare.
- RVP.8.340 8.3.2 (p.119) R Attempts to execute HFENCE.VVMA or HFENCE.GVMA when V=1 cause a virtual instruction trap, while attempts to do the same in U-mode cause an illegal instruction trap.
- RVP.8.341 8.3.2 (p.119) R Attempting to execute HFENCE.GVMA in HS-mode when mstatus.TVM=1 also causes an illegal instruction trap.
- RVP.8.342 8.4 (p.119) H Machine-Level CSRs
- RVP.8.343 8.4 (p.119) I The hypervisor extension augments or modifies machine CSRs mstatus, mstatusush, mideleg, mip, and mie, and adds CSRs mtval2 and mtinst.
- RVP.8.344 8.4.1 (p.119) H Machine Status Registers (mstatus and mstatusush)
- RVP.8.345 8.4.1 (p.119) R The hypervisor extension adds two fields, MPV and GVA, to the machine-level mstatus or mstatusush CSR, and modifies the behavior of several existing mstatus fields.
- RVP.8.346 8.4.1 (p.119)
Figure 8.34 R The modified mstatus (machine status) register when the hypervisor extension is implemented and MXLEN=64.

MXLEN-1	MXLEN-2	...	40	39	38	37	36	35	34	33	32
SD	WPRI		MPV	GVA	MBE	SBE	SXL		UXL		

31	...	23	22	21	20	19	18	17	16	15	14	13
WPRI	TSR	TW	TVM	MXR	SUM	MPRV	XS	FS				

12	11	10	9	8	7	6	5	4	3	2	1	0
MPP	VS	SPP	MPIE	UBE	SPIE	WPRI	MIE	WPRI	SIE	WPRI		

- RVP.8.347 8.4.1 (p.119) R When MXLEN=32, the hypervisor extension adds MPV and GVA not to mstatus but to mstatusush.

ID REFERENCE TYPE DEFINITION

- RVP.8.348 8.4.1 (p.119) R the `mstatus` register when the hypervisor extension is implemented and `MXLEN=32`. The format of `mstatus` is unchanged for RV32.
- | | | | | | | | | | |
|------|-----|---|-----|-----|-----|-----|------|-----|---|
| 31 | ... | 8 | 7 | 6 | 5 | 4 | 3 | ... | 0 |
| WPRI | | | MPV | GVA | MBE | SBE | WPRI | | |
- RVP.8.349 8.4.1 (p.119) R The MPV bit (Machine Previous Virtualization Mode) is written by the implementation whenever a trap is taken into M-mode.
- RVP.8.350 8.4.1 (p.119) R Just as the MPP field is set to the (nominal) privilege mode at the time of the trap, the MPV bit is set to the value of the virtualization mode V at the time of the trap.
- RVP.8.351 8.4.1 (p.119) R When an MRET instruction is executed, the virtualization mode V is set to MPV, unless MPP=3, in which case V remains 0.
- RVP.8.352 8.4.1 (p.119) R Field GVA (Guest Virtual Address) is written by the implementation whenever a trap is taken into M-mode.
- RVP.8.353 8.4.1 (p.119) R For any trap (breakpoint, address misaligned, access fault, page fault, or guest-page fault) that writes a guest virtual address to `mtval`, GVA is set to 1.
- RVP.8.354 8.4.1 (p.119) R For any other trap into M-mode, GVA is set to 0.
- RVP.8.355 8.4.1 (p.120) R The TSR and TVM fields of `mstatus` affect execution only in HS-mode, not in VS-mode.
- RVP.8.356 8.4.1 (p.120) R The TW field affects execution in all modes except M-mode.
- RVP.8.357 8.4.1 (p.120) R Setting TVM=1 prevents HS-mode from accessing `hgatp` or executing HFENCE.GVMA or HINVAL.GVMA, but has no effect on accesses to `vsatp` or instructions HFENCE.VVMA or HINVAL.VVMA.
- RVP.8.358 8.4.1 (p.120) C TVM exists in `mstatus` to allow machine-level software to modify the address translations managed by a supervisor-level OS, usually for the purpose of inserting another stage of address translation below that controlled by the OS. The instruction traps enabled by TVM=1 permit machine level to co-opt both `satp` and `hgatp` and substitute shadow page tables that merge the OS's chosen page translations with M-level's lower-stage translations, all without the OS being aware. M-level software needs this ability not only to emulate the hypervisor extension if not already supported, but also to emulate any future RISC-V extensions that may modify or add address translation stages, perhaps, for example, to improve support for nested hypervisors, i.e., running hypervisors atop other hypervisors.
- RVP.8.359 8.4.1 (p.120) C However, setting TVM=1 does not cause traps for accesses to `vsatp` or instructions HFENCE.VVMA or HINVAL.VVMA, or for any actions taken in VS-mode, because M-level software is not expected to need to involve itself in VS-stage address translation. For virtual machines, it should be sufficient, and in all likelihood faster as well, to leave VS-stage address translation alone and merge all other translation stages into G-stage shadow page tables controlled by `hgatp`. This assumption does place some constraints on possible future RISC-V extensions that current machines will be able to emulate efficiently.
- RVP.8.360 8.4.1 (p.120) R The hypervisor extension changes the behavior of the Modify Privilege field, MPRV, of `mstatus`.
- RVP.8.361 8.4.1 (p.120) R When MPRV=0, translation and protection behave as normal.

ID REFERENCE TYPE DEFINITION

RVP.8.362	8.4.1 (p.120, p.121)	R	When MPRV=1, explicit memory accesses are translated and protected, and endianness is applied, as though the current virtualization mode were set to MPV and the current nominal privilege mode were set to MPP.																												
RVP.8.363	8.4.1 (p.121) Table 8.5	R	Effect of MPRV on the translation and protection of explicit memory accesses.																												
			<table border="1"> <thead> <tr> <th>MPRV</th><th>MPV</th><th>MPP</th><th>Effect</th></tr> </thead> <tbody> <tr> <td>0</td><td>-</td><td>-</td><td>Normal access; current privilege mode applies.</td></tr> <tr> <td>1</td><td>0</td><td>0</td><td>U-level access with HS-level translation and protection only</td></tr> <tr> <td>1</td><td>0</td><td>1</td><td>HS-level access with HS-level translation and protection only.</td></tr> <tr> <td>1</td><td>-</td><td>3</td><td>M-level access with no translation</td></tr> <tr> <td>1</td><td>1</td><td>0</td><td>VU-level access with two-stage translation and protection. The Hslevel MXR bit makes any executable page readable. <code>vsstatus.MXR</code> makes readable those pages marked executable at the VS translation stage, but only if readable at the guest-physical translation stage.</td></tr> <tr> <td>1</td><td>1</td><td>1</td><td>VS-level access with two-stage translation and protection. The Hslevel MXR bit makes any executable page readable. <code>vsstatus.MXR</code> makes readable those pages marked executable at the VS translation stage, but only if readable at the guest-physical translation stage. <code>vsstatus.SUM</code> applies instead of the HS-level SUM bit.</td></tr> </tbody> </table>	MPRV	MPV	MPP	Effect	0	-	-	Normal access; current privilege mode applies.	1	0	0	U-level access with HS-level translation and protection only	1	0	1	HS-level access with HS-level translation and protection only.	1	-	3	M-level access with no translation	1	1	0	VU-level access with two-stage translation and protection. The Hslevel MXR bit makes any executable page readable. <code>vsstatus.MXR</code> makes readable those pages marked executable at the VS translation stage, but only if readable at the guest-physical translation stage.	1	1	1	VS-level access with two-stage translation and protection. The Hslevel MXR bit makes any executable page readable. <code>vsstatus.MXR</code> makes readable those pages marked executable at the VS translation stage, but only if readable at the guest-physical translation stage. <code>vsstatus.SUM</code> applies instead of the HS-level SUM bit.
MPRV	MPV	MPP	Effect																												
0	-	-	Normal access; current privilege mode applies.																												
1	0	0	U-level access with HS-level translation and protection only																												
1	0	1	HS-level access with HS-level translation and protection only.																												
1	-	3	M-level access with no translation																												
1	1	0	VU-level access with two-stage translation and protection. The Hslevel MXR bit makes any executable page readable. <code>vsstatus.MXR</code> makes readable those pages marked executable at the VS translation stage, but only if readable at the guest-physical translation stage.																												
1	1	1	VS-level access with two-stage translation and protection. The Hslevel MXR bit makes any executable page readable. <code>vsstatus.MXR</code> makes readable those pages marked executable at the VS translation stage, but only if readable at the guest-physical translation stage. <code>vsstatus.SUM</code> applies instead of the HS-level SUM bit.																												
RVP.8.364	8.4.1 (p.121)	R	MPRV does not affect the virtual-machine load/store instructions, HLV, HLVX, and HSV.																												
RVP.8.365	8.4.1 (p.121)	R	The explicit loads and stores of these instructions always act as though V=1 and the nominal privilege mode were <code>hstatus.SPVP</code> , overriding MPRV.																												
RVP.8.366	8.4.1 (p.121)	R	The <code>mstatus</code> register is a superset of the HS-level <code>sstatus</code> register but is not a superset of <code>vsstatus</code> .																												
RVP.8.367	8.4.2 (p.121)	H	Machine Interrupt Delegation Register (<code>mideleg</code>)																												
RVP.8.368	8.4.2 (p.121)	R	When the hypervisor extension is implemented, bits 10, 6, and 2 of <code>mideleg</code> (corresponding to the standard VS-level interrupts) are each read-only one.																												
RVP.8.369	8.4.2 (p.121)	R	Furthermore, if any guest external interrupts are implemented (GEILEN is nonzero), bit 12 of <code>mideleg</code> (corresponding to supervisor-level guest external interrupts) is also read-only one.																												
RVP.8.370	8.4.2 (p.121)	R	VS-level interrupts and guest external interrupts are always delegated past M-mode to HS-mode.																												
RVP.8.371	8.4.2 (p.121)	R	For bits of <code>mideleg</code> that are zero, the corresponding bits in <code>hideleg</code> , <code>hip</code> , and <code>hie</code> are read-only zeros.																												
RVP.8.372	8.4.3 (p.121)	H	Machine Interrupt Registers (<code>mip</code> and <code>mie</code>)																												
RVP.8.373	8.4.3 (p.121)	R	The hypervisor extension gives registers <code>mip</code> and <code>mie</code> additional active bits for the hypervisor-added interrupts.																												

ID REFERENCE TYPE DEFINITION

RVP.8.374	8.4.3 (p.122)	R	Standard portion (bits 15:0) of <code>mip</code> when the hypervisor extension is implemented:																															
	Figure 8.36																																	
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>15</td><td>...</td><td>13</td><td>12</td><td>11</td><td>10</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr> <td>0</td><td></td><td>SGEIP</td><td>MEIP</td><td>VSEIP</td><td>SEIP</td><td>0</td><td>MTIP</td><td>VSTIP</td><td>STIP</td><td>0</td><td>MSIP</td><td>VSSIP</td><td>SSIP</td><td>0</td></tr> </table>	15	...	13	12	11	10	9	8	7	6	5	4	3	2	1	0	0		SGEIP	MEIP	VSEIP	SEIP	0	MTIP	VSTIP	STIP	0	MSIP	VSSIP	SSIP	0
15	...	13	12	11	10	9	8	7	6	5	4	3	2	1	0																			
0		SGEIP	MEIP	VSEIP	SEIP	0	MTIP	VSTIP	STIP	0	MSIP	VSSIP	SSIP	0																				
RVP.8.375	8.4.3 (p.122)	R	Standard portion (bits 15:0) of <code>mie</code> when the hypervisor extension is implemented:																															
	Figure 8.37																																	
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>15</td><td>...</td><td>13</td><td>12</td><td>11</td><td>10</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr> <tr> <td>0</td><td></td><td>SGEIE</td><td>MEIE</td><td>VSEIE</td><td>SEIE</td><td>0</td><td>MTIE</td><td>VSTIE</td><td>STIE</td><td>0</td><td>MSIE</td><td>VSSIE</td><td>SSIE</td><td>0</td></tr> </table>	15	...	13	12	11	10	9	8	7	6	5	4	3	2	1	0	0		SGEIE	MEIE	VSEIE	SEIE	0	MTIE	VSTIE	STIE	0	MSIE	VSSIE	SSIE	0
15	...	13	12	11	10	9	8	7	6	5	4	3	2	1	0																			
0		SGEIE	MEIE	VSEIE	SEIE	0	MTIE	VSTIE	STIE	0	MSIE	VSSIE	SSIE	0																				
RVP.8.376	8.4.3 (p.121)	R	Bits SGEIP, VSEIP, VSTIP, and VSSIP in <code>mip</code> are aliases for the same bits in hypervisor CSR <code>hip</code> , while SGEIE, VSEIE, VSTIE, and VSSIE in <code>mie</code> are aliases for the same bits in <code>hie</code> .																															
RVP.8.377	8.4.4 (p.122)	H	Machine Second Trap Value Register (<code>mtval2</code>)																															
RVP.8.378	8.4.4 (p.122)	R	The <code>mtval2</code> register is an MXLEN-bit read/write register.																															
RVP.8.379	8.4.4 (p.122)	R	Machine second trap value register (<code>mtval2</code>).																															
	Figure 8.38																																	
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>MXLEN-1</td><td>...</td><td>0</td></tr> <tr> <td colspan="2">mtval2</td><td></td></tr> </table>	MXLEN-1	...	0	mtval2																											
MXLEN-1	...	0																																
mtval2																																		
RVP.8.380	8.4.4 (p.122)	R	When a trap is taken into M-mode, <code>mtval2</code> is written with additional exception-specific information, alongside <code>mtval</code> , to assist software in handling the trap.																															
RVP.8.381	8.4.4 (p.122)	R	When a guest-page-fault trap is taken into M-mode, <code>mtval2</code> is written with either zero or the guest physical address that faulted, shifted right by 2 bits.																															
RVP.8.382	8.4.4 (p.122)	R	For other traps, <code>mtval2</code> is set to zero, but a future standard or extension may redefine <code>mtval2</code> 's setting for other traps.																															
RVP.8.383	8.4.4 (p.122)	R	If a guest-page fault is due to an implicit memory access during first-stage (VS-stage) address translation, a guest physical address written to <code>mtval2</code> is that of the implicit memory access that faulted.																															
RVP.8.384	8.4.4 (p.122)	R	Additional information is provided in CSR <code>mtinst</code> to disambiguate such situations.																															
RVP.8.385	8.4.4 (p.122)	R	Otherwise, for misaligned loads and stores that cause guest-page faults, a nonzero guest physical address in <code>mtval2</code> corresponds to the faulting portion of the access as indicated by the virtual address in <code>mtval</code> .																															
RVP.8.386	8.4.4 (p.122)	R	For instruction guest-page faults on systems with variable-length instructions, a nonzero <code>mtval2</code> corresponds to the faulting portion of the instruction as indicated by the virtual address in <code>mtval</code> .																															
RVP.8.387	8.4.4 (p.122)	R	<code>mtval2</code> is a WARL register that must be able to hold zero and may be capable of holding only an arbitrary subset of other 2-bit-shifted guest physical addresses, if any.																															
RVP.8.388	8.4.5 (p.122)	H	Machine Trap Instruction Register (<code>mtinst</code>)																															
RVP.8.389	8.4.5 (p.122)	R	The <code>mtinst</code> register is an MXLEN-bit read/write register.																															

ID	REFERENCE	TYPE	DEFINITION
RVP.8.390	8.4.5 (p.122) Figure 8.39	R	Machine trap instruction register (<code>mtinst</code>). <pre> MXLEN-1 ... mtinst +-----+-----+ 4 bits 48 bits </pre>
RVP.8.391	8.4.5 (p.122)	R	When a trap is taken into M-mode, <code>mtinst</code> is written with a value that, if nonzero, provides information about the instruction that trapped, to assist software in handling the trap.
RVP.8.392	8.4.5 (p.122)	R	The values that may be written to <code>mtinst</code> on a trap are documented in Section 8.6.3.
RVP.8.393	8.4.5 (p.123)	R	<code>mtinst</code> is a WARL register that need only be able to hold the values that the implementation may automatically write to it on a trap.
RVP.8.394	8.5 (p.123)	H	Two-Stage Address Translation
RVP.8.395	8.5 (p.123)	R	Whenever the current virtualization mode <code>V</code> is 1, two-stage address translation and protection is in effect.
RVP.8.396	8.5 (p.123)	R	For any virtual memory access, the original virtual address is converted in the first stage by VS-level address translation, as controlled by the <code>vsatp</code> register, into a guest physical address.
RVP.8.397	8.5 (p.123)	R	The guest physical address is then converted in the second stage by guest physical address translation, as controlled by the <code>hgatp</code> register, into a supervisor physical address.
RVP.8.398	8.5 (p.123)	I	The two stages are known also as VS-stage and G-stage translation.
RVP.8.399	8.5 (p.123)	R	Although there is no option to disable twostage address translation when <code>V=1</code> , either stage of translation can be effectively disabled by zeroing the corresponding <code>vsatp</code> or <code>hgatp</code> register.
RVP.8.400	8.5 (p.123)	R	The <code>vsstatus</code> field MXR, which makes execute-only pages readable, only overrides VS-stage page protection.
RVP.8.401	8.5 (p.123)	R	Setting MXR at VS-level does not override guest-physical page protections.
RVP.8.402	8.5 (p.123)	R	Setting MXR at HS-level, however, overrides both VS-stage and G-stage execute-only permissions.
RVP.8.403	8.5 (p.123)	R	When <code>V=1</code> , memory accesses that would normally bypass address translation are subject to G-stage address translation alone.
RVP.8.404	8.5 (p.123)	R	This includes memory accesses made in support of VS-stage address translation, such as reads and writes of VS-level page tables.
RVP.8.405	8.5 (p.123)	R	Machine-level physical memory protection applies to supervisor physical addresses and is in effect regardless of virtualization mode.
RVP.8.406	8.5.1 (p.123)	H	Guest Physical Address Translation
RVP.8.407	8.5.1 (p.123)	R	The mapping of guest physical addresses to supervisor physical addresses is controlled by CSR <code>hgatp</code> (Section 8.2.10).
RVP.8.408	8.5.1 (p.123)	R	When the address translation scheme selected by the MODE field of <code>hgatp</code> is Bare, guest physical addresses are equal to supervisor physical addresses without modification, and no memory protection applies in the trivial translation of guest physical addresses to supervisor physical addresses.

ID REFERENCE TYPE DEFINITION

- RVP.8.409 8.5.1 (p.123) R When `hgatp.MODE` specifies a translation scheme of Sv32x4, Sv39x4, Sv48x4, or Sv57x4, G-stage address translation is a variation on the usual page-based virtual address translation scheme of Sv32, Sv39, Sv48, or Sv57, respectively.
- RVP.8.410 8.5.1 (p.123) R In each case, the size of the incoming address is widened by 2 bits (to 34, 41, or 50 bits).
- RVP.8.411 8.5.1 (p.123) R To accommodate the 2 extra bits, the root page table (only) is expanded by a factor of four to be 16 KiB instead of the usual 4 KiB.
- RVP.8.412 8.5.1 (p.123) R Matching its larger size, the root page table also must be aligned to a 16 KiB boundary instead of the usual 4 KiB page boundary
- RVP.8.413 8.5.1 (p.124) R Except as noted, all other aspects of Sv32, Sv39, Sv48, or Sv57 are adopted unchanged for G-stage translation.
- RVP.8.414 8.5.1 (p.124) R Non-root page tables and all page table entries (PTEs) have the same formats as documented in Sections 4.3, 4.4, 4.5, and 4.6.
- RVP.8.415 8.5.1 (p.124) R For Sv32x4, an incoming guest physical address is partitioned into a virtual page number (VPN) and page offset as shown below
- | | | | | | | | | |
|--------|-----|----|----|--------|----|----|-------------|---|
| 33 | ... | 22 | 21 | ... | 12 | 11 | ... | 0 |
| VPN[1] | | | | VPN[0] | | | Page offset | |
- RVP.8.416 8.5.1 (p.124) I This partitioning is identical to that for an Sv32 virtual address (page 79), except with 2 more bits at the high end in VPN[1].
- RVP.8.417 8.5.1 (p.124) I Note that the fields of a partitioned guest physical address also correspond one-for-one with the structure that Sv32 assigns to a physical address, depicted in RVP.4.228)
- RVP.8.418 8.5.1 (p.124) R For Sv39x4, an incoming guest physical address is partitioned as shown below
- | | | | | | | | | | | |
|--------|----|----|-----|--------|----|-----|--------|----|-----|-------------|
| 40 | 30 | 29 | ... | 21 | 20 | ... | 12 | 11 | ... | 0 |
| VPN[2] | | | | VPN[1] | | | VPN[0] | | | Page offset |
- RVP.8.419 8.5.1 (p.124) R This partitioning is identical to that for an Sv39 virtual address as depicted in RVP.4.290, except with 2 more bits at the high end in VPN[2].
- RVP.8.420 8.5.1 (p.124) R Address bits 63:41 must all be zeros, or else a guest-page-fault exception occurs.
- RVP.8.421 8.5.1 (p.124) R For Sv48x4, an incoming guest physical address is partitioned as shown below
- | | | | | | | | | | | | | | | |
|--------|-----|----|----|--------|----|----|--------|----|----|--------|----|----|-------------|---|
| 49 | ... | 39 | 38 | ... | 30 | 29 | ... | 21 | 20 | ... | 12 | 11 | ... | 0 |
| VPN[3] | | | | VPN[2] | | | VPN[1] | | | VPN[0] | | | Page offset | |
- RVP.8.422 8.5.1 (p.124) I This partitioning is identical to that for an Sv48 virtual address as depicted in RVP.4.314, except with 2 more bits at the high end in VPN[3].
- RVP.8.423 8.5.1 (p.124) R Address bits 63:50 must all be zeros, or else a guest-page-fault exception occurs.

ID REFERENCE TYPE DEFINITION

RVP.8.424	8.5.1 (p.124)	R	For Sv57x4, an incoming guest physical address is partitioned as shown below																																				
			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>58</td><td>...</td><td>50</td><td>49</td><td>...</td><td>39</td><td>38</td><td>...</td><td>30</td><td>29</td><td>...</td><td>21</td><td>20</td><td>...</td><td>12</td><td>11</td><td>...</td><td>0</td></tr> <tr> <td>VPN[4]</td><td></td><td>VPN[3]</td><td></td><td>VPN[2]</td><td></td><td>VPN[1]</td><td></td><td>VPN[0]</td><td></td><td>Page offset</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table>	58	...	50	49	...	39	38	...	30	29	...	21	20	...	12	11	...	0	VPN[4]		VPN[3]		VPN[2]		VPN[1]		VPN[0]		Page offset							
58	...	50	49	...	39	38	...	30	29	...	21	20	...	12	11	...	0																						
VPN[4]		VPN[3]		VPN[2]		VPN[1]		VPN[0]		Page offset																													
RVP.8.425	8.5.1 (p.124)	I	This partitioning is identical to that for an Sv57 virtual address as depicted in RVP.4.330, except with 2 more bits at the high end in VPN[3].																																				
RVP.8.426	8.5.1 (p.124)	R	Address bits 63:50 [†] must all be zeros, or else a guest-page-fault exception occurs.																																				
RVP.8.427	8.5.1 (p.124, p.125)	C	The page-based G-stage address translation scheme for RV32, Sv32x4, is defined to support a 34-bit guest physical address so that an RV32 hypervisor need not be limited in its ability to virtualize real 32-bit RISC-V machines, even those with 33-bit or 34-bit physical addresses. This may include the possibility of a machine virtualizing itself, if it happens to use 33-bit or 34-bit physical addresses. Multiplying the size and alignment of the root page table by a factor of four is the cheapest way to extend Sv32 to cover a 34-bit address. The possible wastage of 12 KiB for an unnecessarily large root page table is expected to be of negligible consequence for most (maybe all) real uses.																																				
RVP.8.428	8.5.1 (p.125)	C	A consistent ability to virtualize machines having as much as four times the physical address space as virtual address space is believed to be of some utility also for RV64. For a machine implementing 39-bit virtual addresses (Sv39), for example, this allows the hypervisor extension to support up to a 41-bit guest physical address space without either necessitating hardware support for 48-bit virtual addresses (Sv48) or falling back to emulating the larger address space using shadow page tables.																																				
RVP.8.429	8.5.1 (p.125)	R	The conversion of an Sv32x4, Sv39x4, Sv48x4, or Sv57x4 guest physical address is accomplished with the same algorithm used for Sv32, Sv39, Sv48, or Sv57, as presented in Section 4.3.2, except that: <ul style="list-style-type: none"> • <code>hgatp</code> substitutes for the usual <code>satp</code>; • for the translation to begin, the effective privilege mode must be VS-mode or VU-mode; • when checking the U bit, the current privilege mode is always taken to be U-mode; and • guest-page-fault exceptions are raised instead of regular page-fault exceptions. 																																				
RVP.8.430	8.5.1 (p.125)	R	For G-stage address translation, all memory accesses (including those made to access data structures for VS-stage address translation) are considered to be user-level accesses, as though executed in U-mode.																																				
RVP.8.431	8.5.1 (p.125)	R	Access type permissions—readable, writable, or executable—are checked during G-stage translation the same as for VS-stage translation.																																				
RVP.8.432	8.5.1 (p.125)	R	For a memory access made to support VS-stage address translation (such as to read/write a VS-level page table), permissions are checked as though for a load or store, not for the original access type.																																				
RVP.8.433	8.5.1 (p.125)	R	However, any exception is always reported for the original access type (instruction, load, or store/AMO).																																				
RVP.8.434	8.5.1 (p.125)	R	The G bit in all G-stage PTEs is reserved for future standard use.																																				

[†] Probably a mistyping? My expectation is 63:59 bits.

ID	REFERENCE	TYPE	DEFINITION
RVP.8.435	8.5.1 (p.125)	R	Until its use is defined by a standard extension, it should be cleared by software for forward compatibility, and must be ignored by hardware.
RVP.8.436	8.5.1 (p.125)	C	G-stage address translation uses the identical format for PTEs as regular address translation, even including the U bit, due to the possibility of sharing some (or all) page tables between G-stage translation and regular HS-level address translation. Regardless of whether this usage will ever become common, we chose not to preclude it.
RVP.8.437	8.5.2 (p.125)	H	Guest-Page Faults
RVP.8.438	8.5.2 (p.125)	R	Guest-page-fault traps may be delegated from M-mode to HS-mode under the control of CSR medeleg, but cannot be delegated to other privilege modes.
RVP.8.439	8.5.2 (p.125)	R	On a guest-page fault, CSR mtval or stval is written with the faulting guest virtual address as usual, and mtval2 or htval is written either with zero or with the faulting guest physical address, shifted right by 2 bits.
RVP.8.440	8.5.2 (p.125)	R	CSR mtinst or htinst may also be written with information about the faulting instruction or other reason for the access, as explained in Section 8.6.3.
RVP.8.441	8.5.2 (p.126)	R	When an instruction fetch or a misaligned memory access straddles a page boundary, two different address translations are involved.
RVP.8.442	8.5.2 (p.126)	R	When a guest-page fault occurs in such a circumstance, the faulting virtual address written to mtval/stval is the same as would be required for a regular page fault.
RVP.8.443	8.5.2 (p.126)	R	Thus, the faulting virtual address may be a page-boundary address that is higher than the instruction's original virtual address, if the byte at that page boundary is among the accessed bytes.
RVP.8.444	8.5.2 (p.126)	R	When a guest-page fault is not due to an implicit memory access for VS-stage address translation, a nonzero guest physical address written to mtval2/htval shall correspond to the exact virtual address written to mtval/stval.
RVP.8.445	8.5.3 (p.126)	H	Memory-Management Fences
RVP.8.446	8.5.3 (p.126)	R	The behavior of the SFENCE.VMA instruction is affected by the current virtualization mode V.
RVP.8.447	8.5.3 (p.126)	R	When V=0, the virtual-address argument is an HS-level virtual address, and the ASID argument is an HS-level ASID.
RVP.8.448	8.5.3 (p.126)	R	The instruction orders stores only to HS-level address-translation structures with subsequent HS-level address translations.
RVP.8.449	8.5.3 (p.126)	R	When V=1, the virtual-address argument to SFENCE.VMA is a guest virtual address within the current virtual machine, and the ASID argument is a VS-level ASID within the current virtual machine.
RVP.8.450	8.5.3 (p.126)	R	The current virtual machine is identified by the VMID field of CSR hgatp, and the effective ASID can be considered to be the combination of this VMID with the VS-level ASID.
RVP.8.451	8.5.3 (p.126)	R	The SFENCE.VMA instruction orders stores only to the VS-level address-translation structures with subsequent VS-stage address translations for the same virtual machine, i.e., only when hgatp.VMID is the same as when the SFENCE.VMA executed.

ID	REFERENCE	TYPE	DEFINITION
RVP.8.452	8.5.3 (p.126)	R	Hypervisor instructions HFENCE.VVMA and HFENCE.GVMA provide additional memory-management fences to complement SFENCE.VMA. These instructions are described in Section 8.3.2.
RVP.8.453	8.5.3 (p.126)	R	Section 3.7.2 discusses the intersection between physical memory protection (PMP) and page-based address translation.
RVP.8.454	8.5.3 (p.126)	R	It is noted there that, when PMP settings are modified in a manner that affects either the physical memory that holds page tables or the physical memory to which page tables point, M-mode software must synchronize the PMP settings with the virtual memory system.
RVP.8.455	8.5.3 (p.126)	R	For HS-level address translation, this is accomplished by executing in M-mode an SFENCE.VMA instruction with $rs1=x0$ and $rs2=x0$, after the PMP CSRs are written.
RVP.8.456	8.5.3 (p.126)	R	If G-stage address translation is in use and is not Bare, synchronization with its data structures is also needed.
RVP.8.457	8.5.3 (p.126)	R	When PMP settings are modified in a manner that affects either the physical memory that holds guest-physical page tables or the physical memory to which guest-physical page tables point, an HFENCE.GVMA instruction with $rs1=x0$ and $rs2=x0$ must be executed in M-mode after the PMP CSRs are written. An HFENCE.VVMA instruction is not required.
RVP.8.458	8.6 (p.127)	H	Traps
RVP.8.459	8.6.1 (p.127)	H	Trap Cause Codes
RVP.8.460	8.6.1 (p.127)	I	The hypervisor extension augments the trap cause encoding.
RVP.8.461	8.6.1 (p.127)	I	Codes are added for VS-level interrupts (interrupts 2, 6, 10), for supervisor-level guest external interrupts (interrupt 12), for virtual instruction exceptions (exception 22), and for guest-page faults (exceptions 20, 21, 23).
RVP.8.462	8.6.1 (p.127)	R	Furthermore, environment calls from VS-mode are assigned cause 10, whereas those from HS-mode or S-mode use cause 9 as usual.
RVP.8.463	8.6.1 (p.127)	C	HS-mode and VS-mode ECALLs use different cause values so they can be delegated separately.

ID REFERENCE TYPE DEFINITION

RVP.8.464 8.6.1 (p.127) R
Table 8.6 The table below lists the possible M-mode and HS-mode trap cause codes (Machine and supervisor cause register (`mcause` and `scause`) values) when the hypervisor extension is implemented.

Interrupt	Exception Code	Description
1	0	Reserved
1	1	Supervisor software interrupt
1	2	Virtual supervisor software interrupt
1	3	Machine software interrupt
1	4	Reserved
1	5	Supervisor timer interrupt
1	6	Virtual supervisor timer interrupt
1	7	Machine timer interrupt
1	8	Reserved
1	9	Supervisor external interrupt
1	10	Virtual supervisor external interrupt
1	11	Machine external interrupt
1	12	Supervisor guest external interrupt
1	13 - 15	Reserved
1	≥ 16	Designated for platform or custom use
0	0	Instruction address misaligned
0	1	Instruction access fault
0	2	Illegal instruction
0	3	Breakpoint
0	4	Load address misaligned
0	5	Load access fault
0	6	Store/AMO address misaligned
0	7	Store/AMO access fault
0	8	Environment call from U-mode or VU-mode
0	9	Environment call from HS-mode
0	10	Environment call from VS-mode
0	11	Environment call from M-mode
0	12	Instruction page fault
0	13	Load page fault
0	14	Reserved
0	15	Store/AMO page fault
0	16 - 19	Reserved
0	20	Instruction guest-page fault
0	21	Load guest-page fault
0	22	Virtual instruction
0	23	Store/AMO guest-page fault
0	24 - 31	Designated for custom use
0	32 - 47	Reserved
0	48 - 63	Designated for custom use
0	≥ 64	Reserved

RVP.8.465 8.6.1 (p.127) R When $V=1$, a virtual instruction exception (code 22) is normally raised instead of an illegal instruction exception if the attempted instruction is *HS-qualified* but is prevented from executing when $V=1$ either due to insufficient privilege or because the instruction is expressly disabled by a supervisor or hypervisor CSR such as `scounteren` or `hcounteren`.

ID REFERENCE TYPE DEFINITION

RVP.8.466	8.6.1 (p.127)	R	An instruction is <i>HS-qualified</i> if it would be valid to execute in HS-mode (for some values of the instruction's register operands), assuming fields TSR and TVM of CSR mstatus are both zero.
RVP.8.467	8.6.1 (p.127)	R	Special rules apply for CSR instructions that access 32-bit high-half CSRs such as <code>cycleh</code> and <code>htimedeltah</code> .
RVP.8.468	8.6.1 (p.127)	R	When V=1 and XLEN>32, an attempt to access a high-half supervisor-level CSR, high-half hypervisor CSR, high-half VS CSR, or high-half unprivileged CSR always raises an illegal instruction exception.
RVP.8.469	8.6.1 (p.127)	R	And in VS-mode, if the XLEN for VU-mode is greater than 32, an attempt to access a high-half user-level CSR (distinct from an unprivileged CSR) always raises an illegal instruction exception.
RVP.8.470	8.6.1 (p.127)	R	On the other hand, when V=1 and XLEN=32, an invalid attempt to access a high-half S-level, hypervisor, VS, or unprivileged CSR raises a virtual instruction exception instead of an illegal instruction exception if the same CSR instruction for the partner low-half CSR (e.g. <code>cycle</code> or <code>htimedelta</code>) is HS-qualified.
RVP.8.471	8.6.1 (p.127)	R	Likewise, in VS-mode, if the XLEN for VU-mode is 32, an invalid attempt to access a high-half user-level CSR raises a virtual instruction exception instead of an illegal instruction exception if the same CSR instruction for the partner low-half CSR is HS-qualified.
RVP.8.472	8.6.1 (p.127)	C	The RISC-V Privileged Architecture currently defines no user-level CSRs, but they might be added by a future version of this standard or by an extension.

ID REFERENCE TYPE DEFINITION

RVP.8.473	8.6.1 (p.127, p.129)	R	<p>Specifically, a virtual instruction exception is raised for the following cases:</p> <ul style="list-style-type: none"> • in VS-mode, attempts to access a non-high-half counter CSR when the corresponding bit in <code>hcounteren</code> is 0 and the same bit in <code>mcounteren</code> is 1; • in VS-mode, if $XLEN=32$, attempts to access a high-half counter CSR when the corresponding bit in <code>hcounteren</code> is 0 and the same bit in <code>mcounteren</code> is 1; • in VU-mode, attempts to access a non-high-half counter CSR when the corresponding bit in either <code>hcounteren</code> or <code>scounteren</code> is 0 and the same bit in <code>mcounteren</code> is 1; • in VU-mode, if $XLEN=32$, attempts to access a high-half counter CSR when the corresponding bit in either <code>hcounteren</code> or <code>scounteren</code> is 0 and the same bit in <code>mcounteren</code> is 1; • in VS-mode or VU-mode, attempts to execute a hypervisor instruction (HLV, HLVX, HSV, or HFENCE); • in VS-mode or VU-mode, attempts to access an implemented non-high-half hypervisor CSR or VS CSR when the same access (read/write) would be allowed in HS-mode, assuming <code>mstatus.TVM=0</code>; • in VS-mode or VU-mode, if $XLEN=32$, attempts to access an implemented high-half hypervisor CSR or high-half VS CSR when the same access (read/write) to the CSR's low-half partner would be allowed in HS-mode, assuming <code>mstatus.TVM=0</code>; • in VU-mode, attempts to execute WFI when <code>mstatus.TW=0</code>, or to execute a supervisor instruction (SRET or SFENCE); • in VU-mode, attempts to access an implemented non-high-half supervisor CSR when the same access (read/write) would be allowed in HS-mode, assuming <code>mstatus.TVM=0</code>; • in VU-mode, if $XLEN=32$, attempts to access an implemented high-half supervisor CSR when the same access to the CSR's low-half partner would be allowed in HS-mode, assuming <code>mstatus.TVM=0</code>; • in VS-mode, attempts to execute WFI when <code>hstatus.VTW=1</code> and <code>mstatus.TW=0</code>, unless the instruction completes within an implementation-specific, bounded time; • in VS-mode, attempts to execute SRET when <code>hstatus.VTSR=1</code>; and • in VS-mode, attempts to execute an SFENCE.VMA or SINVAL.VMA instruction or to access <code>satp</code>, when <code>hstatus.VTVM=1</code>.
RVP.8.474	8.6.1 (p.129)	R	Other extensions to the RISC-V Privileged Architecture may add to the set of circumstances that cause a virtual instruction exception when $V=1$.
RVP.8.475	8.6.1 (p.129)	R	On a virtual instruction trap, <code>mtval</code> or <code>stval</code> is written the same as for an illegal instruction trap.
RVP.8.476	8.6.1 (p.129)	C	It is not unusual that hypervisors must emulate the instructions that raise virtual instruction exceptions, to support nested hypervisors or for other reasons. Machine level is expected ordinarily to delegate virtual instruction traps directly to HS-level, whereas illegal instruction traps are likely to be processed first in M-mode before being conditionally delegated (by software) to HS-level. Consequently, virtual instruction traps are expected typically to be handled faster than illegal instruction traps.
RVP.8.477	8.6.1 (p.129)	C	When not emulating the trapping instruction, a hypervisor should convert a virtual instruction trap into an illegal instruction exception for the guest virtual machine.

ID REFERENCE TYPE DEFINITION

RVP.8.478 8.6.1 (p.129) C Because TSR and TVM in mstatus are intended to impact only S-mode (HS-mode), they are ignored for determining exceptions in VS-mode.

RVP.8.479 8.6.1 (p.130) R Table 8.7 If an instruction may raise multiple synchronous exceptions, the decreasing priority order of the following table indicates which exception is taken and reported in mcause or scause. Synchronous exception priority when the hypervisor extension is implemented.

Priority	Exception Code	Description
Highest	3	Instruction address breakpoint
	12, 20, 1	During instruction address translation: First encountered page fault, guest-page fault, or access fault
	1	With physical address for instruction: Instruction access fault
	2	Illegal instruction
	22	Virtual instruction
	0	Instruction address misaligned
8, 9, 10, 11		Environment call
	3	Environment break
	3	Load/store/AMO address breakpoint
	4, 6	Optionally: Load/store/AMO address misaligned
	13, 15, 21, 23, 5, 7	During address translation for an explicit memory access: First encountered page fault, guest-page fault, or access fault
	5, 7	With physical address for an explicit memory access: Load/store/AMO access fault
Lowest	4, 6	If not higher priority: Load/store/AMO address misaligned

RVP.8.480 8.6.2 (p.130) H Trap Entry

RVP.8.481 8.6.2 (p.130) R When a trap occurs in HS-mode or U-mode, it goes to M-mode, unless delegated by medeleg or mideleg, in which case it goes to HS-mode.

RVP.8.482 8.6.2 (p.130) R When a trap occurs in VS-mode or VU-mode, it goes to M-mode, unless delegated by medeleg or mideleg, in which case it goes to HS-mode, unless further delegated by hedeleg or hideleg, in which case it goes to VS-mode.

RVP.8.483 8.6.2 (p.130) R Table 8.8 When a trap is taken into M-mode, virtualization mode V gets set to 0, and fields MPV and MPP in mstatus (or mstatush) are set according to the table below.

Previous Mode	MPV	MPP
U-mode	0	0
HS-mode	0	1
M-mode	0	3
VU-mode	1	0
VS-mode	1	1

RVP.8.484 8.6.2 (p.130) R A trap into M-mode also writes fields GVA, MPIE, and MIE in mstatus/mstatush and writes CSRs mepc, mcause, mtval, mtval2, and mtinst.

ID REFERENCE TYPE DEFINITION

- RVP.8.485 8.6.2 (p.130) R Upon trap return, MPV is ignored when MPP=3
- RVP.8.486 8.6.2 (p.131) R Table 8.9 When a trap is taken into HS-mode, virtualization mode V is set to 0, and hstatus.SPV and sstatus.SPP are set according to the table below.
- | Previous Mode | SPV | SPP |
|---------------|-----|-----|
| U-mode | 0 | 0 |
| HS-mode | 0 | 1 |
| VU-mode | 1 | 0 |
| VS-mode | 1 | 1 |
- RVP.8.487 8.6.2 (p.131) R If V was 1 before the trap, field SPVP in hstatus is set the same as sstatus.SPP; otherwise, SPVP is left unchanged.
- RVP.8.488 8.6.2 (p.131) R A trap into HS-mode also writes field GVA in hstatus, fields SPIE and SIE in sstatus, and CSRs sepc, scause, stval, htval, and htinst.
- RVP.8.489 8.6.2 (p.131) R Table 8.10 When a trap is taken into VS-mode, vsstatus.SPP is set according to the table below
- | Previous Mode | SPP |
|---------------|-----|
| VU-mode | 0 |
| VS-mode | 1 |
- RVP.8.490 8.6.2 (p.131) R Register hstatus and the HS-level sstatus are not modified, and the virtualization mode V remains 1.
- RVP.8.491 8.6.2 (p.131) R A trap into VS-mode also writes fields SPIE and SIE in vsstatus and writes CSRs vsepc, vscause, and vstval.
- RVP.8.492 8.6.3 (p.131) H Transformed Instruction or Pseudoinstruction for mtinst or htinst
- RVP.8.493 8.6.3 (p.131) R On any trap into M-mode or HS-mode, one of these values is written automatically into the appropriate trap instruction CSR, mtinst or htinst:
 - zero;
 - a transformation of the trapping instruction;
 - a custom value (allowed only if the trapping instruction is nonstandard); or
 - a special pseudoinstruction.
- RVP.8.494 8.6.3 (p.131) R Except when a pseudoinstruction value is required (described later), the value written to mtinst or htinst may always be zero, indicating that the hardware is providing no information in the register for this particular trap.
- RVP.8.495 8.6.3 (p.131) C The value written to the trap instruction CSR serves two purposes. The first is to improve the speed of instruction emulation in a trap handler, partly by allowing the handler to skip loading the trapping instruction from memory, and partly by obviating some of the work of decoding and executing the instruction. The second purpose is to supply, via pseudoinstructions, additional information about guest-page-fault exceptions caused by implicit memory accesses done for Vs-stage address translation.
- RVP.8.496 8.6.3 (p.131, p.132) C A transformation of the trapping instruction is written instead of simply a copy of the original instruction in order to minimize the burden for hardware yet still provide to a trap handler the information needed to emulate the instruction. An implementation may at any time reduce its effort by substituting zero in place of the transformed instruction.

ID REFERENCE TYPE DEFINITION

RVP.8.497	8.6.3 (p.132)	R	On an interrupt, the value written to the trap instruction register is always zero.
RVP.8.498	8.6.3 (p.132)	R	<p>On a synchronous exception, if a nonzero value is written, one of the following shall be true about the value:</p> <ul style="list-style-type: none"> • Bit 0 is 1, and replacing bit 1 with 1 makes the value into a valid encoding of a standard instruction. In this case, the instruction that trapped is the same kind as indicated by the register value, and the register value is the transformation of the trapping instruction, as defined later. For example, if bits 1:0 are binary 11 and the register value is the encoding of a standard LW (load word) instruction, then the trapping instruction is LW, and the register value is the transformation of the trapping LW instruction. • Bit 0 is 1, and replacing bit 1 with 1 makes the value into an instruction encoding that is explicitly designated for a custom instruction (not an unused reserved encoding). This is a custom value. The instruction that trapped is a nonstandard instruction. The interpretation of a custom value is not otherwise specified by this standard. • The value is one of the special pseudoinstructions defined later, all of which have bits 1:0 equal to 00.
RVP.8.499	8.6.3 (p.132)	R	These three cases exclude a large number of other possible values, such as all those having bits 1:0 equal to binary 10.
RVP.8.500	8.6.3 (p.132)	R	A future standard or extension may define additional cases, thus allowing values that are currently excluded.
RVP.8.501	8.6.3 (p.132)	R	Software may safely treat an unrecognized value in a trap instruction register the same as zero.
RVP.8.502	8.6.3 (p.132)	C	To be forward-compatible with future revisions of this standard, software that interprets a nonzero value from <code>mtinst</code> or <code>htinst</code> must fully verify that the value conforms to one of the cases listed above. For instance, for RV64, discovering that bits 6:0 of <code>mtinst</code> are 0000011 and bits 14:12 are 010 is not sufficient to establish that the first case applies and the trapping instruction is a standard LW instruction; rather, software must also confirm that bits 63:32 of <code>mtinst</code> are all zeros. A future standard might define new values for 64-bit <code>mtinst</code> that are nonzero in bits 63:32 yet may coincidentally have in bits 31:0 the same bit patterns as standard RV64 instructions.
RVP.8.503	8.6.3 (p.132)	C	Unlike for standard instructions, there is no requirement that the instruction encoding of a custom value be of the same “kind” as the instruction that trapped (or even have any correlation with the trapping instruction).

ID REFERENCE TYPE DEFINITION

RVP.8.504 8.6.3 (p.132) R Table 8.11 The table below shows the values that may be automatically written to the trap instruction register (`mtinst` or `htinst`) for each standard exception cause.

Exception	Zero	Transformed Standard Instruction	Custom Value	Pseudo-instruction Value
Instruction address misaligned	Yes	No	Yes	No
Instruction access fault	Yes	No	No	No
Illegal instruction	Yes	No	No	No
Breakpoint	Yes	No	Yes	No
Virtual instruction	Yes	No	Yes	No
Load address misaligned	Yes	Yes	Yes	No
Load access fault	Yes	Yes	Yes	No
Store/AMO address misaligned	Yes	Yes	Yes	No
Store/AMO access fault	Yes	Yes	Yes	No
Environment call	Yes	No	Yes	No
Instruction page fault	Yes	No	No	No
Load page fault	Yes	Yes	Yes	No
Store/AMO page fault	Yes	Yes	Yes	No
Instruction guest-page fault	Yes	No	No	Yes
Load guest-page fault	Yes	Yes	Yes	Yes
Store/AMO guest-page fault	Yes	Yes	Yes	Yes

RVP.8.505 8.6.3 (p.132) R For exceptions that prevent the fetching of an instruction, only zero or a pseudoinstruction value may be written.

RVP.8.506 8.6.3 (p.132) R A custom value may be automatically written only if the instruction that traps is nonstandard.

RVP.8.507 8.6.3 (p.132) R A future standard or extension may permit other values to be written, chosen from the set of allowed values established earlier.

RVP.8.508 8.6.3 (p.132) R As enumerated in the table, a synchronous exception may write to the trap instruction register a standard transformation of the trapping instruction only for exceptions that arise from explicit memory accesses (from loads, stores, and AMO instructions).

RVP.8.509 8.6.3 (p.132) R Accordingly, standard transformations are currently defined only for these memory-access instructions.

RVP.8.510 8.6.3 (p.132, p.133) R If a synchronous trap occurs for a standard instruction for which no transformation has been defined, the trap instruction register shall be written with zero (or, under certain circumstances, with a special pseudoinstruction value).

RVP.8.511 8.6.3 (p.133) R Figure 8.44 For a standard load instruction that is not a compressed instruction and is one of LB, LBU, LH, LHU, LW, LWU, LD, FLW, FLD, FLQ, or FLH, the transformed instruction has the format shown below. (Transformed noncompressed load instruction (LB, LBU, LH, LHU, LW, LWU, LD, FLW, FLD, FLQ, or FLH). Fields `funct3`, `rd`, and `opcode` are the same as the trapping load instruction).

31	...	25	24	...	20	19		15	14	...	12	11	...	7	6	...	0	
0		0																

RVP.8.512 8.6.3 (p.133) R The fields `funct3`, `rd`, and `opcode` are the same as the trapping load instruction.

ID REFERENCE TYPE DEFINITION

RVP.8.513	8.6.3 (p.133)	R	For a standard store instruction that is not a compressed instruction and is one of SB, SH, SW, SD, FSW, FSD, FSQ, or FSH, the transformed instruction has the format shown below. (Transformed noncompressed store instruction (SB, SH, SW, SD, FSW, FSD, FSQ, or FSH). Fields <i>rs2</i> , <i>funct3</i> , and <i>opcode</i> are the same as the trapping store instruction).																																							
			<table border="1"> <tr> <td>31</td><td>...</td><td>25</td><td>24</td><td>...</td><td>20</td><td>19</td><td></td><td>15</td><td>14</td><td>...</td><td>12</td><td>11</td><td>...</td><td>7</td><td>6</td><td>...</td><td>0</td></tr> <tr> <td>0</td><td></td><td></td><td><i>rs2</i></td><td></td><td></td><td>Address Offset</td><td></td><td><i>funct3</i></td><td></td><td>0</td><td></td><td></td><td></td><td><i>opcode</i></td><td></td><td></td><td></td></tr> </table>	31	...	25	24	...	20	19		15	14	...	12	11	...	7	6	...	0	0			<i>rs2</i>			Address Offset		<i>funct3</i>		0				<i>opcode</i>						
31	...	25	24	...	20	19		15	14	...	12	11	...	7	6	...	0																									
0			<i>rs2</i>			Address Offset		<i>funct3</i>		0				<i>opcode</i>																												
RVP.8.514	8.6.3 (p.133)	R	For a standard atomic instruction (load-reserved, store-conditional, or AMO instruction), the transformed instruction has the format shown below. (Transformed atomic instruction (load-reserved, store-conditional, or AMO instruction). All fields are the same as the trapping instruction except bits 19:15, Addr. Offset).																																							
			<table border="1"> <tr> <td>31</td><td>...</td><td>27</td><td>26</td><td>25</td><td>24</td><td>...</td><td>20</td><td>19</td><td>...</td><td>15</td><td>14</td><td>...</td><td>12</td><td>11</td><td>...</td><td>7</td><td>6</td><td>...</td><td>0</td></tr> <tr> <td><i>funct7</i></td><td></td><td><i>aq</i></td><td><i>rl</i></td><td></td><td><i>rs2</i></td><td></td><td></td><td>Address Offset</td><td></td><td><i>funct3</i></td><td></td><td><i>rd</i></td><td></td><td><i>opcode</i></td><td></td><td></td><td></td><td></td></tr> </table>	31	...	27	26	25	24	...	20	19	...	15	14	...	12	11	...	7	6	...	0	<i>funct7</i>		<i>aq</i>	<i>rl</i>		<i>rs2</i>			Address Offset		<i>funct3</i>		<i>rd</i>		<i>opcode</i>				
31	...	27	26	25	24	...	20	19	...	15	14	...	12	11	...	7	6	...	0																							
<i>funct7</i>		<i>aq</i>	<i>rl</i>		<i>rs2</i>			Address Offset		<i>funct3</i>		<i>rd</i>		<i>opcode</i>																												
RVP.8.515	8.6.3 (p.133)	R	For a standard virtual-machine load/store instruction (HLV, HLVX, or HSV), the transformed instruction has the format shown below. (Transformed virtual-machine load/store instruction (HLV, HLVX, HSV). All fields are the same as the trapping instruction except bits 19:15, Addr. Offset.)																																							
			<table border="1"> <tr> <td>31</td><td>...</td><td>25</td><td>24</td><td>...</td><td>20</td><td>19</td><td></td><td>15</td><td>14</td><td>...</td><td>12</td><td>11</td><td>...</td><td>7</td><td>6</td><td>...</td><td>0</td></tr> <tr> <td><i>funct7</i></td><td></td><td></td><td><i>rs2</i></td><td></td><td></td><td>Address Offset</td><td></td><td><i>funct3</i></td><td></td><td><i>rd</i></td><td></td><td><i>opcode</i></td><td></td><td></td><td></td><td></td><td></td></tr> </table>	31	...	25	24	...	20	19		15	14	...	12	11	...	7	6	...	0	<i>funct7</i>			<i>rs2</i>			Address Offset		<i>funct3</i>		<i>rd</i>		<i>opcode</i>								
31	...	25	24	...	20	19		15	14	...	12	11	...	7	6	...	0																									
<i>funct7</i>			<i>rs2</i>			Address Offset		<i>funct3</i>		<i>rd</i>		<i>opcode</i>																														
RVP.8.516	8.6.3 (p.134)	R	In all the transformed instructions above, the Address Offset field that replaces the instruction's <i>rs1</i> field in bits 19:15 is the positive difference between the faulting virtual address (written to <i>mtval</i> or <i>stval</i>) and the original virtual address.																																							
RVP.8.517	8.6.3 (p.134)	R	This difference can be nonzero only for a misaligned memory access.																																							
RVP.8.518	8.6.3 (p.134)	R	Note also that, for basic loads and stores, the transformations replace the instruction's immediate offset fields with zero.																																							
RVP.8.519	8.6.3 (p.134)	R	For a standard compressed instruction (16-bit size), the transformed instruction is found as follows: 1. Expand the compressed instruction to its 32-bit equivalent. 2. Transform the 32-bit equivalent instruction. 3. Replace bit 1 with a 0.																																							
RVP.8.520	8.6.3 (p.134)	R	Bits 1:0 of a transformed standard instruction will be binary 01 if the trapping instruction is compressed and 11 if not.																																							
RVP.8.521	8.6.3 (p.134)	C	In decoding the contents of <i>mtinst</i> or <i>htinst</i> , once software has determined that the register contains the encoding of a standard basic load (LB, LBU, LH, LHU, LW, LWU, LD, FLW, FLD, FLQ, or FLH) or basic store (SB, SH, SW, SD, FSW, FSD, FSQ, or FSH), it is not necessary to confirm also that the immediate offset fields (31:25, and 24:20 or 11:7) are zeros. The knowledge that the register's value is the encoding of a basic load/store is sufficient to prove that the trapping instruction is of the same kind.																																							
RVP.8.522	8.6.3 (p.134)	C	A future version of this standard may add information to the fields that are currently zeros. However, for backwards compatibility, any such information will be for performance purposes only and can safely be ignored.																																							

ID REFERENCE TYPE DEFINITION

- RVP.8.523 8.6.3 (p.135) R For guest-page faults, the trap instruction register is written with a special pseudoinstruction value if:
 (a) the fault is caused by an implicit memory access for VS-stage address translation, and
 (b) a nonzero value (the faulting guest physical address) is written to `mtval2` or `htval`.
- RVP.8.524 8.6.3 (p.135) R If both conditions are met, the value written to `mtinst` or `htinst` must be taken from the table below; zero is not allowed.
- | Value | Meaning |
|------------|--|
| 0x00002000 | 32-bit read for VS-stage address translation (RV32) |
| 0x00002020 | 32-bit write for VS-stage address translation (RV32) |
| 0x00003000 | 64-bit read for VS-stage address translation (RV64) |
| 0x00003020 | 64-bit write for VS-stage address translation (RV64) |
- RVP.8.525 8.6.3 (p.135) R For the special pseudoinstruction values for guest-page faults, the RV32 values are used when `VSXLEN=32`, and the RV64 values when `VSXLEN=64`.
- RVP.8.526 8.6.3 (p.135) I Table 8.13 The defined pseudoinstruction values are designed to correspond closely with the encodings of basic loads and stores, as illustrated by below
- | Encoding | Instruction |
|------------|--------------------------|
| 0x00002003 | <code>lw x0,0(x0)</code> |
| 0x00002023 | <code>sw x0,0(x0)</code> |
| 0x00003003 | <code>ld x0,0(x0)</code> |
| 0x00003023 | <code>sd x0,0(x0)</code> |
- RVP.8.527 8.6.3 (p.135) R A write pseudoinstruction (`0x00002020` or `0x00003020`) is used for the case that the machine is attempting automatically to update bits A and/or D in VS-level page tables.
- RVP.8.528 8.6.3 (p.135) R All other implicit memory accesses for VS-stage address translation will be reads.
- RVP.8.529 8.6.3 (p.135) R If a machine never automatically updates bits A or D in VS-level page tables (leaving this to software), the write case will never arise.
- RVP.8.530 8.6.3 (p.135) R The fact that such a page table update must actually be atomic, not just a simple write, is ignored for the pseudoinstruction.
- RVP.8.531 8.6.3 (p.135) C If the conditions that necessitate a pseudoinstruction value can ever occur for M-mode, then `mtinst` cannot be entirely read-only zero; and likewise for HS-mode and `htinst`. However, in that case, the trap instruction registers may minimally support only values 0 and `0x00002000` or `0x00003000`, and possibly `0x00002020` or `0x00003020`, requiring as few as one or two flip-flops in hardware, per register.
- RVP.8.532 8.6.3 (p.135) C There is no harm here in ignoring the atomicity requirement for page table updates, because a hypervisor is not expected in these circumstances to emulate an implicit memory access that fails. Rather, the hypervisor is given enough information about the faulting access to be able to make the memory accessible (e.g. by restoring a missing page of virtual memory) before resuming execution by retrying the faulting instruction.
- RVP.8.533 8.6.4 (p.135) H Trap Return

ID REFERENCE TYPE DEFINITION

RVP.8.534	8.6.4 (p.135)	R	The MRET instruction is used to return from a trap taken into M-mode.
RVP.8.535	8.6.4 (p.135)	R	MRET first determines what the new privilege mode will be according to the values of MPP and MPV in <code>mstatus</code> or <code>mstatush</code> as encoded in RVP.8.483
RVP.8.536	8.6.4 (p.135)	R	MRET then in <code>mstatus/mstatush</code> sets MPV=0, MPP=0, MIE=MPIE, and MPIE=1.
RVP.8.537	8.6.4 (p.135)	R	Lastly, MRET sets the privilege mode as previously determined, and sets <code>pc=mepc</code> .
RVP.8.538	8.6.4 (p.135)	R	The SRET instruction is used to return from a trap taken into HS-mode or VS-mode.
RVP.8.539	8.6.4 (p.135)	R	Its (SRET) behavior depends on the current virtualization mode.
RVP.8.540	8.6.4 (p.135)	R	When executed in M-mode or HS-mode (i.e., <code>V=0</code>), SRET first determines what the new privilege mode will be according to the values in <code>hstatus.SPV</code> and <code>sstatus.SPP</code>
RVP.8.541	8.6.4 (p.135)	R	SRET then sets <code>hstatus.SPV=0</code> , and in <code>sstatus</code> sets <code>SPP=0</code> , <code>SIE=SPIE</code> , and <code>SPIE=1</code> .
RVP.8.542	8.6.4 (p.135)	R	Lastly, SRET sets the privilege mode as previously determined, and sets <code>pc=sepcc</code> .
RVP.8.543	8.6.4 (p.135)	R	When executed in VS-mode (i.e., <code>V=1</code>), SRET sets the privilege mode according to <code>vsstatus.SPP</code> , in <code>vsstatus</code> sets <code>SPP=0</code> , <code>SIE=SPIE</code> , and <code>SPIE=1</code> , and lastly sets <code>pc=vsepc</code> .