Simics Cheatsheet

1 Simics Usage (command line)

1.1 Glossary & Documentation

Simics *Base*	simics executable + the set of supporting shared libraries (DLLs) + tools
simulation	running of code (target) on a model/platform (target) with advancement of time
host	a computer where simulation runs
target	a simulated code running in its isolated memory region, e.g. Linux or Windows guest
platform	a complete runnable model: full set-up of devices with CPU or with at least a clock provider
package	a set of devices, oftentimes constituting 1 platform, distributed as a whole in an archive and unpacked into 1 directory
*[**Simics**] Script*	simple Unix-shell-like language (a wrapper over Python) used for connecting devices and command line automation
Simics User's Guide	documentation on **Simics** usage — both command line and Eclipse

Below **$** stands for Unix shell prompt, **>** for **Simics** prompt. *Big_italic* text means user-supplied arguments for commands/functions.

1.2 Set up a workspace with platform package

```
$ path/to/simics-base/bin/project-setup .
$ bin/addon-manager -c # remove default package associations
# Allow scripts & shared libraries be found:
$ bin/addon-manager -s /path/to/platform-package
$ bin/addon-manager -s /path/to/additional/package
```

1.3 Start up

```
$ ./simics targets/platform/platform.simics
```

Shell command line arguments ⟶ **Simics** command line correspondence:

	$ ./simics start.simics	
→	$ ./simics > run-command-file start.simics	
	$ ./simics script.py	
→	$ ./simics > run-python-file script.py	
	$ ./simics -e '$config_variable1=value; $config_var2=value' start.simics # ⚠ **NOT ./simics start.simics -e $varibables ...**	
→	$ ./simics > $config_variable=value > $config_var2=value > run-command-file start.simics	

1.4 Environment & Packages

```
> version # list of installed packages
$ ./simics -v # the same
> pwd # current directory where simics is running
> list-directories # where Simics searches files
```

To debug chain of called auxiliary scripts include s:

```
$ ./simics -script-trace targets/platform/platform.simics
```

1.5 Commands for running simulation

```
> c[ontinue]
> r[un] 100 cycles     # or 10 steps or 0.1 seconds
> ptime [-all]     # to show target's time
> print-event-queue     # show all pending events (e.g. timers)
# To know CPU/clock which advances time for the device (and executes events):
> platform.myDevice->queue
```

1.6 Printing device structure

To find devices by name/class or interface name:

```
> list-objects -all name     # searches also for the class
> list-objects -all substr = mem # object names containing mem
> list-objects -all iface = my_interface # by interface name
```

To examine device structure (**Simics** *components* and *devices*) of a given component *myPlatform*:

```
# 1-level representation: immediate children myPlatform:
> list-objects namespace = myPlatform
# Multi-level one: all children of myPlatform with all hierarchy:
> list-objects namespace = myPlatform -tree
```

To find all objects with the same class as given device:

```
> platform.myDevice->classname
myClass
> list-objects -all myClass
> list-objects -all class = myClass
```

1.7 Registers

```
# Print all registers:
> print-device-regs platform.myDevice
# Print fields of register myRegister:
> print-device-reg-info platform.myDevice.myBank.myRegister
```

1.7.1 Writing/reading with side effects

```
> write-device-reg
    platform.myDevice.bank.Bank.Group.myRegister 0x1
# (register groups like myGrp may be omitted in devices)
> read-device-reg platform.myDevice.bank.Bank.Group.myRegister
```

1.7.2 Writing/reading **without** side effects (aka set/get)

```
# You can use set-device-reg / get-device-reg...
# ...or do it through attributes, e.g. to set to value 0x1:
platform.myDevice->Bank_Group_register = 0x1
# To get the value:
platform.myDevice->Bank_Group_register
```

1.8 Connects — attributes that point to other devices

```
# To set a connect attribute:
> platform.myDevice->myConnect = ”platform.Device2”
# To zero connect attribute:
> platform.myDevice->myConnect = FALSE      # obvious ;-)
```

1.9 Device information: static

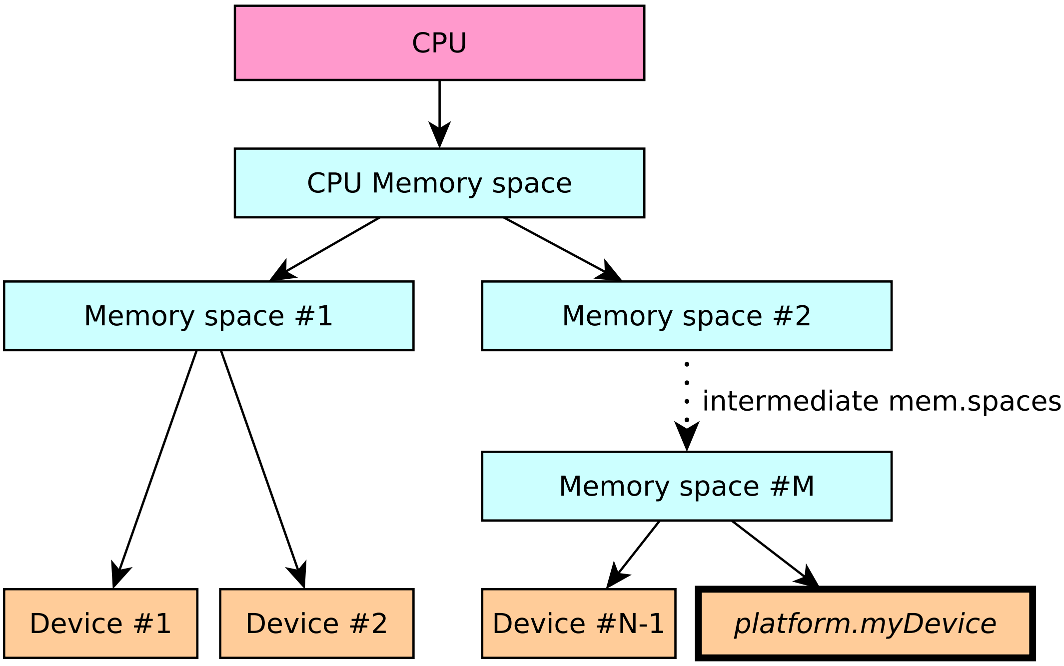
```
# To find info about class/module/package for your device:
> help platform.myDevice
    Class myClass
    Provided By
        myModule (from myPackage)
    # ...then documentation about the device is printed.
# To list all classes provided by a module:
> list-classes -m myModule
# Configuration information:
> platform.myDevice.info
```

1.10 Device information: dynamic

 # Runtime information:
> *platform.myDevice*.status
 # pretty-print device attributes with values:
> list-attributes *platform.myDevice*
 # to search all attributes/registers containing *mem***:**
list-attributes *platform.myDevice* substr = *mem*

1.11 Memory spaces

All target software runs on CPU and can access devices only through hierarchy of memory spaces:



 # To find memory spaces the device is mapped in:
> devs *platform.myDevice*

1.12 Getting help

 # Get help on some command:
> help *instantiate-components*
 # Finding sections of documentation mentioning it:
> apropos *instantiate-components*
 # To open Simics Documentation in browser run from workspace:
$ ./documentation **# or .\documentation.bat on Windows**

1.13 Debugger commands

To use **Simics** to debug target:

```
dis[assemble] # show assembler commands at current address
# Set break point on physical memory access from current CPU:
break address [-r] [-w] [-x] # -rw by default
# To break from specific CPU:
cpu.phys_mem.break address [-r] [-w] [-x]
# To break on access from any memory space to myDevice:
break-io myDevice Bank Offset Length
# To break on specific conditions, "HAP"s:
break-hap Core-Magic-Instruction # run list-haps for options
```

1.14 Examining current state

pselect	show currently running CPU
memory-map	print all mapped devices
pregs	print all CPU registers
probe-address *addr*	path to target *addr*

1.15 x86-specific and platform-specific commands

memory-trace *addr*	path to target *addr*
pregs	to know x86 mode (16/32/64-bit), 1st line
reset-button-press	to reboot the target
power-button-press	to press power button

1.16 Moving files target ⟷ host

```
> start-simicsfs-server
```

```
target$ mkdir a
target$ simicsfs-client a
```

1.17 Saving info

Save logs from current point

```
> start-command-line-capture filename
```

To save simics variables to a file:

```
> start-command-line-capture filename
> list-variables
> stop-command-line-capture
```

1.18 Check points

write-configuration "*checkpoint_name*"	— save checkpoint
read-configuration "*checkpoint_name*"	— restore it back

1.19 Creating components dynamically (for hot plug)

```
> create-myDevice-comp "platform.myDeviceComp"
> connect platform.myDeviceComp.connectorName ↩
  platform.Device2.connectorName
> instantiate-components
```

1.20 Miscellaneous

```
# To dump network packages (for analysis with Wireshark):
> pcap-dump link=ethernet_switch0 filename=myFile
```

```
# Treat all input as Python code:
> python-mode
> > > Enter your Python code
```

2 Simics DML 1.4 Programming & C/DML API

2.1 Glossary & Documentation

DML	Device Modelling Language is a wrapper over C for writing (fast) devices. Its compiler is included into **Simics** Base.
device	any **Simics** class for modelling real devices. Different **Simics** devices communicate via *interfaces*.
Model Builder User's Guide	overview of **Simics**/DML programming
DML 1.4 Reference Manual	language specification
API Reference Manual	API function list for DML & C, describes ownership rules
model writers	those who write **Simics** devices
users	those who use **Simics** devices: device driver writers, firmware/UEFI writers, validators/testers, etc

2.2 Getting help

```
# Print explanation of C/Python/DML API functions:
> api-help SIM_add_configuration
```

2.3 Create stub device

```
$ bin/project-setup --device example-dev
$ ls modules/example-dev
test/ example-dev.dml Makefile module_load.py
```

The header of *example-dev*.dml is then:

```
dml 1.4;                // obligatory .dml header
device example_dev;     // class name.
                        // Note: - changed to underscore _
```

2.4 Create stub interface with Python wrapper

```
$ bin/project-setup --interface sample
$ ls modules/sample-interface
Makefile sample-interface.dml sample-interface.h
```

Python support is enabled by `IFACE_FILES` in the Makefile. The generated C **struct** name is `sample_interface_t`.

2.5 Arithmetics

2.5.1 RHS is int64, LHS truncates

Assignments are equivalent to casts and hence can truncate:

```
local uint8 x = 0xffff // results in x == 0xff
```

All aritmetic operators like $+$, $*$ convert its operands to int64:

```
local uint16 i = 0x7fff; local int8 j = 2; // Let us sum them:
local int16 x = i + j;   // calculates as int64 → 0x8001, truncates to int16
// finally results in x == 1.
```

2.5.2 Comparisons act as uint64 or int64: ==, <, <=

Comparisons on only **uint64** act as proper **uint64**, however in comparisons **int64** vs. **uint64** the operands are converted to **int64**!

```
local uint64 u;
u = -1;     // equivalent to u = cast(-1, uint64) = 2^64 - 1, all ones
u == -1    // FALSE! Equivalent to int64(u) == int64(-1),
           // where upper bit is cropped: int64(u) == (2^63 - 1).
u == cast(-1, uint64) // true. As comparison is b/w two uint64
u > -1     // true, but unlike C! it's int64(u) > int64(-1): 2^63 - 1 > 1
```

2.6 Syntax

2.6.1 Statements

```
// Printing through log statements:
log log-type, level, groups: "format-string", arg_1, ..., arg_N;
                (level: default 1; groups: default 0 (no group))
// (the "format-string" is the same as in C, see 'man 3 printf')
```

log-level	usage rule
1	most important messages (for both users and model writers), typically `error`
2	crucial events for boards/devices, e.g. their resets
3	any other messages (for users)
4	internal device debug messages (for model writers)

log-type	usage rule
`info`	informational message
`spec_viol`	specification violation by target software (for users)
`unimpl`	attempt to use not implemented functionality (for users)
`error`	internal device error (for model writers). ⚠ There is a limit (default 10_000) after which simulation stops!
`critical`	like `spec_viol` or error, but ⚠ stops simulation

```
// Dynamic allocation (like malloc() in C):
local type * x = new type;
// E.g. for int array:
local int * x = new int[100];
delete x; // deallocation like free() in C
// Raising/catching exceptions:
try {
    throw; // YES, no data can be carried by exception
} catch {
    ...
}
```

2.6.2 Expressions

```
sizeof value // : int — get byte size of the value
sizeoftype type // : int — get byte size of the type
x[10:8] // get bits 10—8 of integer x:
x[8] // get bit 8 of integer x:
```

2.6.3 Scalar types

DML-specific: **uint1**...**uint64** and **int1**...**int64** (+ aliases: **int** → **int32**, **char** → **int8**), **uint8_be/le_t** ... **uint64_be/le_t**.
C-like types: **size_t**, **uintptr_t**, **double**, **bool**.

2.6.4 Derived types

```
typedef struct { member declarations; } typeName;
// Layout members can be only whole-byte (int8, int16, ...):
typedef layout "big-endian" { member declarations; } typeName;
// Bitfield size sizeBits can be 1 ... 64 and field size arbitrary:
typedef bitfields sizeBits {
    uint3 a @ [31:29];      // just an example
    ...
} typeName;
// All the types can be used for variable definitions inline, e.g.:
{
    local struct { uint8 field; } variableName;
    variableName.field = 255;
```

2.6.5 Methods

They are called *methods*, not functions, because they accept **implicit** 1st argument — object (current device), like C++ methods. Thus multiple instances of each device are allowed.

```
method name(inputType₁ arg₁) -> (outputType₁, outputType₂) {
    ...
    local outputType₁ var₁ = ...; local outputType₂ var₂ = ...;
    return (var₁,var₂);
}
// Calling this method:
local inputType₁ val = ...;
local outputType₁ x; local outputType₂ y;
(x, y) = name(val);
```

2.6.6 Bitfields

```
bitfields 32 {
    uint3 upper_bits @ [31:29];
    ...
}
```

2.6.7 Object declarations

```
objectType objectName {
    method methodName {
        ...
    }
}
register regName @ offset is (template₁, ...);
// @ offset is a syntax for "param offset = offset;"
```

2.6.8 Module variables and other data objects

DML construct	check-pointed	fields	address-mapped	arbitrary data
session	-	-	-	+
saved	+	-	-	-
attribute	+	-	-	+
unmapped register	+	+	-	-
[normal] register	+	+	+	-

2.6.9 Interfaces

Definition in `.dml`:

```
extern typedef struct {
    method name(conf_object_t *obj, type₁ value₁)
        -> out_type;
} sample_interface_t;
```

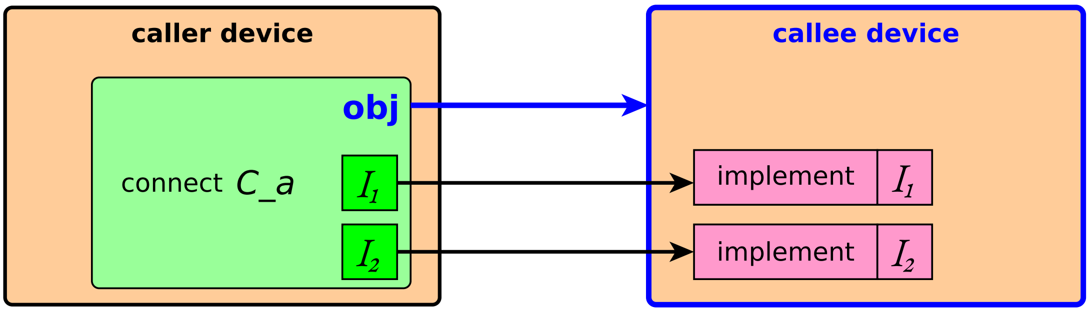
Obligatory definition in C `.h` file **for using the interface from Python**:

```
SIM_INTERFACE(sample) { // essentially 'typedef struct' also
    out_type (*name)(conf_object_t *obj, type₁ value₁);
}
#define SAMPLE_INTERFACE "sample"    // necessary!
```

Then it is called **without** `obj`: just `name(value₁)`.

2.6.10 Explaining connects and implements

- connects are for **out**bound calls
- implements are for **in**bound calls



	unnamed (whole-device)	named (wrapped in attribute)

connect	-	connect C_a { ❶
		  interface I_1 { ❷
		    ...
		  }
		  interface I_2 { ❷
		    ...
		  }
		}
		connect C_b { ❶
		  interface I_2 { ❷
		    ...

implement	implement I_1 {
	  ...
	}
	implement I_2 {
	  ...
	}
	as in picture above
		port P_A {
		  implement I_1 {
		    ...
		  }
		  implement I_2 {
		    ... *1st way of* I_2 ...
		  }
		}
		port P_B {
		  implement I_2 {
		    ... *2nd way of* I_2 ...

To make the whole connect required:

❶
```
param configuration = "required";
// other variants: "optional" (default), "pseudo", "none"
```

❷ Individual interfaces are already **required** by default, to make them optional:

```
param required = false;
```

⚠ implement {} does NOT check that all (or any!) methods of an interface are really provided, defaulting to **NULL**.

2.7 Calling device code from Python

If *device* implements interface $iface_1$ then its methouds can be invoked from **Simics** command line via Python:

```
@conf.platform.device.iface.iface_1.method_1(argument_1, ...)
```

2.8 Debugging with Gdb

To debug simics and its modules itself:

Terminal #1:

```
# Recompile your module with debugging support:
$ make clobber-my-module
$ make D=1 my-module
$ ./simics
> pid
12345
```

Terminal #2:

```
$ bin/gdb
>>> attach 12345
>>> br file.dml:100      # set break point on line 100 of file.dml
>>> continue
```

Back to terminal #1:

```
> run-command-file targets/platform/platform.simics
```

2.8.1 Using gdb for debugging target

```
load-module gdb-remote
new-gdb-remote 50000      # open port 50000
```

2.9 Attribute values

attr_value_t is a C union that can hold one of a few predefined types.

Attributes values are allocated/packed by:

`attr_value_t x = SIM_make_attr_T(cType val)`, and extracted by:

`cType val = SIM_attr_T(x)`, where *T* and *cType* can be:

T	type spec	*cType* — DML/C type
uint64, int64	i	**uint64**, **int64**
boolean	b	**bool**
floating	f	**double**
string	s	**char***
object	o	**conf_object_t**
list	[x_1...x_n]	fixed-width tuple with n elements of types x_1, ..., x_n
list	[x*]	arbitrary-width array of x
list	[x+]	non-empty arbitrary-width array of x
list	[$x\{m:n\}$]	array of x with $m \le size \le n$
list	[$x\{n\}$]	fixed-width tuple with n elements of x
dict	D	array of **attr_dict_pair_t**
data	d	**uint8***
nil	n	**void** or x*
invalid		(none, used for indicating errors)

List items are accessed by `SIM_attr_list_item`. Type specs can be OR'ed as $x_1|x_2$. Type spec is used in `param type = "..."`. For first 4 types there are predefined DML templates `uint64_attr`, `int64_attr`, `bool_attr`, `double_attr`.

2.10 Attribute initialization

Execution stage	SIM_object_is_-configured(obj)	SIM_is_-restoring_-state()
Create object at 1st platform init	-	-
Load checkpoint	-	+
Load micro-checkpoint (reverse execution)	+	+
Manual attribute assignment (hot plug from **Simics** command line)	+	-

2.11 Standard register templates

`read`, `write` — make a register readable/writeable, `init_val` — reset a register to value of `param init_val = ...` of the same name.

2.12 Compile-time statements & conditional compilation

```
param p1 = 10; // non-overridable parameter
param p2 default "value"; // an overridable parameter
template myTemplate {
    // Undefined value — must be given
    // on myTemplate instantiation:
    param p3;
    ...
}
// Compile-time if:
#if (p1 == 20) {
    ...
} #else #if {
    ...
} #else {
    ...
}
// Compile-time ternary operator #? #: :
param mode = p1 == 20 #? "equal 20" #: "not equal 20";
// Represent value of parameter as string:
param p1_str = stringify(p1); // results in "10"
```

2.13 Hash tables

```
import "simics/util/hashtab.dml";
...
local ht_str_table_t tab; // str — string (aka const char*) keys.
ht_init_str_table(&tab, /*keys_owned*/ true);
local double *value = new double; *value = 10.0;
ht_insert_str(&table, "key", cast(value, void *));
local double *get_back = cast(ht_lookup_str(&tab, "key"), double*);
assert *get_back == 10.0;
```

There are also tables for `int` keys or general (`common`) keys.

2.14 The secret of DML

Many "internal" features like registers and even connects are actually normal templates for objects (`is object;`) in plain DML defined in `simicsBase/{linux64|win64}/bin/dml/1.4/dml-builtins.dml` and thus they can be expanded.

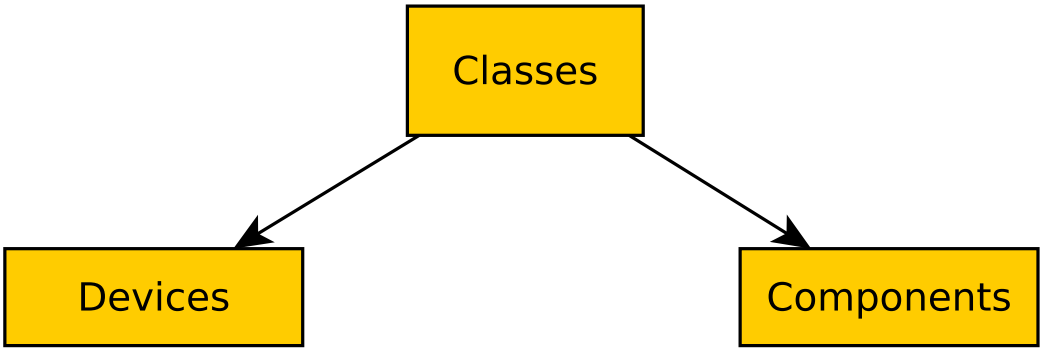
2.15 C API

It's possible to do most things in C, e.g. create device by `SIM_create_object`, though normally it's done from Python components.

3 Simics configuration and build system

3.1 Glossary & Documentation

Python	this language is used for connecting devices together (writing components), for writing some (slow) devices, for unit-testing
Component	a special **Simics** class that forms a namespace tree and (typically) in its nodes contains instances of device classses. Components implement required `component` interface and optional `component_connector` interface.



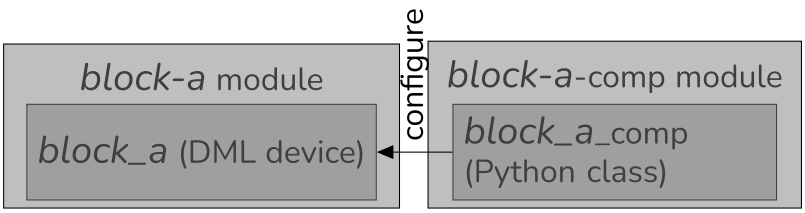
3.2 Modules/Components/Classes

A **Simics** module includes classes, there are 2 types of them:

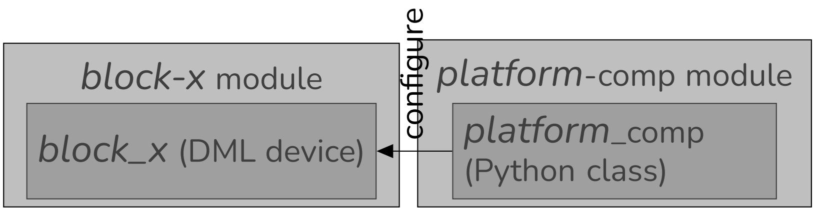
- devices, typically written in DML
- *components*, typically written in Python

Component is a **support** entity: normally components are used only on initialization phase to **configure** devices (set their attributes). During simulation only device instances act (the known exception is hot-plug).

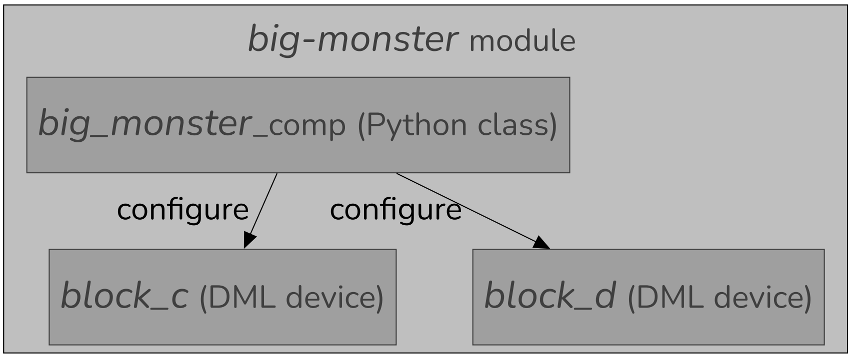
A typical layout with 1-to-1 device-component correspondence:



In simplest case there are no components for a device, so its *platform* will have to instantiate and configure the device:



There can be a module with 1 component and many classes:



3.3 Components vs simple devices

Components/connectors are used:

- when there is a need to unite big number of devices to prevent pollution of the surrounding namespace
- when this is a separate device that can be used across different packages independently

Otherwise use simple devices by just assigning *connects* to *implements* directly using **Simics** Script or Python:

```
> platform.device1->connect1 = platform.device2
@conf.platform.device1.connect1 = conf.platform.device2
```

⚠ Do not confuse: *Connectors* connect *component* objects, while *connects* (+implements) connect *device* objects. The `connect` command acts on (component) connectors only!

3.4 Creating devices in tests

```
x = simics.pre_conf_object("myDevice", "device_name")
x.some_required_attribute = y
   # (where y can be another pre_conf_object)
simics.SIM_add_configuration([x], None)
```

3.5 Creating devices in components

```
class Component_name(Standard_component):
   def add_objects(self):
      x = self.add_pre_obj('myDevice', 'device_name')
      x.some_required_attribute = y
```

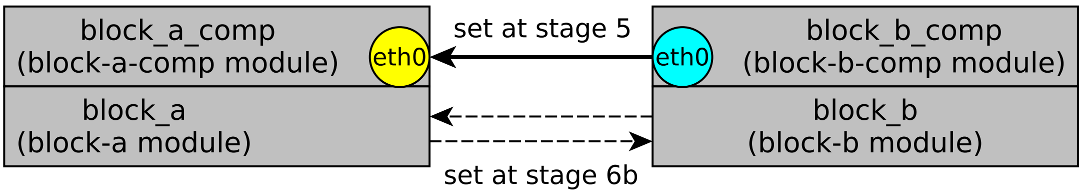
Then slot *myDevice* is created inside any instance of *Component_name*.

3.6 Structure and initialization order

A typical structure of component class code:

```
class block_a_comp(StandardComponent):
    @classmethod
    def register(cls):
        ...
    def __init__(self):
        ...
    def setup(self):
        ...                    calls
    def add_objects(self):
        ...
    class attribute_name(ConfigAttribute):
        def _initialize(self):
            ...
        def _finalize(self):
            ...
    class component_connector(Interface):
        def get_connect_data(self, block_a_connector):
            ...
        def connect(self, block_a_connector, data_from_b):
            ...
    ...
    class component(StandardComponent.component):
    ...
```

Imagine we want to connect 2 components with their corresponding devices, where block_b has an *Up* connector eth0 and block_a has a *Down* connector eth0:

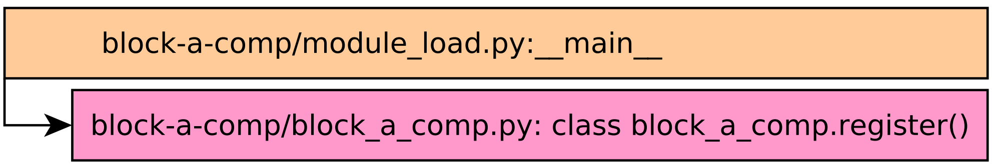


Let us examine initialization of modules ⟶ components ⟶ devices for this sample program:

```
1 load-module block-a-comp
2 load-module block-b-comp
3 create-block-a-comp "block_a_component"
4 create-block-b-comp "block_b_component"
5 connect block_a_component.eth0 block_b_component.eth0
6 instantiate-components
```

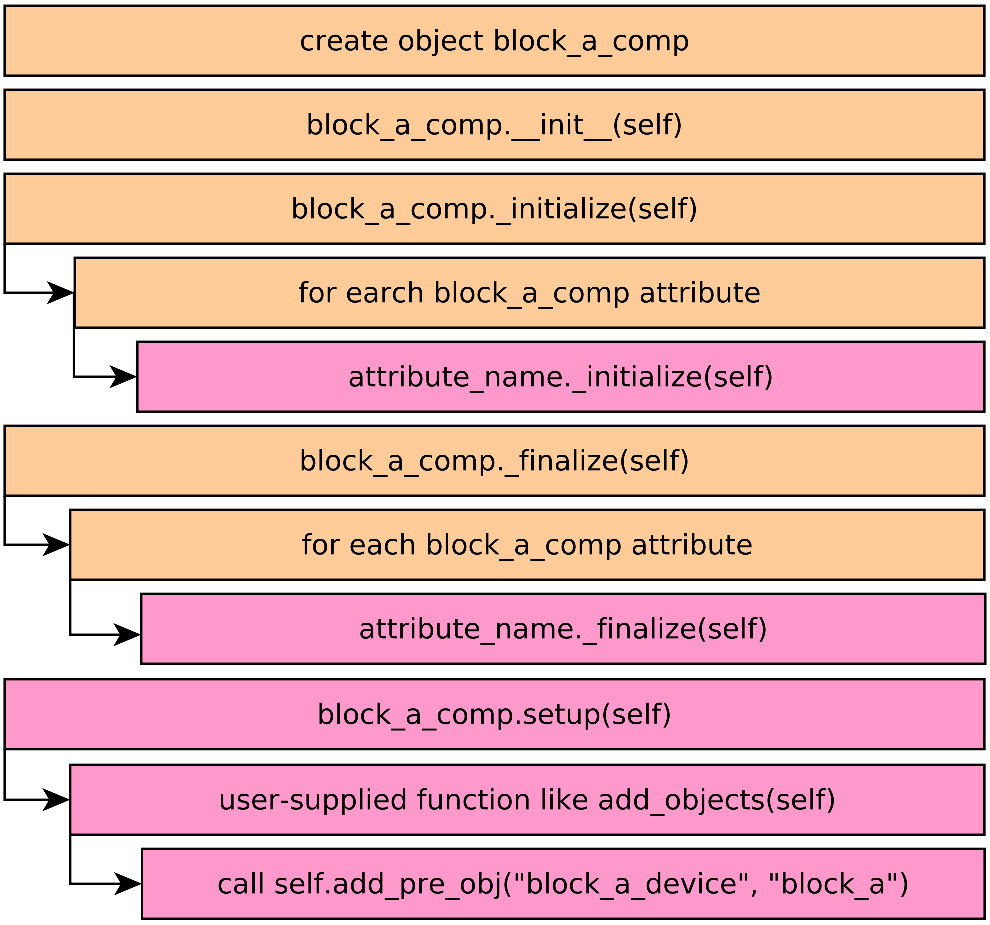
The corresponding break down of functions that are normally simics-defined or user-defined.

1



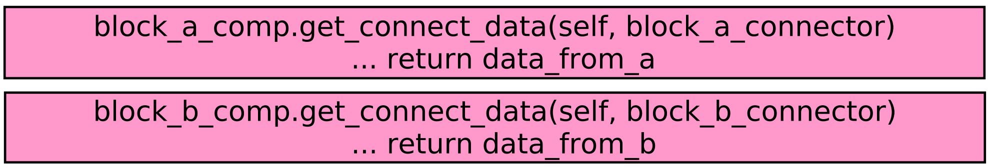
❷ The same for block_b_comp

❸ Note that add_objects adds normally pre-configured objects:



❹ The same for block_b_comp & block_b

❺



Note get_connect_data is basically just a switch/case statement that chooses which data (object references, port names, etc) to pass to connect function call below.

6a

block_b_comp.class component_connector(Interface).connect(
self, block_b_connector, data_from_a)

set connects of block_b DML device:
block_b_component.block_b_device = data_from_a["field"]

block_a_comp.class component_connector(Interface).connect(
self, block_a_connector, data_from_b)

set connects of block_a DML device:
block_a_component.block_a_device = data_from_b["field"]

block_a_comp.component.pre_instantiate(self)
block_b_comp.component.pre_instantiate(self)

6b Pre-configuration phase ends and finally `instantiate-components` begins to configure real DML objects:

block_a: call init() on all attributes with `init` template applied.
block_a: call device method init()

block_b: call init() on all attributes with `init` template applied.
block_b: call device method init()

block_a: call set() for all connects/attributes

block_b: call set() for all connects/attributes

block_a: call device method post_init()

block_b: call device method post_init()

After that phase `self.get_slot(”name”)` returns real, already configured, device objects.

6c Rarely some additional tweaks are required on configured objects:

block_a_comp.component.post_instantiate(self)

block_b_comp.component.post_instantiate(self)