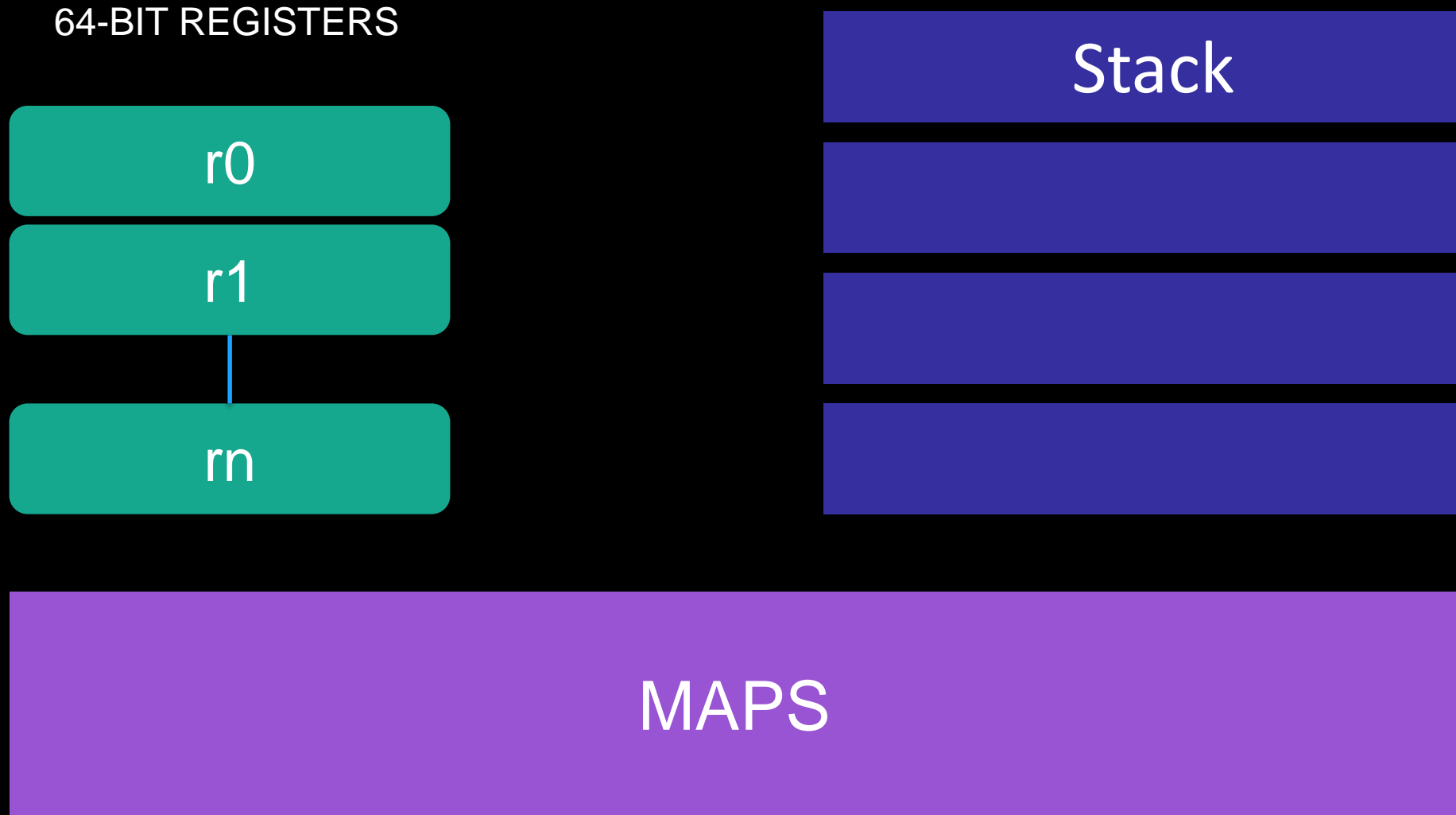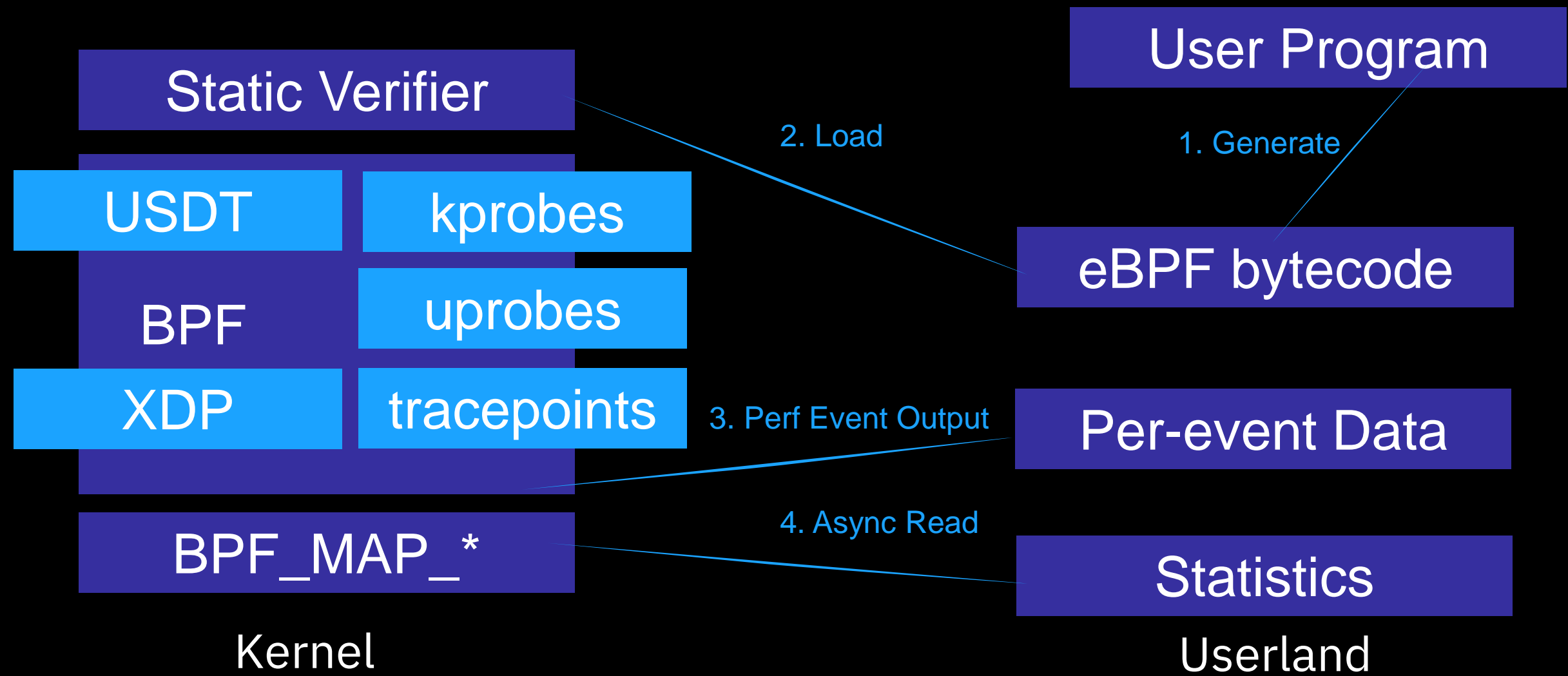# What is eBPF?

- eBPF = Extended Berkley Packet Filter | BPF
- WASM for Kernels!!
- Safe Reduced Instruction Set Computer
- Excellent kernel enhancement framework

Runtime Architecture

64-BIT REGISTERS

r0

r1

rn

Stack

MAPS

eBPF Program Life Cycle

Static Verifier

USDT · BPF · XDP · kprobes · uprobes · tracepoints

BPF_MAP_*

Kernel

User Program

eBPF bytecode

Per-event Data

Statistics

Userland

1. Generate

2. Load

3. Perf Event Output

4. Async Read

http://www.brendangregg.com/ebpf.html

EBPF Script Creation Options

BPF Compiler Collection BCC	bpftrace

libbcc

EBPF