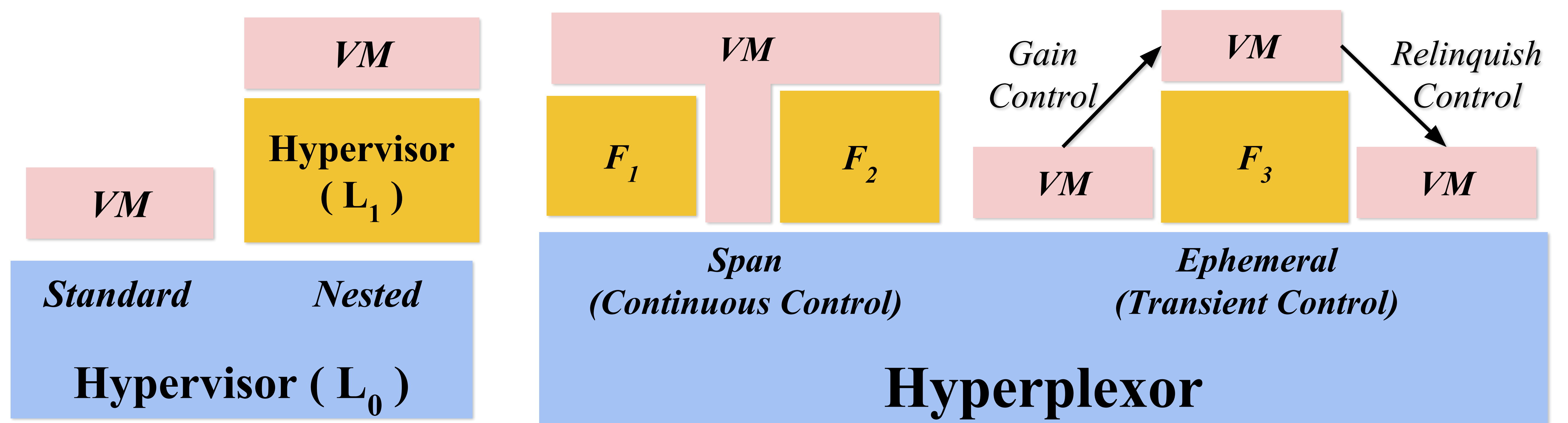


Problem: Support for 3rd-Party Hypervisor-level Services

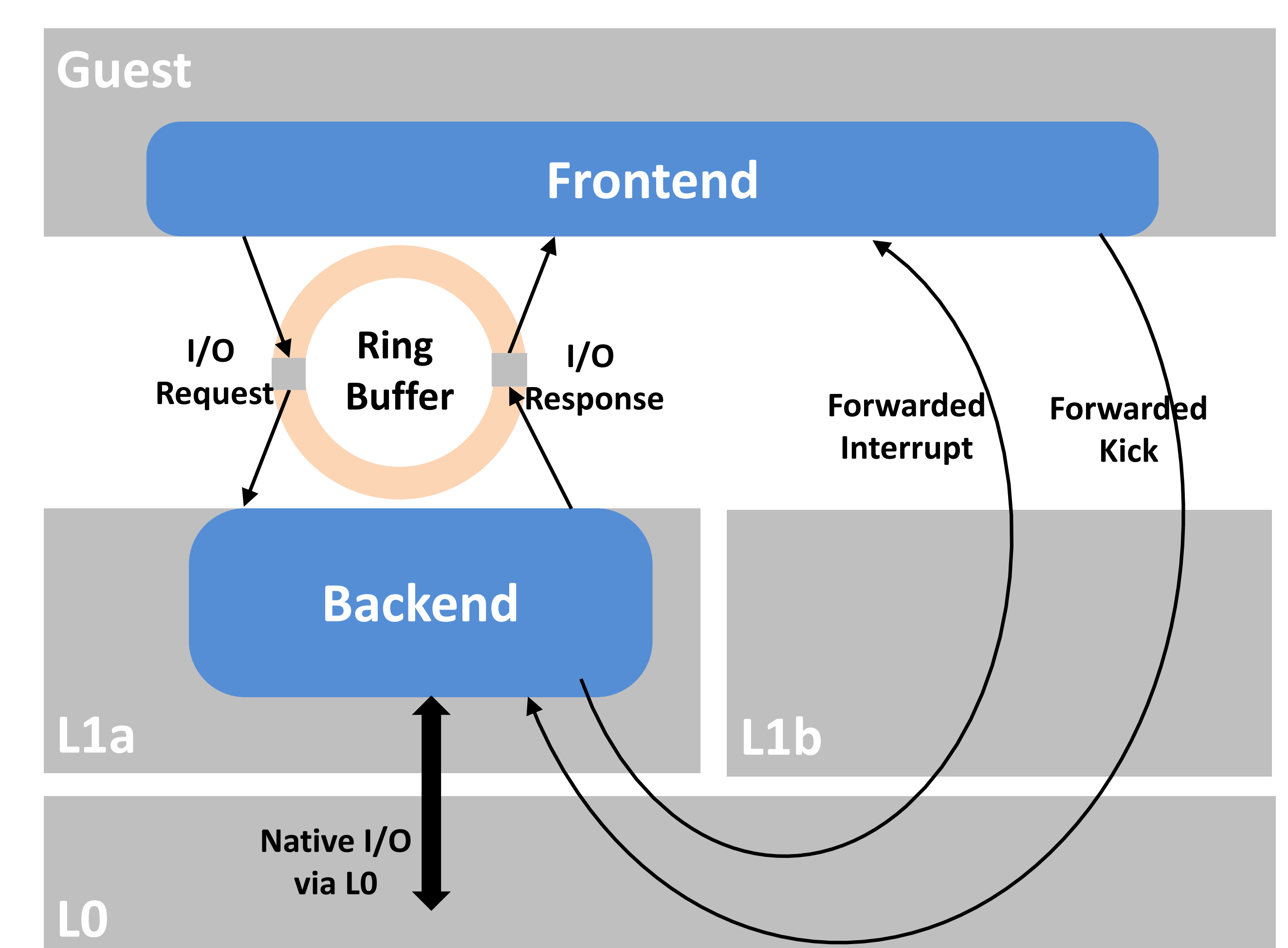
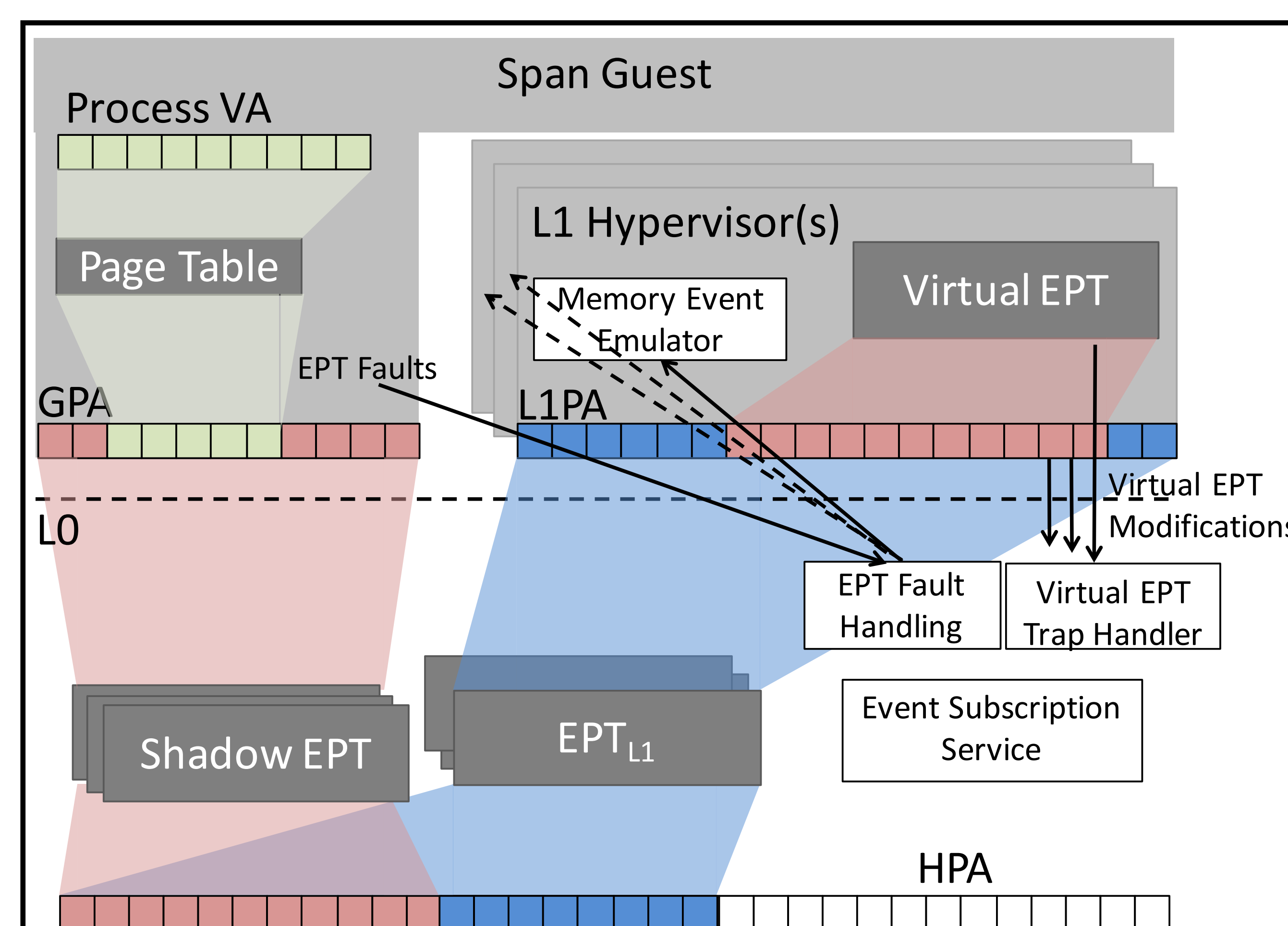
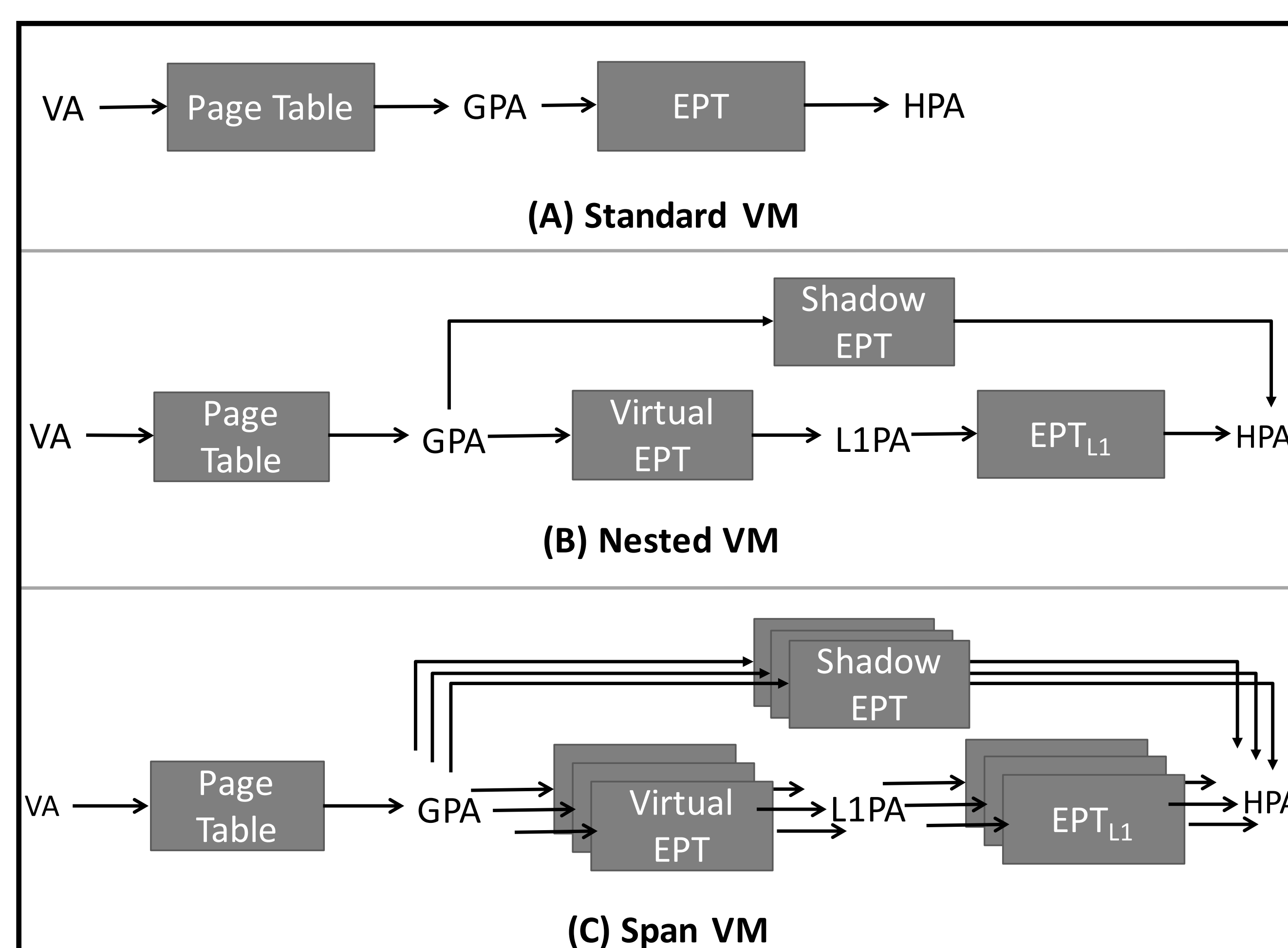
- 1. Growing Number of Hypervisor-level Services:** VM Introspection, Intrusion Detection, High Availability, Live Migration, Live Patching, etc.
- 2. Guests Cannot Simultaneously Use Multiple 3rd-party Services:** E.g. Cross-cloud migration, Customized guest security, Attestation, etc.

Solution: Compartmentalize Services & Share Guest Control



Featurevisors (F) : 3rd-party deprivileged “Hypervisors” providing guest services. **Hyperplexor** : Base L0 hypervisor.

Approach: Transparent and Simultaneous Control of Guest by Multiple L1 Hypervisors



- **Guest Transparent:** No modifications to guest.
- **Attach/Detach L1s to/from guest at runtime:** Partial/full control over guest memory, VCPUs, and I/O devices.
- **Event Subscription:** L1s subscribe to guest events via L0.

Status, Results, and Future Work

- **Key Publications:**
 1. *Multi-hypervisor Virtual Machines: Enabling an Eco-system of Hypervisor-level Services*, **Accepted in USENIX ATC, 2017**
 2. *Enabling Hypervisor-as-a-service Clouds with Ephemeral Virtualization*, **VEE 2016.**
- **Prototype on KVM/QEMU Platform**
 - 0—15% overhead on benchmarks: Kernbench, iperf, quicksort.
 - Ephemeral virtualization: 80ms average switching times
 - Page fault servicing: 3.6—4.2us; Event Redirection: 13-41us.
- **Ongoing/Future Work:**
 - Supporting unmodified L1 hypervisors.
 - Live hypervisor patching.
 - Support on public clouds.

```

nested@spanvm-11a$ sudo tcpdump -q -i br0 -n src 10.128.24.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on br0, link-type EN10MB (Ethernet), capture size 96 bytes
17:29:31.716554 ARP, Request who-has 10.128.0.1 tell 10.128.24.1, length 28
17:29:43.824093 IP 10.128.24.1.22 > 10.128.0.9.48050: tcp 0
17:29:43.829140 IP 10.128.24.1.22 > 10.128.0.9.48050: tcp 0
17:29:43.846370 IP 10.128.24.1.22 > 10.128.0.9.48050: tcp 32
17:29:43.848073 IP 10.128.24.1.22 > 10.128.0.9.48050: tcp 0
17:29:43.849475 IP 10.128.24.1.22 > 10.128.0.9.48050: tcp 252
17:29:43.867730 IP 10.128.24.1.22 > 10.128.0.9.48050: tcp 280
17:29:44.013728 IP 10.128.24.1.22 > 10.128.0.9.48050: tcp 0
17:29:44.014700 IP 10.128.24.1.22 > 10.128.0.9.48050: tcp 0
17:29:44.015604 IP 10.128.24.1.22 > 10.128.0.9.48050: tcp 56

nested@spanvm-11b$
nested@spanvm-11b$ python vol.py -f /mnt/l2dump --profile=LinuxUbuntu
ntu1204x64 plugin name linux psaux | tac | grep evil
Volatility Foundation Volatility Framework 2.4
883 1000 1000 ./evil

nested@spanvm-11b$
nested@spanvm-11b$
nested@spanvm-11b$
nested@spanvm-11b$
nested@spanvm-11b$
nested@spanvm-11b$
nested@spanvm-11b$

l2g@l2g:~$ cat evil.c
main(void)
{
    while(1)
        sleep(1000);
}

l2g@l2g:~$ ./evil &
[1] 883
l2g@l2g:~$ ps -e | grep evil
l2g@l2g:~$
```