



The NIC should be part of the OS.

Pengcheng Xu

ETH Zurich

Switzerland

pengcheng.xu@inf.ethz.ch

Timothy Roscoe

ETH Zurich

Switzerland

troscoe@inf.ethz.ch

Abstract

The network interface adapter (NIC) is a critical component of a cloud server occupying a unique position. Not only is network performance vital to efficient operation of the machine, but unlike compute accelerators like GPUs, the network subsystem must react to unpredictable events like the arrival of a network packet and communicate with the appropriate application end point with minimal latency.

Current approaches to server stacks navigate a trade-off between flexibility, efficiency, and performance: the fastest kernel-bypass approaches dedicate cores to applications, busy-wait on receive queues, etc. while more flexible approaches appropriate to more dynamic workload mixes incur much greater software overhead on the data path.

However, we reject this trade-off, which we ascribe to an arbitrary (and sub-optimal) split in system state between the OS and the NIC. Instead, by exploiting the properties of cache-coherent interconnects and integrating the NIC closely with the OS kernel, we can achieve something surprising: performance for RPC workloads *better than the fastest kernel-bypass approaches* without sacrificing the robustness and dynamic adaptation of kernel-based network subsystems.

CCS Concepts

• **Networks** → **Cloud computing**; • **Software and its engineering** → **Operating systems**; • **Computer systems organization** → *Processors and memory architectures*.

Keywords

Remote procedure calls, Serverless computing, Networking, Smart NICs, Cache coherence

ACM Reference Format:

Pengcheng Xu and Timothy Roscoe. 2025. The NIC should be part of the OS.. In *Workshop on Hot Topics in Operating Systems (HOTOS '25)*, May 14–16, 2025, Banff, AB, Canada. ACM, New York, NY, USA, 7 pages. <https://doi.org/10.1145/3713082.3730388>



This work is licensed under a Creative Commons Attribution 4.0 International License.

HOTOS '25, Banff, AB, Canada

© 2025 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-1475-7/2025/05

<https://doi.org/10.1145/3713082.3730388>

1 Introduction

The NIC is central to the operation of a data center server, responsible for all performance-critical communication with the machine. It differs from other devices in a critical aspect: unpredictable events (packets arriving) happen to it during normal operation. This is in contrast to components like GPUs (to which the OS submits application tasks with relatively predictable behavior) or local storage devices (where the OS issues a request, assuming a response will arrive).

Networking in modern servers is notable for a clear partition of networking state between the OS, application, and NIC: broadly, the NIC holds state for (de)multiplexing flows, while the OS holds state related to scheduling of tasks across cores. This has evolved over many years and modern NICs (including new architectures proposed in research) encode a number of implicit and explicit assumptions about trust, OS design, and applications which we survey in [section 2](#).

Surprisingly, these assumptions are preserved in high-performance kernel-bypass architectures which attempt to bring the NIC closer to the application, or CPU designs which integrate the NIC with the processor cores. These techniques deliver gains in performance, but at the cost of flexibility: bypass generally relies on a relatively fixed assignment of processes to cores and queues together with busy-waiting to achieve higher speeds. This works well for fairly static workloads, but has limited applicability for more dynamic application mixes.

Our focus in this paper is on the network receive path, although it is also closely connected to the transmit path. We also focus on Remote Procedure Calls (RPCs), whether data center microservices or serverless function invocations. While some are large, the great majority of RPC requests and responses are small [\[23\]](#). Our goal is to exploit this insight to reduce the CPU cycle overhead of a small RPC call *to essentially zero* for many workloads, within an architecture that nevertheless supports dynamic workloads with better performance than modern kernel-based stacks.

While the end-to-end latency of RPCs is dominated by propagation time, *end-system latency* reflects CPU cycles consumed by the invocation and is therefore a good measurable proxy for the efficiency of the software stack (unmarshaling, demultiplexing, function dispatch, etc.).

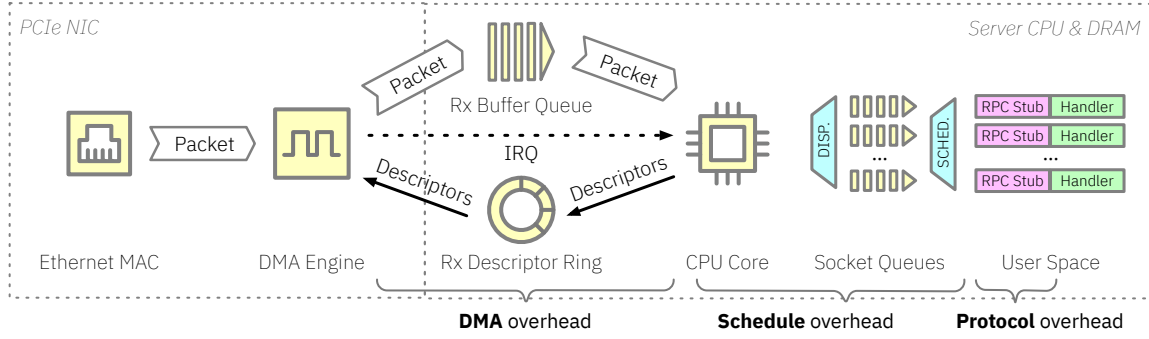


Figure 1: Architecture of a traditional PCIe DMA NIC's receive path.

We suggest that kernel-bypass optimization is at its limit, and argue for a radically different, more OS-centric approach where the NIC is a full, trusted component *of the OS itself*.

Our approach combines several new ideas. First, we exploit *cache-coherent peripheral interconnects* and well-established techniques for protocol offload to transfer data between user-mode CPU registers and the NIC with no memory access overhead and no energy wasted in spinning. Second, we use the same fine-grained mechanism to have the kernel *keep the NIC updated with the current OS scheduling state*, allowing the NIC to always steer packets to the correct user-space process. Finally, the NIC gathers load information and *requests the OS to reschedule processes* in response to new packets arriving over the network, via the same lightweight mechanism.

We explore what this means for hardware and software, and the prototype NIC, LAUBERHORN, that we are building on the Enzian research platform to demonstrate the idea.

2 The traditional NIC paradigm

Most server network stacks, and also most NIC hardware designs, are based around the model in Figure 1: incoming packets are demultiplexed and transferred using Direct Memory Access (DMA) into one of a set of descriptor-based queues, with interrupts used for synchronization when the OS has stopped polling the queue. DMA occurs using addresses that are translated (and protected) via an I/O Memory Management Unit (IOMMU) or System Memory Management Unit (SMMU), and interrupts can be steered to cores using the demultiplexing information, or some other heuristic.

This model has evolved over decades from the very simplistic model of Ethernet interface used in the Xerox Alto, to handle 400Gb/s network links connected to machines with 100s of cores. We discuss recent alternatives below, but observe that most kernel bypass approaches still look like Figure 1, but move some parts from the OS kernel to application user space. In more detail, a minimal set of things have to happen to turn a network packet into a function invocation on the host is:

- (1) Read the packet contents.
- (2) Perform protocol processing (checksums, etc.).
- (3) Demultiplex the packet to an in-memory queue.
- (4) Interrupt some CPU core to notify the OS, hypervisor, or guest OS.
- (5) Perform some general protocol processing.
- (6) Identify the OS process (or thread, or task) that should handle the message.
- (7) Find a (perhaps different) core to execute this process.
- (8) Schedule the process on the core.
- (9) Context switch to the process if needed.
- (10) Unmarshal/deserialize arguments and function name.
- (11) Find the address of the start of the function.
- (12) Jump to this instruction.

A typical NIC performs steps 1 to 4, and then hands things over to the OS or application.

Kernel-bypass approaches like Arrakis [18], IX [3], and Demikernel [24] variously trade off latency and throughput against flexibility and energy efficiency by replacing step 4 with spinning or polling, and simplifying steps 5 through 9 by binding application processes to in-memory queues in advance. The data plane is moved to application space, while the control plane can be left in the OS kernel or moved to dedicated cores (Shinjuku [12], Shenango [17], Caladan [7]) or userspace processes (ghOST [8]). Snap [14], meanwhile, dedicates a subset of the CPU cores to provide applications a uniform, yet highly configurable, abstraction of a NIC that allows rapid deployment of new network stack features.

All these approaches, however, retain the same division of labor between software and the NIC; indeed, all of them resemble Figure 1. The principal differences concern the kernel/user space boundary (and where the different receive path stages execute) and the design of the control plane (which is implemented in software on the CPU as a separate component). To a large extent, kernel bypass turns what was OS functionality into application-level functionality, *integrating the NIC more with the user application*.

Other work from architecture has explored closely **integrating the NIC with the CPU**. nanoPU [10] delivers packets processed by P4 directly into the register file of a RISC-V core, while CC-NIC [22] uses a NUMA server to explore by emulation the implications of cache-coherent peripheral interconnects for NICs. This, again, preserves the same hardware/software boundary, while heavily optimizing hardware steps 3 and 4.

As with bypass, this works well when the workload is relatively static, can be bound to dedicated cores, and is rarely idle. However, when the workload is dynamic with many more end-points than spare cores, the up-front cost of mapping the NIC’s demultiplexing to queues onto the scheduling of applications on cores quickly becomes cumbersome. Even newer Data Processing Unit (DPU) [1] and Infrastructure Processing Unit (IPU) [9] systems share these characteristics.

Moreover, tightly coupling the NIC and CPU may not be desirable: Networking parts do not develop in lock-step with CPUs and different workloads have very different compute-to-network I/O ratios, so there is valuable flexibility gained by keeping the NIC as a separate component.

3 Why this split?

The historical stability of the hardware/software boundary in NICs is arguably due to the state required to perform each step. For example, steps 10–12 require application-specific state: argument formats, interface signatures, and code layout. In contrast, steps 5–9 cannot be performed without reference to central OS state.

A key factor is that **the OS doesn’t trust the NIC**. Kernel developers have been keen to limit the coupling between OS and NIC [16] due to the perception that the NIC never does quite what the OS designer wants. Ironically, the result continues to be an increase of the complexity of device *drivers* as hardware vendors adopt ad-hoc solutions to exposing functionality to users. This in turn means that the functionality that the vendors add to a NIC is limited to *that which can easily be exposed to users*.

Moreover the introduction of IOMMUs and SMMUs has led to a philosophy that, as far as possible the NIC should not be trusted as a device. This is an anomaly, given that devices like disks, CPU cores, GPUs, and DRAM are, for the most part, trusted by at least part of the OS. One reason for this is confusion about different roles of the SMMU: on the one hand, providing a convenient memory translation function on the data path to facilitate device pass-through to virtual machines, and on the other, to firewall off a kernel running on a set of application cores from the rest of the machine.

The philosophy is compounded by protocols like RDMA which regard the NIC as a relatively dumb device with little connection to the host OS that can nevertheless perform

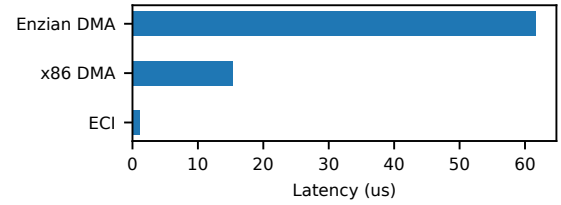


Figure 2: 64-byte message round-trip latencies.

memory accesses on behalf of a remote peer, using an authorization framework that is naive at best in multi-tenant scenarios. A more OS-centric perspective on RDMA-like functionality views the NIC as providing *to the OS* additional, specialized cores close to the network interface which can execute a limited number of RPC operations.

A related factor is that **architecture researchers like to ignore the OS** [15]. User applications are a different matter, and so there are many proposals for accelerating subsets of steps 10–12 for memory latency benefits. Cereal [11] proposed an accelerator targeting a custom message format; the accelerator sits directly on the system interconnect *inside* the CPU package. Optimus Prime [19] proposed a format-agnostic transformation architecture and focused on implementing an accelerator sitting on the system interconnect inside the CPU package as well. Cerebras [20] builds upon Optimus Prime towards a fully-offloading RPC framework. ProtoAcc [13] targets Protocol Buffers instead with an accelerator attached to the custom RoCC [2] interface directly on the RISC-V core pipeline. Like kernel bypass, these primarily target static assignments of applications to cores and accelerate single application performance in part by imposing strong assumptions to minimize steps 5–9.

Underlying this apparent trade-off between performance (static assignment of cores) and flexibility (more OS involvement) is the **misconception that fine-grained interaction between OS and NIC is slow**: the NIC is not just untrustworthy but also hard to talk to. In cases such as Receive-Side Scaling (RSS) the goal is to provide offload (e.g. load balancing) without involving the OS *at all*. This assumption may hold for DMA descriptor rings, but much less so for loads/stores to device registers over modern PCI Express (PCIe), and even less the case when accessing the device over new, cache-coherent interconnects like CXL.mem 3.0.

4 Breaking the impasse

We are pursuing a different approach in order to deliver performance *better than current kernel bypass* for relatively stable RPC and serverless workloads, while providing all the flexibility of the traditional approach with better efficiency for highly dynamic workloads. We exploit three new insights.

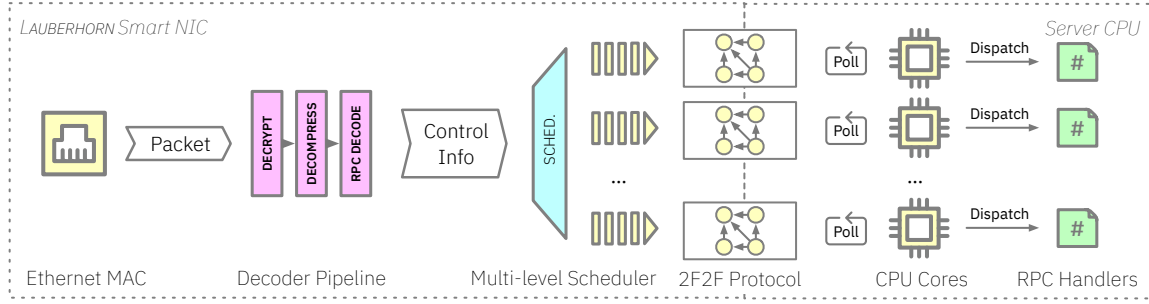


Figure 3: Overview of the LAUBERHORN receive path.

Firstly, new **cache-coherent peripheral interconnects** between devices and cores can radically change communication between CPU and NIC. Examples are CXL.mem 3.0 [6], CCIX [4], and the Enzian Coherence Interface (ECI) [5]. Crucially, this allows lightweight signaling to the device: a NIC can interpret cache operations on certain addresses as specific signals or requests, and return information back to the CPU in response or trigger other actions such as interrupts. Figure 2 shows the dramatically better interaction latency possible using even the (comparatively slow) ECI vs. DMA over PCIe on the same machine, and on a modern PC server; we anticipate comparable gains with CXL 3.0.

For the data plane, such protocols allow packets to be transferred directly as cache lines to the destination core’s L1 cache and registers [21], providing dramatically lower latency than can be achieved using DMA with descriptors.

For the control plane, communication with between CPU cores (running either application code or the OS kernel) is lightweight and efficient, and easily protected using conventional MMU mechanisms. It also conveys rich information, for example, a NIC can infer whether a core is polling in user mode or in kernel mode based on which address is requested from its home address space.

Secondly, **it’s time to trust the NIC**. The NIC is a critical part of the OS function of the machine. Unlike, e.g., the GPU, it is enabling infrastructure for the whole system. Viewing it as a potential part of the OS rather than an untrusted peripheral is the only way to fully exploit its hardware resources and unique position in the data path.

In particular, since the NIC is responsible for demultiplexing an incoming packet to an application end-point, it should have access to all the relevant OS state: which processes are currently in the run queues on which cores, which are currently executing, and which are waiting. Some of this can be inferred from the cache traffic the NIC observes as in the example above, while any other state can be explicitly pushed to the NIC via the interconnect with negligible overhead.

Finally, adopting the previous positions allows us to **fully implement RPC dispatch** on the NIC. Integrating existing

techniques for accelerating deserialization with rich knowledge of the OS state enables RPC dispatch with essentially zero software overhead: in the common case, it is possible to execute *every* step in Section 2 on the NIC, and have a stalled load on a processor core return a carefully prepared cache line with only the information needed to dispatch an RPC: just the arguments and virtual address of the first instruction of the target function to jump to.

Sharing the OS state means that this efficiency is preserved when executing dynamic workloads where statically associating DMA queues, cores, threads, and sockets is not practical: the NIC already has information about whether, and where, a target process is running and can notify either it or the OS accordingly. Moreover, the OS has up-to-date information from LAUBERHORN about which core are polling and where, so as to guide scheduling decisions.

5 Implementation Sketch

We are building a prototype, LAUBERHORN, to demonstrate the feasibility of these ideas on the context of microservices. LAUBERHORN exploits the large FPGA, 100Gb/s interfaces, and cache-coherent interconnect on the Enzian research computer [5]. We sketch two key components of the design: the receive fast path, and the sharing of scheduling state between the OS and NIC; we return to additional, non-functional issues to be addressed in this design in section 6.

5.1 Receive fast path

Figure 3 shows an overview of a minimal receive path, in the case where the receiving process is already executing on at least one core in the system and at least one execution thread of that process is ready to process a request.

LAUBERHORN demultiplexes and unmarshals an incoming RPC request packet using information provided in advance by the OS kernel (and, indirectly, the application service) to give (1) a process and communication end-point, (2) a *code pointer* and *data pointer* inside that process corresponding to the request, and the *call arguments*, corresponding to steps 1-3, 5-6, 10, and 11 in section 2. This can be achieved using

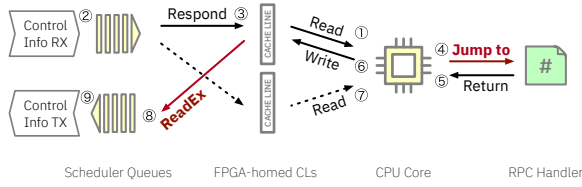


Figure 4: The LAUBERHORN protocol between NIC and CPU

a variation of existing NIC techniques like protocol offload and RPC deserialization acceleration (e.g. [19]).

In the FPGA implementation, an Ethernet frame streams in from the Ethernet MAC IP block and passes through various streaming-mode header decoders to demultiplex the packet and remove the Ethernet, IP, and UDP headers, storing them in SRAM for any upper protocol layers that require buffering.

LAUBERHORN then delivers a minimal data structure to the destination communication end-point which consists of the target code and data pointers, together with the RPC arguments. It does this using an extension of the protocol described by Ruzhanskaia *et al.* [21] (Figure 4). Each end-point comprises a set of cache lines homed on the NIC: two CONTROL lines plus multiple AUXILIARY lines to handle payloads larger than a single cache line (128 B on Enzian). The transmit path uses a similar, disjoint set of cache lines.

To receive a request, a process issues a load to one CONTROL cache line to receive a request. The NIC with respond to this load with the data listed above when an appropriate packet arrives and has been decoded; until then the core is stalled (rather than spinning).

The CPU now has all the information it needs to start executing the first instruction of the user procedure in registers and L1 cache, and is already in the correct address space. It executes the RPC handler and writes the RPC result into the same CONTROL cache line, and loads the second CONTROL line for the next packet. LAUBERHORN sees the load for the second line and thus knows that the CPU has finished serving the first request. Before responding to the read on the second cache line, the NIC issues a *fetch exclusive* over coherence protocol to request the first line (containing the RPC response) from the CPU’s cache and sends it out over the network. Finally, when the next packet arrives and is decoded, LAUBERHORN responds to the CPU’s read on the second CONTROL cache line.

Of course, LAUBERHORN cannot block a cache fill from a core *indefinitely* without a timeout in the coherence protocol causing an unrecoverable “bus error” which leaves the system in an inconsistent state. We avoid this by returning TRYAGAIN dummy messages after 15ms, reducing the polling overhead (both bus traffic and CPU spinning) to almost zero and improving energy efficiency.

Moreover, this provides a mechanism for cleanly descheduling the process: while the OS can still preempt a running process at any time, a core blocked on such a communication load provides a useful synchronization point. LAUBERHORN can notify the OS that the process has blocked, the OS (or the NIC) can send an Inter-Processor Interrupt (IPI) to the process’ core, and then LAUBERHORN can send the process a TRYAGAIN message, unblocking it and causing to immediately enter the kernel.

5.2 Demultiplexing and scheduling

A key novelty of LAUBERHORN is how it uses precise kernel scheduling state to dispatch requests. In the fast case, a request arrives directly at the correct process without kernel intervention, since LAUBERHORN is aware which core is running the process and waiting for a cache line holding the request. Efficiently keeping this state up to date across context switches is practical in part due to the extremely low latency of communication between the CPU and NIC enabled by the interconnect.

When no core is running the destination process for a received packet, LAUBERHORN quickly delivers the request to the kernel, allowing it schedule the target process and deliver the unmarshalled request in software. Figure 5 compares this approach to the traditional Linux dispatch loop.

A CPU core running a regular kernel thread uses the protocol in Section 5 to monitor a pair of CONTROL cache lines for incoming requests; LAUBERHORN can dispatch a request for *any* process to this CPU core and end-point, whereupon the CPU switches to the corresponding process to handle the request. As it is a conventional kernel thread, it periodically calls `schedule()` ③ and can handle regular critical kernel operations like Read-Copy-Update.

Thereafter ① the core remains in the same process and runs a user-mode loop on a *different* pair of CONTROL cache lines which LAUBERHORN has dedicated to that process. At this point, dispatching requests to this service involves almost no software overhead: the load executed by the core immediately returns the address to jump to.

This works well under the assumption that the number of “hot” services is less than the number of available cores – 48 on Enzian, and often in the hundreds for modern server-class processors.

The user-mode loop can give up the CPU in a variety of ways ②. The process can voluntarily yield the CPU by executing a system call whenever it is executing; in the case that the core is blocked on a load of a CONTROL cache line, this will occur when it receives an RPC payload or a TRYAGAIN message from LAUBERHORN. Alternatively, the kernel and LAUBERHORN can cooperate to fully *preempt* the user process by sending an interrupt to the core, and then resuming it

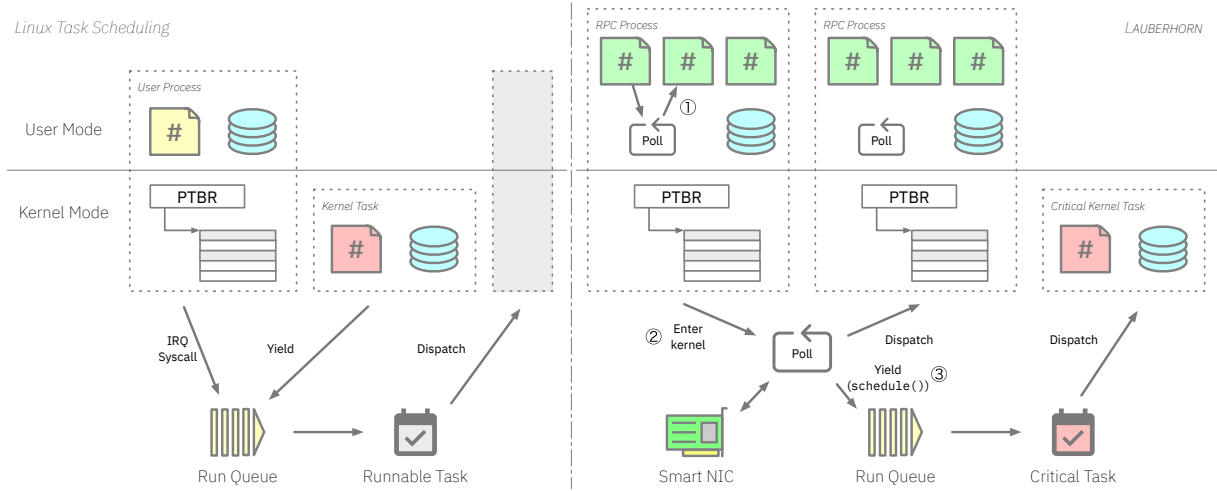


Figure 5: Comparison between normal task scheduling and NIC-driven scheduling of RPC isolation domains.

(allowing it to receive the interrupt) with a subsequent TRYAGAIN as described above. Note that this can be initiated by the kernel scheduler, or by LAUBERHORN based on statistics it gathers about the instantaneous load on each server process. This approach therefore also supports dynamic scaling of the cores used for RPC based on load.

Many data center deployments use non-preemptive kernels for throughput. LAUBERHORN provides dynamic load information to the kernel (using, again, the kernel-mode control channels) to reallocate cores between RPC services and non-RPC processes. Much as we already preempt user-space threads blocked waiting for a cache line, any non-preemptable kernel thread waiting on LAUBERHORN can be reallocated by sending it a RETIRE message from the NIC.

6 Open questions and concerns

The fine-grained concurrent interaction in LAUBERHORN between application threads, OS kernel processes, the cache coherence protocol, and the NIC itself is subtle, and correct operation of the system requires us to ensure that all races are benign. Fortunately, we have found that the problem is highly amenable to specification using TLA+, and can be model-checked for correctness relatively easily.

LAUBERHORN as described so far will support full-featured RPC interaction with high efficiency, but is lacking some non-functional features that become important in real data center settings. While encryption can be handled with fairly standard techniques, support for tracing, debugging, and statistics presents interesting properties for further close integration with the OS.

For large messages, the direct, low-latency approach becomes less efficient and it is best to revert back to DMA-based transfers since throughput comes to dominate over latency.

The trade-off will depend on the platform, empirically for Enzian this happens at about 4KiB.

Nested RPCs will benefit from the ability to rapidly create a dedicated end-point for an RPC reply. Fine-grained interaction with the NIC should make creating this continuation a cheap operation with significant performance benefits.

The design of standard OS-NIC and application-NIC interface is an open question, one which we hope to answer through building LAUBERHORN as a prototype thus evolving the interfaces we provide.

7 Acknowledgements

We thank the anonymous reviewers for their constructive comments on the paper, and the rest of the Enzian team for their support and ideas. This work was partly funded by a gift from the Google Systems Research Group, for which we are grateful.

References

- [1] AMAZON WEB SERVICES. *The Security Design of the AWS Nitro System*, Nov. 2022. <https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html>.
- [2] ASANOVIĆ, K., AVIZIENIS, R., BACHRACH, J., BEAMER, S., BIANCOLIN, D., CELIO, C., COOK, H., DABBELT, D., HAUSER, J., IZRAELEVITZ, A., KARANDIKAR, S., KELLER, B., KIM, D., AND KOENIG, J. The Rocket Chip Generator.
- [3] BELAY, A., PREKAS, G., KLIMOVIC, A., GROSSMAN, S., KOZYRAKIS, C., AND BUGNION, E. Ix: a protected dataplane operating system for high throughput and low latency. In *Proceedings of the 11th USENIX Conference on Operating Systems Design and Implementation (USA, 2014)*, OSDI'14, USENIX Association, p. 49–65.
- [4] CCIX CONSORTIUM AND OTHERS. Cache Coherent Interconnect for Accelerators (CCIX), May 2024.
- [5] COCK, D., RAMDAS, A., SCHWYN, D., GIARDINO, M., TUROWSKI, A.,

- HE, Z., HOSSLE, N., KOROLIJA, D., LICCIARDELLO, M., MARTSENKO, K., ACHERMANN, R., ALONSO, G., AND ROSCOE, T. Enzian: an open, general, CPU/FPGA platform for systems software. In *ASPLOS '22: Proceedings of the Twenty-Seventh International Conference on Architectural Support for Programming Languages and Operating Systems* (February 2022).
- [6] CONSORTIUM, C. Compute Express Link (CXL) version 3.0, Aug. 2022.
- [7] FRIED, J., RUAN, Z., OUSTERHOUT, A., AND BELAY, A. Caladan: Mitigating Interference at Microsecond Timescales. pp. 281–297.
- [8] HUMPHRIES, J. T., NATU, N., CHAUGULE, A., WEISSE, O., RHODEN, B., DON, J., RIZZO, L., ROMBAKH, O., TURNER, P., AND KOZYRAKIS, C. ghOST: Fast & Flexible User-Space Delegation of Linux Scheduling. In *Proceedings of the ACM SIGOPS 28th Symposium on Operating Systems Principles* (Virtual Event Germany, Oct. 2021), ACM, pp. 588–604.
- [9] HUMPHRIES, J. T., NATU, N., KAFFES, K., NOVAKOVIĆ, S., TURNER, P., LEVY, H., CULLER, D., AND KOZYRAKIS, C. Tide: A Split OS Architecture for Control Plane Offloading, Oct. 2024. arXiv:2408.17351.
- [10] IBANEZ, S., MALLERY, A., ARSLAN, S., JEPSEN, T., SHAHBAZ, M., KIM, C., AND MCKEOWN, N. The nanoPU: A Nanosecond Network Stack for Datacenters. pp. 239–256.
- [11] JANG, J., JUNG, S. J., JEONG, S., HEO, J., SHIN, H., HAM, T. J., AND LEE, J. W. A Specialized Architecture for Object Serialization with Applications to Big Data Analytics. In *2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)* (Valencia, Spain, May 2020), IEEE, pp. 322–334.
- [12] KAFFES, K., CHONG, T., HUMPHRIES, J. T., BELAY, A., MAZIÈRES, D., AND KOZYRAKIS, C. Shinjuku: Preemptive Scheduling for {usecond-scale} Tail Latency. pp. 345–360.
- [13] KARANDIKAR, S., LEARY, C., KENNELLY, C., ZHAO, J., PARIMI, D., NIKOLIC, B., ASANOVIC, K., AND RANGANATHAN, P. A Hardware Accelerator for Protocol Buffers. In *MICRO-54: 54th Annual IEEE/ACM International Symposium on Microarchitecture* (Virtual Event Greece, Oct. 2021), ACM, pp. 462–478.
- [14] MARTY, M., DE KRUIJF, M., ADRIAENS, J., ALFELD, C., BAUER, S., CONTAVALLI, C., DALTON, M., DUKKIPATI, N., EVANS, W. C., GRIBBLE, S., KIDD, N., KONONOV, R., KUMAR, G., MAUER, C., MUSICK, E., OLSON, L., RUBOW, E., RYAN, M., SPRINGBORN, K., TURNER, P., VALANCIUS, V., WANG, X., AND VAHDAT, A. Snap: a microkernel approach to host networking. In *Proceedings of the 27th ACM Symposium on Operating Systems Principles* (New York, NY, USA, 2019), SOSP '19, Association for Computing Machinery, p. 399–413.
- [15] MOGUL, J., BAUMANN, A., ROSCOE, T., AND SOARES, L. Mind the Gap: Reconnecting Architecture and OS Research. In *Proceedings of the 13th Workshop on Hot Topics in Operating Systems (HotOS-XIII)* (Napa, CA, USA, May 2011).
- [16] MOGUL, J. C. TCP offload is a dumb idea whose time has come. In *9th Workshop on Hot Topics in Operating Systems (HotOS IX)* (Lihue, HI, May 2003), USENIX Association.
- [17] OUSTERHOUT, A., FRIED, J., BEHRENS, J., BELAY, A., AND BALAKRISHNAN, H. Shenango: Achieving High {CPU} Efficiency for Latency-sensitive Datacenter Workloads. pp. 361–378.
- [18] PETER, S., LI, J., ZHANG, I., PORTS, D. R. K., WOOS, D., KRISHNAMURTHY, A., ANDERSON, T., AND ROSCOE, T. Arrakis: The Operating System is the Control Plane. In *11th Symposium on Operating Systems Design and Implementation (OSDI'14)* (Broomfield, Colorado, USA, October 2014).
- [19] POURHABIBI, A., GUPTA, S., KASSIR, H., SUTHERLAND, M., TIAN, Z., DRUMOND, M. P., FALSAFI, B., AND KOCH, C. Optimus Prime: Accelerating Data Transformation in Servers. In *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems* (Lausanne Switzerland, Mar. 2020), ACM, pp. 1203–1216.
- [20] POURHABIBI, A., SUTHERLAND, M., DAGLIS, A., AND FALSAFI, B. Cerebros: Evading the RPC Tax in Datacenters. In *MICRO-54: 54th Annual IEEE/ACM International Symposium on Microarchitecture* (Virtual Event Greece, Oct. 2021), ACM, pp. 407–420.
- [21] RUZHANSKAIA, A., XU, P., COCK, D., AND ROSCOE, T. Rethinking Programmed I/O for Fast Devices, Cheap Cores, and Coherent Interconnects, Sept. 2024. arXiv:2409.08141 [cs].
- [22] SCHUH, H. N., KRISHNAMURTHY, A., CULLER, D., LEVY, H. M., RIZZO, L., KHAN, S., AND STEPHENS, B. E. CC-NIC: a Cache-Coherent Interface to the NIC. In *Proceedings of the 29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 1* (La Jolla CA USA, Apr. 2024), ACM, pp. 52–68.
- [23] SEEMAKHUP, K., STEPHENS, B. E., KHAN, S., LIU, S., WASSEL, H., YEGANEH, S. H., SNOEREN, A. C., KRISHNAMURTHY, A., CULLER, D. E., AND LEVY, H. M. A Cloud-Scale Characterization of Remote Procedure Calls. In *Proceedings of the 29th Symposium on Operating Systems Principles* (Koblenz Germany, Oct. 2023), ACM, pp. 498–514.
- [24] ZHANG, I., RAYBUCK, A., PATEL, P., OLYNYK, K., NELSON, J., LEIJA, O. S. N., MARTINEZ, A., LIU, J., SIMPSON, A. K., JAYAKAR, S., PENNA, P. H., DEMOULIN, M., CHOUDHURY, P., AND BADAM, A. The Demikernel Datapath OS Architecture for Microsecond-scale Datacenter Systems. In *Proceedings of the ACM SIGOPS 28th Symposium on Operating Systems Principles* (Virtual Event Germany, Oct. 2021), ACM, pp. 195–211.