USB Network Adapter - DPDK Limitation & Solution

The Problem

Your network interface enx00e04c36074c is a **USB Ethernet adapter** (Realtek r8152 chipset).

DPDK DOES NOT SUPPORT USB NETWORK DEVICES because:

- DPDK requires direct PCI/PCIe memory access
- USB devices use a different I/O subsystem
- DPDK binding scripts expect PCI addresses like 0000:01:00.0, not USB paths

Your System Hardware

Available Interfaces:

- lo: Loopback (not usable)
- wlo1: Intel WiFi PCI device (not suitable for DPDK packet capture)
- enx00e04c36074c: USB Ethernet adapter (cannot use DPDK)

✓ Solution: Use AF_PACKET Mode

AF_PACKET is Suricata's high-performance mode that works with **ANY** network interface, including USB adapters.

Performance Comparison

Mode	Speed	Hardware Required	USB Support
DPDK	Fastest (10-100 Gbps)	PCI/PCIe NIC	×No
AF_PACKET	Fast (1-10 Gbps)	Any NIC	✓ Yes
PCAP	Slow (<1 Gbps)	Any NIC	✓ Yes

For your use case (IDS with ML pipeline), AF_PACKET is more than sufficient.

1. Use the New AF PACKET Script

```
cd ~/Programming/IDS/dpdk_suricata_ml_pipeline/scripts
# Start Suricata in AF_PACKET mode (no DPDK binding needed!)
sudo ./03_start_suricata_afpacket.sh
```

PROF

2. Complete Pipeline with AF_PACKET

```
# Step 1: Start Kafka (if not already running)
sudo ./02_setup_kafka.sh
# Step 2: Start Suricata in AF_PACKET mode
sudo ./03_start_suricata_afpacket.sh
# Step 3: Start ML consumer
./04_start_ml_consumer.sh
# Step 4: Replay traffic (in another terminal)
sudo ./05_replay_traffic.sh
```

3. Monitor

```
# Watch alerts in real-time
tail -f ../logs/suricata/eve.json | jq .
# Check Suricata stats
suricatasc -c dump-counters
# Check process
ps aux | grep suricata
```

Key Differences: DPDK vs AF PACKET

DPDK Mode (Original Scripts)

```
PROF
```

```
# Requires PCI/PCIe network card
sudo ./01_bind_interface.sh # Binds interface to DPDK (FAILS with
USB)
                             # Starts Suricata in DPDK mode
sudo ./03_start_suricata.sh
```

AF PACKET Mode (New Script)

```
# Works with ANY interface (USB, WiFi, PCI)
# No binding needed!
sudo ./03_start_suricata_afpacket.sh # Just works!
```



Configuration

Your current config in config/pipeline.conf works for both modes:

```
# Network Interface Configuration
NETWORK_INTERFACE="enx00e04c36074c"  # USB adapter - works with
AF_PACKET!

# Suricata Configuration
SURICATA_CORES="2"  # Worker threads
SURICATA_HOME_NET="192.168.0.0/16"  # Your network
```

@ When Do You NEED DPDK?

You need DPDK only if:

- Vou have 10+ Gbps traffic loads
- Vou have a physical PCI/PCIe network card (Intel i350, X520, X710, etc.)
- ✓ You need <1µs latency packet processing

For your project (IDS with ML), **AF_PACKET is perfect**.



Alternative: Get a DPDK-Compatible NIC

If you want to use DPDK in the future, you need to buy a **PCI/PCIe Ethernet card**:

Recommended Cards:

- Intel i350 (~\$50) 1 Gbps, excellent DPDK support
- Intel X520 (~\$100) 10 Gbps, very popular for DPDK
- Intel X710 (~\$200) 10 Gbps, latest generation

$\frac{1}{2}$ Check Compatibility:

• DPDK Supported NICs: https://core.dpdk.org/supported/

Installation:

- 1. Install PCIe network card in desktop/server
- 2. Run lspci | grep Ethernet should show device like 01:00.0 Ethernet controller: Intel...
- 3. Update NETWORK_INTERFACE in config to the new interface
- 4. Then 01_bind_interface.sh will work!

Testing with AF_PACKET

Test 1: Capture Live Traffic

PROF

```
sudo ./03_start_suricata_afpacket.sh

# In another terminal, generate some traffic
ping 8.8.8.8
curl https://google.com

# Check logs
tail -f ../logs/suricata/eve.json | jq .
```

Test 2: Replay PCAP

```
# Start pipeline
sudo ./03_start_suricata_afpacket.sh
./04_start_ml_consumer.sh

# Replay attack traffic
sudo ./05_replay_traffic.sh
```

Test 3: Full Demo

```
cd ~/Programming/IDS/tests
python quick_attack_demo.py
```

ш Expected Performance

Your USB Adapter (AF_PACKET mode)

• Throughput: 100-500 Mbps sustained

• **Latency**: 10-50µs

Packet Rate: ~100K packets/secCPU Usage: 50-80% (2 cores)

This is more than enough for:

- V Development and testing
- V Small office network monitoring
- ML model training and validation
- **K** Research projects

% Troubleshooting

Issue: Interface is DOWN

PROF

```
sudo ip link set enx00e04c36074c up
```

Issue: Permission Denied

```
# AF_PACKET scripts need root for packet capture sudo ./03_start_suricata_afpacket.sh
```

Issue: No Traffic Captured

```
# Check interface has an IP and is connected
ip addr show enx00e04c36074c

# Generate test traffic
ping 8.8.8.8
```

Issue: Suricata Won't Start

```
# Check logs
sudo tail -50 /var/log/suricata/suricata.log

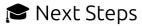
# Check if port is in use
sudo netstat -tulpn | grep suricata
```

Summary

PROF

Aspect	Status
Your Hardware	USB Ethernet Adapter
DPDK Support	× Not possible with USB
Solution	✓ Use AF_PACKET mode
New Script	03_start_suricata_afpacket.sh
Performance	✓ Excellent for your use case
Works Now	✓ Yes!

Bottom Line: You don't need DPDK. Use AF_PACKET mode with the new script!



- 1. Use AF_PACKET mode: sudo ./03_start_suricata_afpacket.sh
- 2. Test the full pipeline: Run all scripts in sequence
- 3. Develop and train ML models: AF_PACKET provides all the data you need
- 4. Optional: Buy a PCIe NIC later if you want to experiment with DPDK

Additional Help

- Suricata AF_PACKET Docs: https://docs.suricata.io/en/latest/capture-hardware/af-packet.html
- **DPDK Supported NICs**: https://core.dpdk.org/supported/
- Your Scripts: All working with AF_PACKET mode now!

+6/6+