Fast Path Direct Cable Replay Guide (Windows → Linux DPDK Suricata)

Goal: Send CICIDS2017 (or any) PCAP from a Windows laptop directly over an Ethernet cable to the DPDK-bound NIC on the IDS with the fewest prep steps.

1. Physical Setup

- Direct Ethernet cable (modern NICs auto-MDI/MDIX; no crossover needed).
- Only two hosts: Windows (replay) → Linux IDS (DPDK NIC). No IP config required.

2. On Linux (Before Binding NIC to DPDK)

Identify target interface (example: eth1).

```
ip link show eth1 | grep ether
# Example output: ether 3c:fd:fe:12:34:56
```

Record: DPDK_NIC_MAC = 3c:fd:fe:12:34:56

(Optional) Verify link partner later with: ethtool eth1 (before binding).

3. Rewrite Only Destination MAC (Recommended Minimal Change)

Do this on Linux (faster tooling). Keep everything else untouched.

```
# Install tools if needed
sudo apt install -y tcpreplay
# Rewrite destination MAC only
tcprewrite \
  --infile=CICIDS2017.pcap \
  --outfile=CICIDS2017_fastpath.pcap \
  --enet-dmac=3c:fd:fe:12:34:56
```

PROF

If original source MAC looks odd (virtual), you may optionally set a simple one:

```
tcprewrite --infile=CICIDS2017.pcap --outfile=CICIDS2017_fastpath.pcap \
  --enet-dmac=3c:fd:fe:12:34:56 --enet-smac=02:11:22:33:44:55
```

(Do NOT remap IPs in fast path; Suricata will still parse flows.)

4. Transfer Rewritten PCAP to Windows

Methods: USB, SMB share, scp to WSL, etc.

5. Start Suricata in DPDK Mode on Linux

Bind interface and launch (adjust script names if different).

```
cd /home/sujay/Programming/IDS/dpdk_suricata_ml_pipeline
sudo ./scripts/01_bind_interface.sh eth1
sudo ./scripts/03_start_suricata.sh
```

Confirm it is running:

```
ps -ef | grep suricata
tail -f logs/suricata.log
```

6. Start ML + Kafka Consumers (If Not Auto-Started)

```
./scripts/02_setup_kafka.sh
source venv/bin/activate
python src/ml_kafka_consumer.py --config config/pipeline.conf
```

7. Replay PCAP From Windows (Simplest Tools)

Option A: Colasoft Packet Player

- Install Npcap (in WinPcap compatible mode).
- Open CICIDS2017_fastpath.pcap → Select NIC → Set speed = e.g. 100 Mbps initially → Play.

Option B: Ostinato

- Add port → Import pcap → Assign stream → Set rate (pps or Mbps) → Start.

PROF

Option C (Power user): WSL + tcpreplay (ensure raw socket allowed)

```
# In elevated PowerShell (once):
wsl --install   # if needed
# Inside WSL:
sudo apt update && sudo apt install -y tcpreplay
# Find Windows NIC name mapping may not expose raw send; prefer native
tool.
```

8. Scale Rate

Start low (100 Mbps), observe no drops, then increase:

- 250 Mbps

- 500 Mbps
- Near line rate (1 Gbps topspeed)

9. Verify Ingestion

Suricata counters (new flows rising):

```
jq '.flow | {tcp,udp,icmp}' /var/run/suricata/counters | head
```

(Or if custom path: logs/stats.json periodically)

Kafka topics:

```
kafka-console-consumer.sh --bootstrap-server localhost:9092 --topic
suricata-alerts --from-beginning --max-messages 5
kafka-console-consumer.sh --bootstrap-server localhost:9092 --topic ml-
predictions --from-beginning --max-messages 5
```

ML output:

```
tail -f logs/ml_predictions.log
```

10. Stop / Reset

```
sudo pkill suricata
sudo ./scripts/unbind_interface.sh eth1   # if you have such a script
```

PROF

Minimal Troubleshooting

Symptom	Likely Cause	Fast Fix
Zero packets	Wrong dest MAC	Re-check tcprewrite MAC
Some packets, no flows	Suricata not fully started	Check suricata.log ready message
High packet drops	Rate too high initially	Lower replay Mbps
ML silent	Consumer not running	Restart ml_kafka_consumer.py
Kafka empty	eve-kafka not enabled	Verify suricata.yaml DPDK + eve output

Check Suricata log for DPDK port stats lines (RX increasing).

Optional Faster Hack (Skip Rewrite)

If you enable promiscuous mode (depends on your Suricata DPDK config), you can replay unmodified PCAP:

- Set in suricata.yaml (dpdk / promisc: yes)
- Less deterministic; preferred only for quick inspection.

Summary Fast Path Sequence

1. Get NIC MAC (eth1)
2. tcprewrite destination MAC only
3. Bind interface → start Suricata DPDK
4. Start Kafka + ML consumer
5. Replay pcap from Windows at moderate rate
6. Observe flow + prediction topics
7. Increase rate as needed

Need a version suitable to append to PRODUCTION_DPDK_GUIDE.md? Ask and it can be formatted for insertion.