“Silence is a source of great strength.” — Lao Tzu

沉默是力量
的源泉
— 老子

Building a Low-Cost Unidirectional File Transfer System

With A Custom Data Diode and Special TFTP Implementation

Presenter: *Douglas Mun*   Date: *14 Aug 2025*

Key points for today’s sharing

“When Silence is a feature not a bug.”

1. Why One-Way?
The *real* threat landscape

2. The Core Idea:
A simple protocol, reimagined for a silent world.

3. The Physical, Network and Protocol Layers:
Light for security, fixing the ARP and killing ACKs to keep data alive.

“沉默是一种功能，
而不是故障。”

SCAN ME

Why One-Way? The *real* threat landscape

Security by Physics, Not Policy

Trust no one. Not even your own network.

Problem: Firewalls can fail. Physical air-gap is better—but how to move data safely?

Solution: Data Diode—hardware-enforced one-way channel.

Application	**Risk Mitigated**
OT/SCADA Log Shipping	Prevents ransomware from jumping from IT to OT
Immutable Backups	Ransomware can’t encrypt what it can’t reach
Intelligence Ingestion	Classified networks receive updates safely

Innovation Angle: Not just a tool—it’s a philosophy of data flow.

Custom Physical Data Diode

Security at Layer 1: When Light Enforces Trust.

Solution: Data Diode, a hardware-enforced one-way channel.

```
[Sender PC Ethernet]
       ↓
[Media Converter](TX) → [Fibre Cable] → (RX)[Media Converter]
                                                ↓
                                         [Receiver PC Ethernet]
```

Data Flow: Arrow is one-way only, no light path back.
Receiver Media Converter: TX fibre port disconnected.
UDP Protocol: Custom TFTP with no ACKs. Immune to protocol exploits.

Innovation Angle: Use a single-mode SC fibre cable over a media converter.

The Networking Challenge

The Static ARP Trick: The Magic of Pre-Knowledge.

Analogy: A teacher shouting into a soundproof room — no feedback, no visibility.

```
There are minimum two Networking Challenges to overcome:

 | Layer          | Problem                 | Consequence                   |
 +----------------+-------------------------+-------------------------------+
 | L2 (Data Link) | ARP requires a reply    | Sender can’t resolve MAC addr |
 | L4 (Transport) | TFTP expects ACKs       | Transfer stalls after 1st blk |
```

Assumptions: Receiver is ready listening. Just keep sending.

The Protocol Layers: Fixing the ARP paradox

The Networking Challenge (cont)

The Silence Problem: Designing for a Deaf Receiver.

The Shouting Sender over ARP:

Sender: “Who has 192.168.1.100?”
Receiver: (silent)
Sender: “No one answered. Giving up.”

```
Fixed via adding a static ARP entry on the Sender PC:
  arp -s 192.168.1.100 00:0A:95:9D:68:16

Benefits:
  Bypasses ARP request
  Hard Coded MAC address
  Prevents ARP spoofing
```

Insight: We’re not discovering the network—we’re declaring it.

The Core Idea: A simple protocol, reimagined for a silent world

Why TFTP over UDP? Not TCP & FTP

Trivial File Transfer Protocol (TFTP) is the Perfect Minimalist Protocol

Why Not TCP?

TCP needs 3-way handshake

Receiver can’t respond → connection fails

UDP:

No handshake

Fire-and-forget → ideal for one-way

TFTP:

Simple block structure

Easy to code

Conclusion: TFTP is simple hence an ideal file transfer protocol over a one-way link.

Standard TFTP PUT flow

The Postcard Protocol with a Receipt System.

TCP: Like a phone call—handshakes, flow control.
UDP: Like a postcard—no guarantee of arrival.

```
TFTP uses ACKs to simulate reliability.

Sender                   Receiver
  | - WRQ (file.txt) ->   |
  | <- ACK (block 0) -    |
  | - DATA (block 1) ->   |
  | <- ACK (block 1) -    |
  | - DATA (block 2) ->   |

Fatal Flaw: Every send requires a reply. No replies = no transfer.
```

Conclusion: TFTP fails on a one-way link. But works once the dependency is removed.

Special TFTP PUT flow

The Opera Artist with an Audience that Never Applauds

One-way TFTP without ACKs.

```
Sender                    Receiver
  | - WRQ (file.txt) ->   |
  | - DATA (block 1) ->   |
  | - DATA (block 2) ->   |
  | - DATA (block n) ->   |
```

Sender uses timing delays between sending packets to ensure the best chance of packet being received.

Receiver flush DATA to disk immediately to ensure the buffer doesn't overflows, leading to data loss.

Sender: Controlled Firehose: The 5ms Rule.

```
Start → Read Input File → Send WRQ → Wait 10ms
Loop:
  Read 512 bytes → Send DATA → Sleep 5ms
  If <512 bytes → Last block → Break
Close
```

Receiver: Write Now, Ask Never: The Philosophy of Resilience.

```
Start → listen → Parse WRQ → Write Output File
Loop:
  Recv DATA
  Write DATA to file → Flush file to disk
  Last block → Clean-up
Close
```

The Core Idea: A simple protocol, reimagined for a silent world

Breaking Assumption & Reflections

Lessons from building a Custom Data Diode and Special TFTP Implementation

We assumed networks were conversational but an one-way broadcast channel is possible.

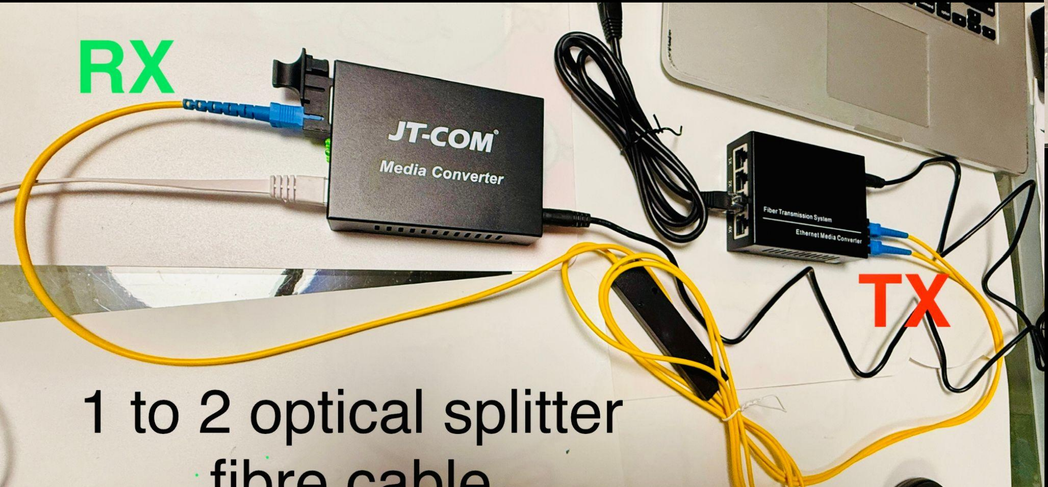
```
Limitations for future work:
  No error correction
  No Auth/Encryption Manual ARP setup
  No congestion control

Reflections:
  Security can be physical
  Reliability doesn’t need replies
  Timing replaces ACKs
```

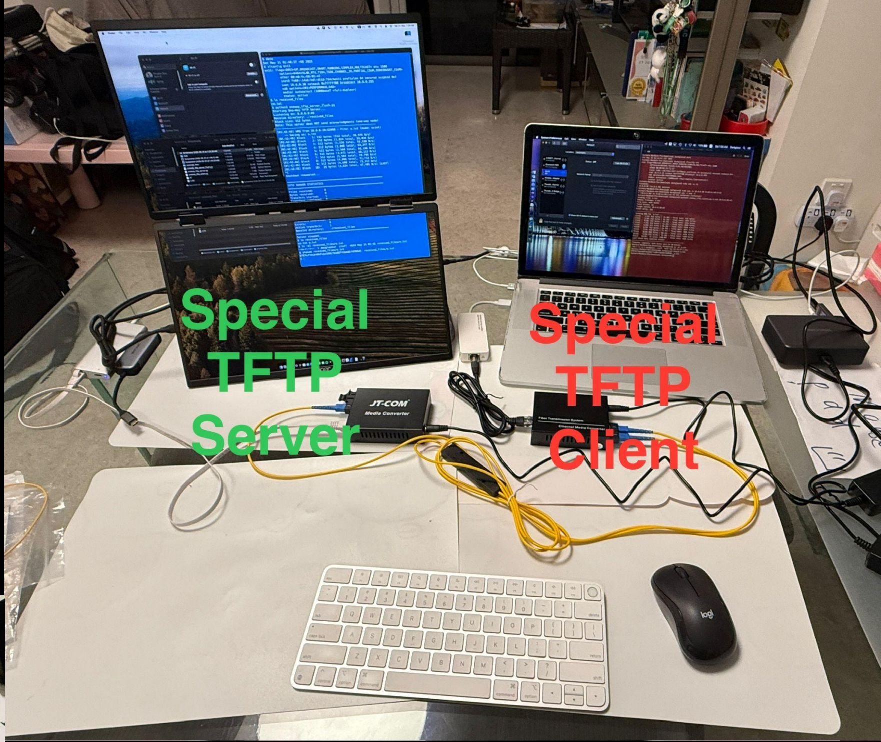
Final Thought: Sometimes, the most powerful thing a system can do is say nothing at all.

Demo Time

Let’s Explore to Learn and Grow Together



1 to 2 optical splitter fibre cable



"Those who know do not speak; those who speak do not know." — Lao Tzu

知者不言，
言者不知。
— 老子

Thank you for your support!

For feedback & presentation material: douglas_mun@csa.gov.sg