

# Wireshark Developer and User Conference

## A-7: Have Wireshark – Will Travel

Wednesday June 15, 2011. 1:15pm – 2:45pm

**Jasper Bongertz**

Senior Consultant | Fast Lane Institute for Knowledge Transfer

**SHARKFEST '11**

Stanford University

June 13-16, 2011

# Agenda

- Wireshark configuration
- At the customer site...
- Preparing captures
- Case files
- Lessons learned



# Wireshark Configuration

- Column configuration
  - No, Source, Destination, Protocol, Info, Size, Cumulative Bytes
  - Delta Time Displayed, Relative Time, Absolute Time
  - others, depending on the task (SMB handles...)
- TCP decode settings
  - No stream reassembly by default
  - Relative Sequence numbers, Track bytes in flight
- Color settings
  - Set to indicate interesting stuff



# At the customer site...

It's an adventure.

# At the customer site...

- Strange expectations
  - „Capture? Can't you just add a route to fix it?“
- „Problematic“ network diagrams (if any, and if you can call it a diagram at all)
- Determining capture points
  - „We have no idea where THAT server is...“
- Fun with corporate security
  - „We installed fingerprint readers just this morning. It's a little difficult to get inside the datacenter.“
  - „Hi, meet our IT risk officer“

# Network Diagram? Here you go...



# Preparing captures


- Wonderful network devices from the early to late 1990s
  - „Oh, cute, a 10MBit hub...” (in 2007)
- TAP trouble
  - CRC errors caused by Aggregation TAP
  - No link on analyzer ports while production works fine (fiber optical tap)
- Inline capture trouble
  - Or: where NOT to place Reset buttons on a capture device

# Preparing captures

- Customer admins and the challenge to configure SPAN ports
  - „SPAN port? What is a SPAN port???”
  - „I have neither IP nor login for THAT switch“
- Fun with switches
  - 3COM: SPAN port vs. STP
  - D-LINK: 1-to-23 SPAN option
  - D-LINK: running in factory default configuration
- Bogus problem reports
  - „My printer takes ages to print a page“



# Next up...



**...some of our  
adventures in  
the world of doing  
network analysis**

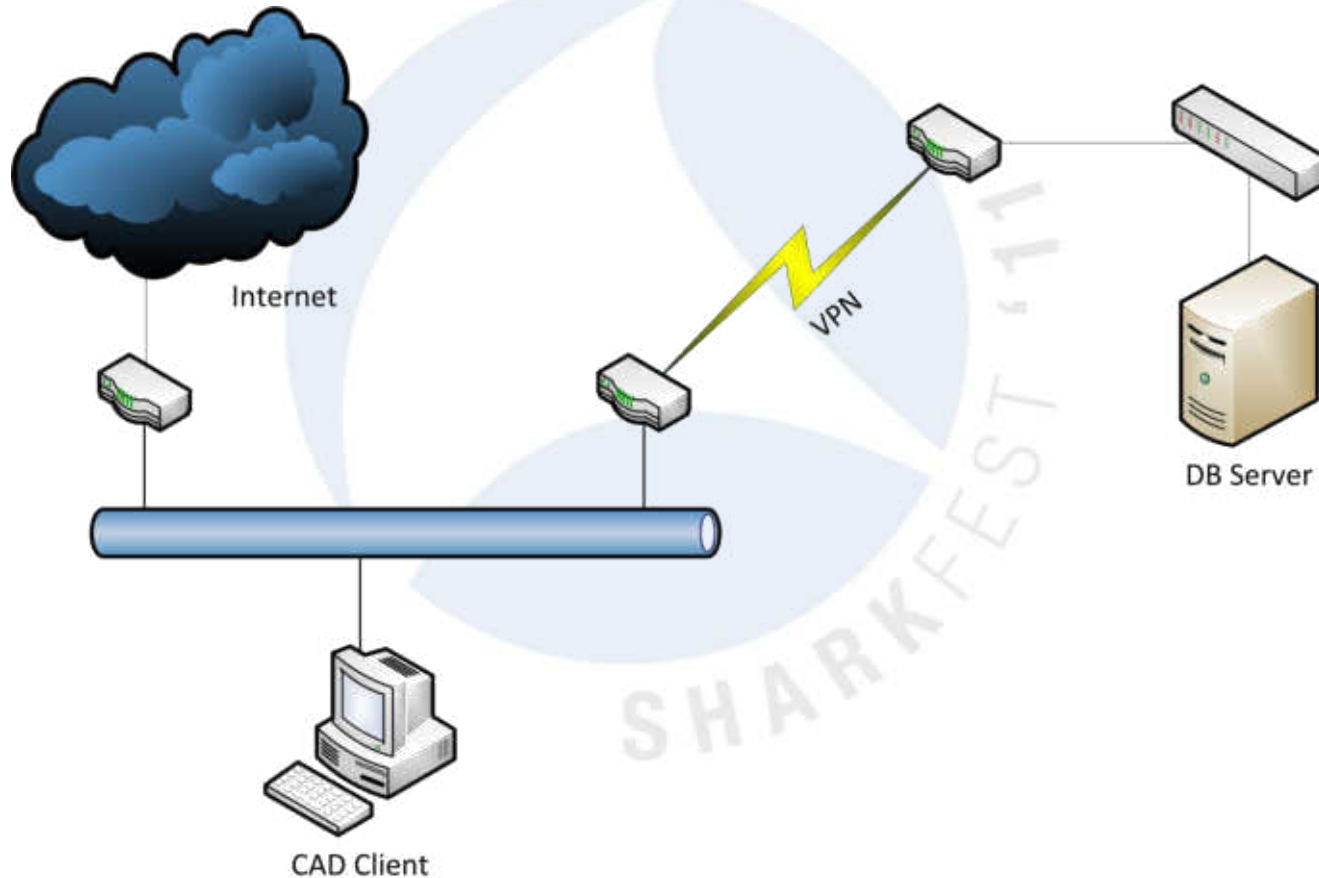


# Lost without a Trace

A couple of projects of which I don't have the  
trace files anymore...

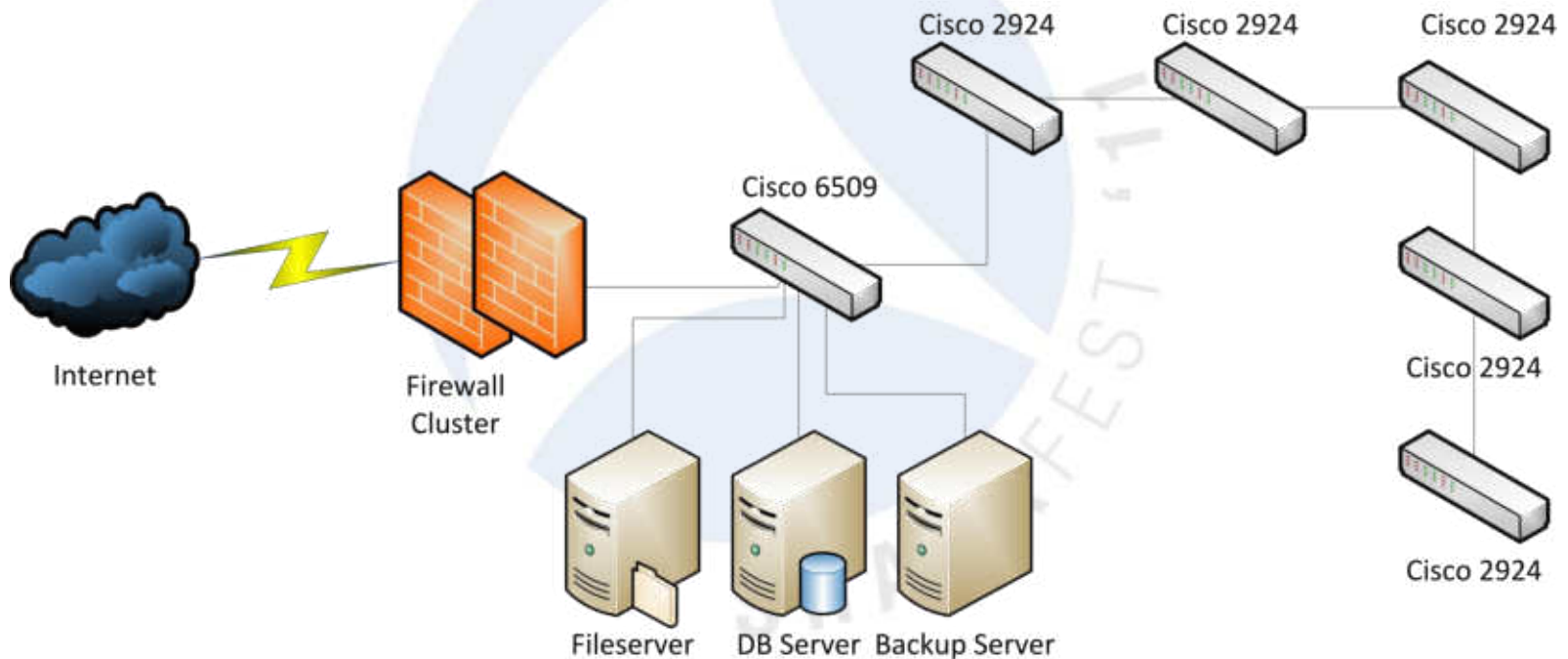
# The lazy network admin

- Customer had several offices, one showing slow loading times for CAD drawings



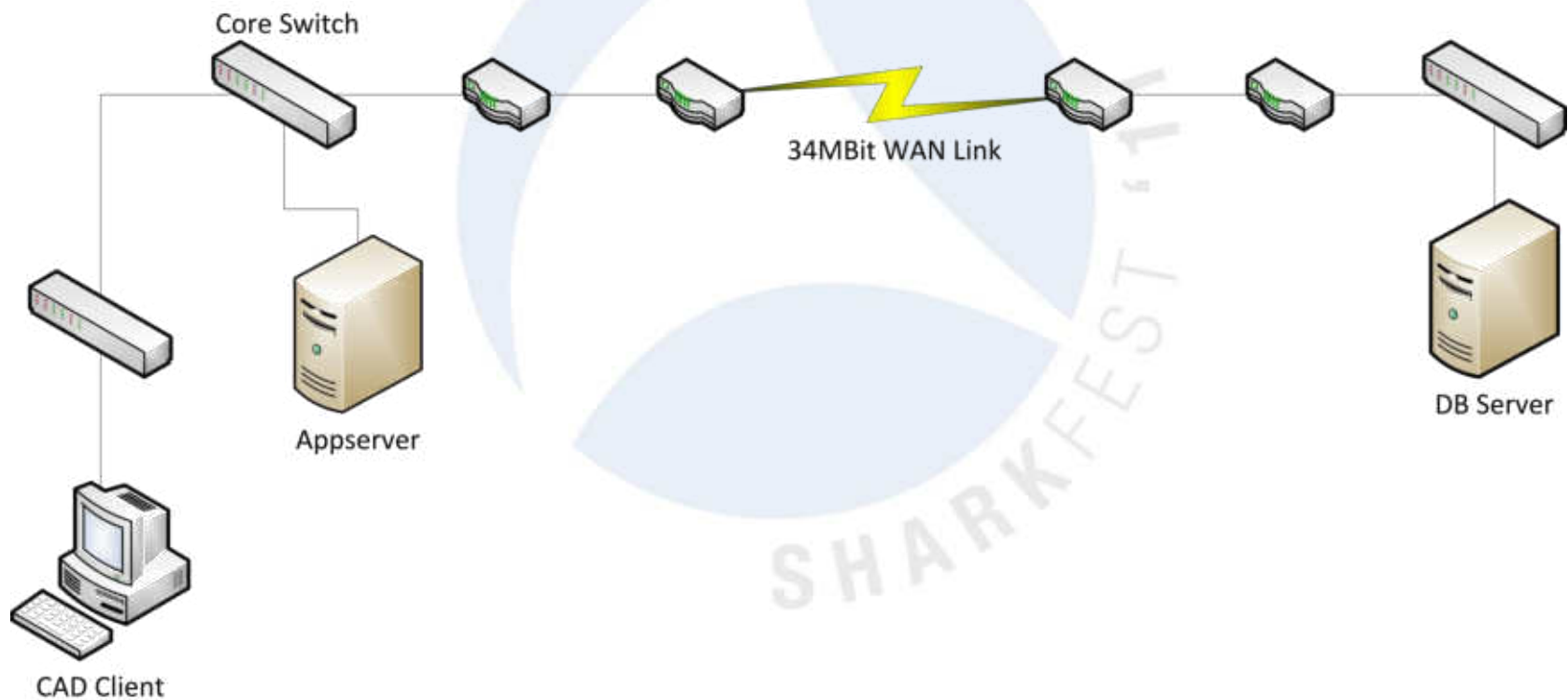
# The random traffic spike

- Diagrams showed massive random traffic spikes on ALL internal interfaces at the same time



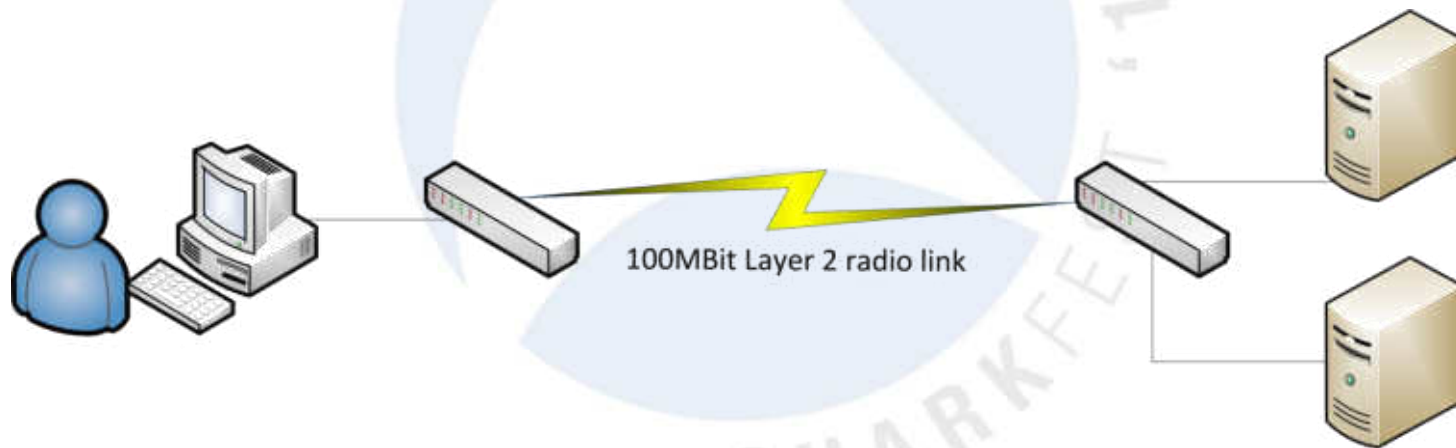
# The unfortunate server move

- Customer moved a DB server to another location, and users started complaining
  - „I tried FTP, it runs perfectly fine...“



# Network bad, admin worse

- Two remote hospital buildings, connected through a 100MBit radio link.
- Most Users losing connectivity every now and then, at the same time, on both sides



# Case files with trace files

Anonymized, of course.

# Firewall trouble

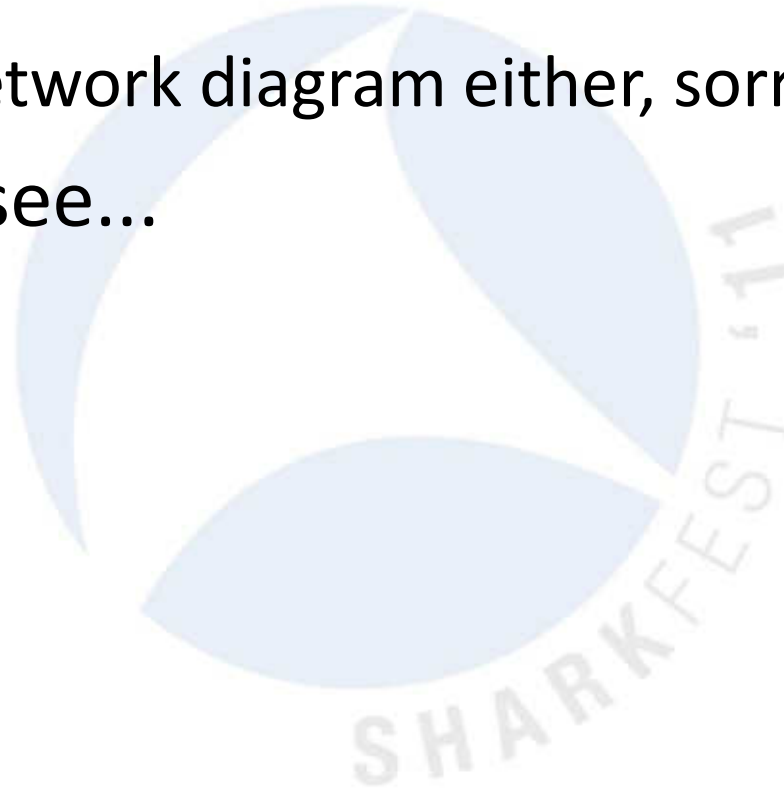
- Customer calls, saying he's being attacked
- Firewall blocks tons of valid connections
  - Attacks appearantly stop at night
- Network capture under stress
- Sorry, no network diagram
- Lets take a look...





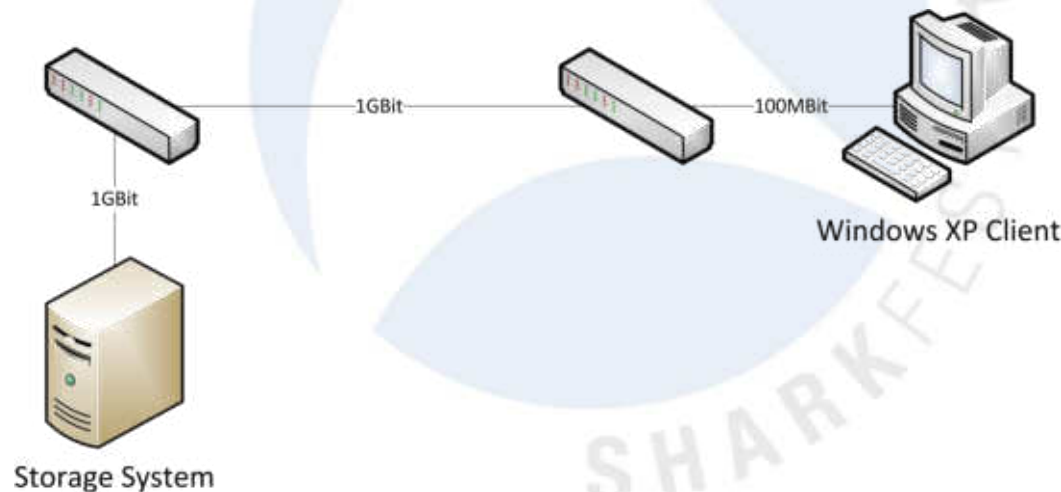
# Network takedown

- Customer calls, saying he's being attacked
  - No, it's not the same customer.
  - No, no network diagram either, sorry 😊
- Okay, lets see...



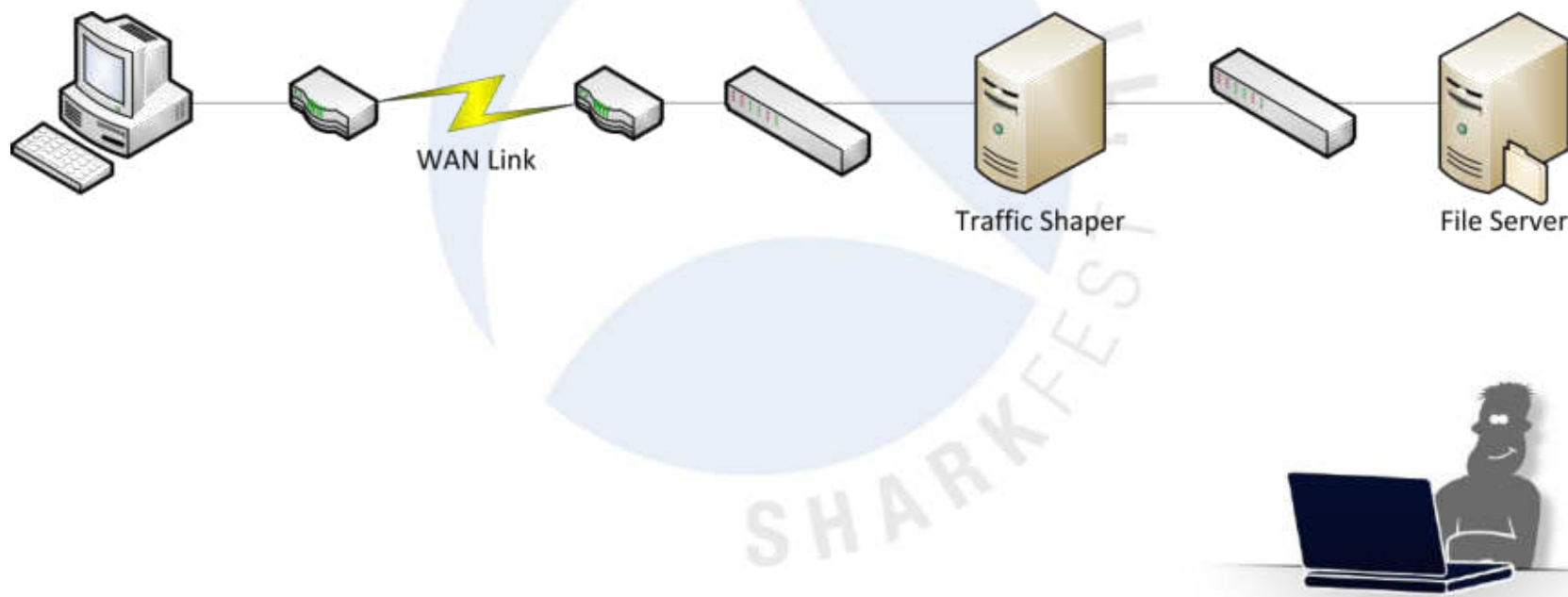
# The slow fast download

- Customer has very slow download speeds from a very fast filer to user locations
  - Of course, going from 1GBit to 100MBit, but the resulting speed was about 5MBit/s



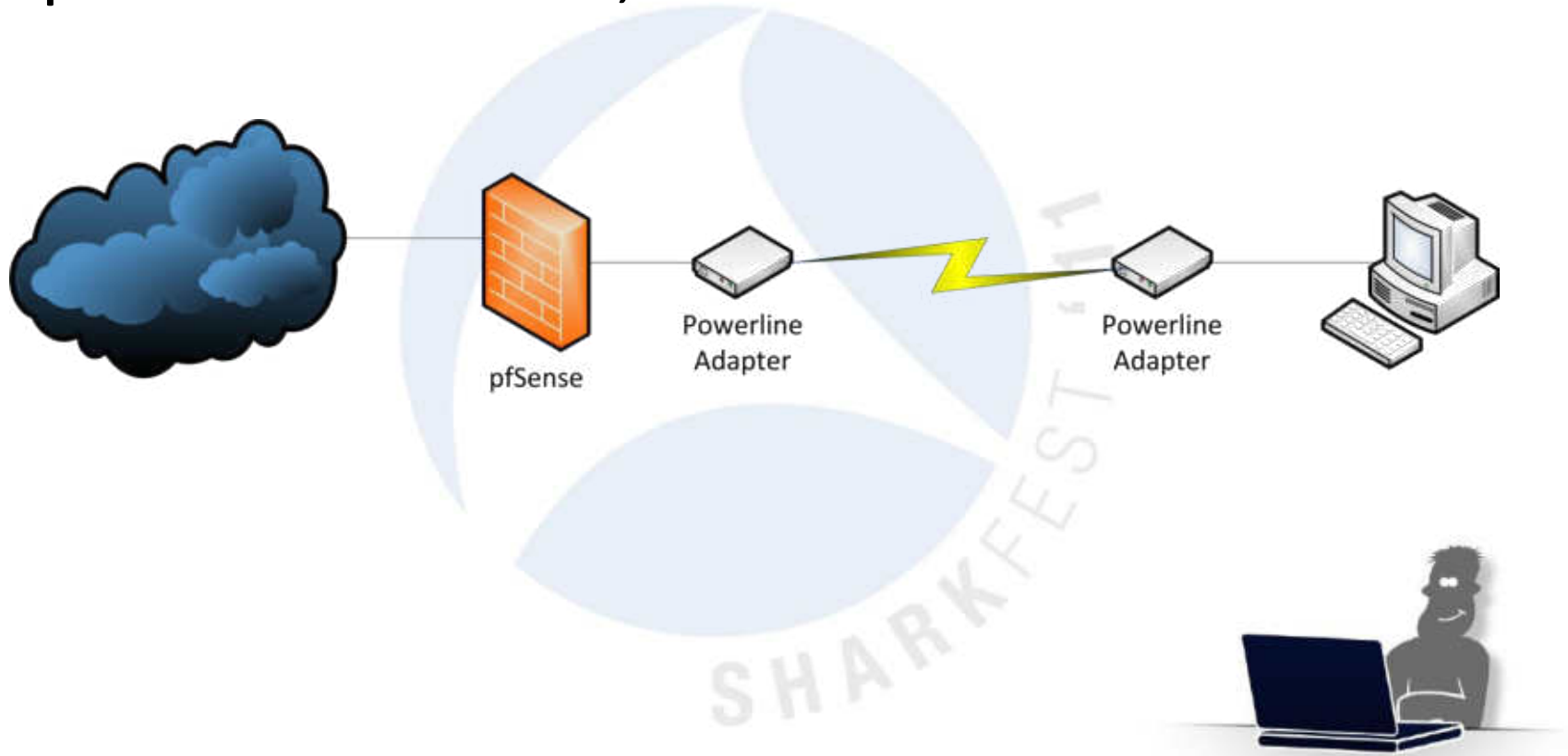
# The network brake

- WAN clients experiencing times of very slow network communication



# The home network job

- My dad calls, telling me he can't access one particular website, while all others work fine...



# Lessons learned

- Always test the equipment before going out into the field
  - Even if it worked fine yesterday
- Diplomacy skills are a big advantage
- Document, document, document
  - You'll need it to help you remember why that trace was captured and how
- Double-check your findings before talking about them
  - It helps to have skilled coworkers asking questions



# Questions?