

Human Factors in a Network Outage

UKNOF26

Paul Thornton

Confessions of someone
who really ought to know
better by now...

Me.

What Happened?

Pretty routine.

A compromised server generated 1Gbps of traffic and tried to send it down a link slower than that.

What Happened (2)?

I became fixated on the fact that the problem was on this link.

It wasn't.

Why?

Two words: Confirmation Bias.

Rebooting one router “helped” the situation...
... but then lead to a serious case of very poor troubleshooting.

In this instance, exacerbated by the fact that this link is (for reasons I won't bore you with today) effectively a SPoF.

Why?

Once you are “committed” to thinking this way – it is very hard to re-assess.

The human brain is very good at making the evidence fit your theory.

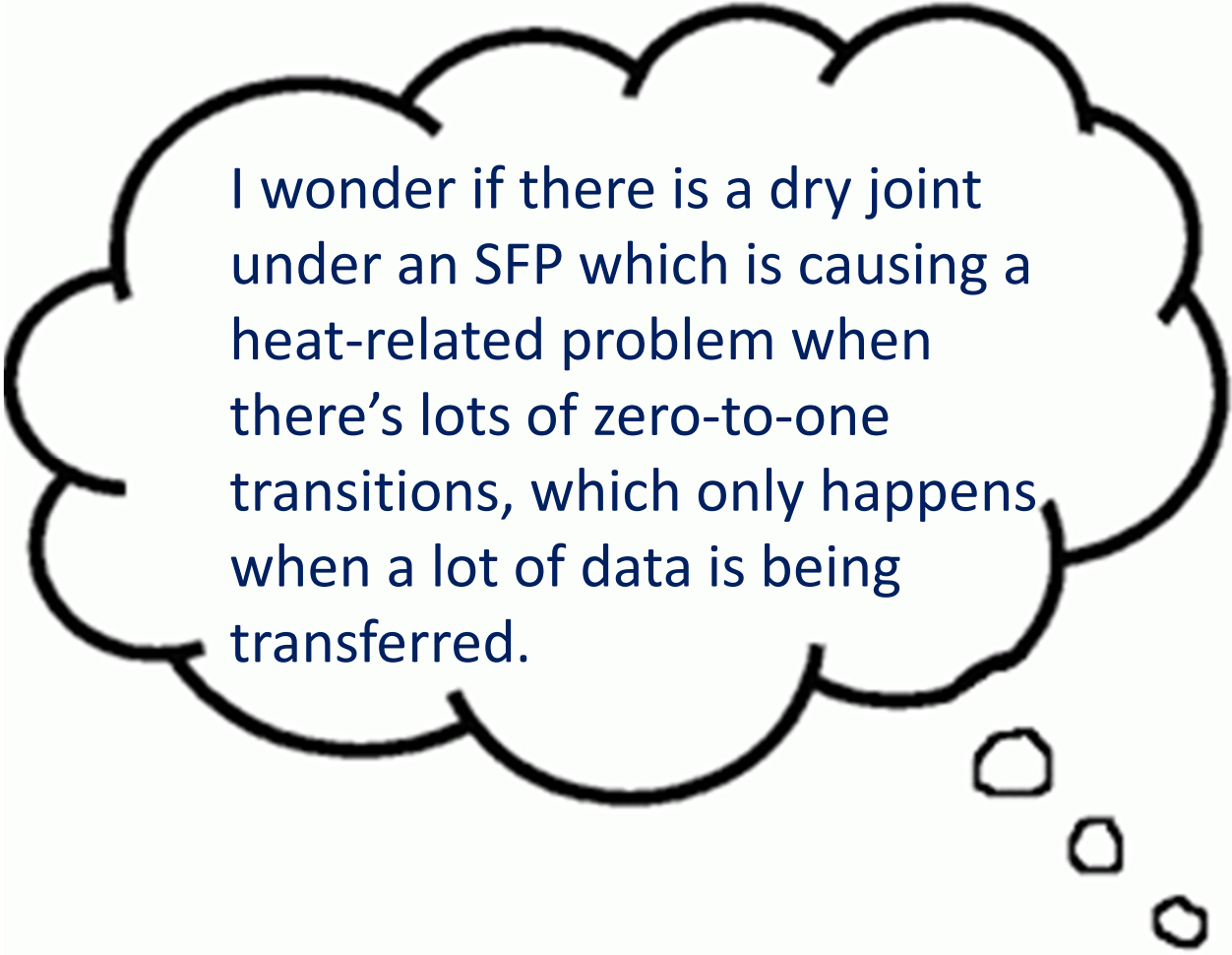
You don't realise that you are in this bad place!

**It isn't always the
Telco's fault.**

(Neil did not pay me to say this)

**It isn't always your
service provider's
fault.**

If you get to this stage...



I wonder if there is a dry joint under an SFP which is causing a heat-related problem when there's lots of zero-to-one transitions, which only happens when a lot of data is being transferred.

If you get to this stage...



Just because you have a
part of your network “at
risk” – don’t jump to
conclusions!

Debugging the Engineer

Methodical approach.

Listen to your colleagues.

Is it really probable that all of these independent things have gone wrong at once?

Debugging the Engineer

Trust your Instruments.

Beware of hidden “gotchas”.

Beware of quick fixes – original compromised server was one.

Questions?

```
GET /administrator/components/com_liv  
vechat/getChat.php?chat=0&last=1%20u  
nion%20select%201,unhex(hex(concat(u  
sername,0x3a,password))) ,3,4%20from%  
20jos_users HTTP/1.1
```