GETTING THE BYTES TO BRO

JUSTIN AZOFF

APRIL, 2016
TWO PROBLEMS

- Getting the bytes off the wire
- Getting the bytes to bro
GETTING THE BYTES OFF THE WIRE
BEST SOLUTION: USE FIBER TAPS
LESS GOOD SOLUTION:
USE SPAN PORTS
THE SPAN PROBLEM:

Regardless of any platform specific limitations monitoring an X gigabit port requires 2X gigabit:

- X gigabit of RX traffic
- X gigabit of TX traffic
- = 2X gigabit total traffic
POTENTIAL SPAN SOLUTIONS:

Like with a fiber tap, SPAN the RX and TX to two different output ports
OTHER ISSUES

- Where to tap
- Duplicate traffic
- Monitoring
GETTING THE BYTES TO BRO

A scaling and redundancy problem
SCALING

With modern hardware, you can aggregate multiple fiber feeds and analyze 10g of traffic on a single host.

But do you want to?
SO YOU FEED 8 FIBER PORTS INTO A SINGLE HOST..

- But then what if it crashes?
- How do you upgrade it without downtime?
- How do you add ‘just one more tap’ when you are out of pcie slots?
- How do you test new hardware or software?
TAP AGGREGATION AND LOAD BALANCING

A must for larger deployments.