Drinking from the Fire Hose

How to get traffic to your Bro cluster

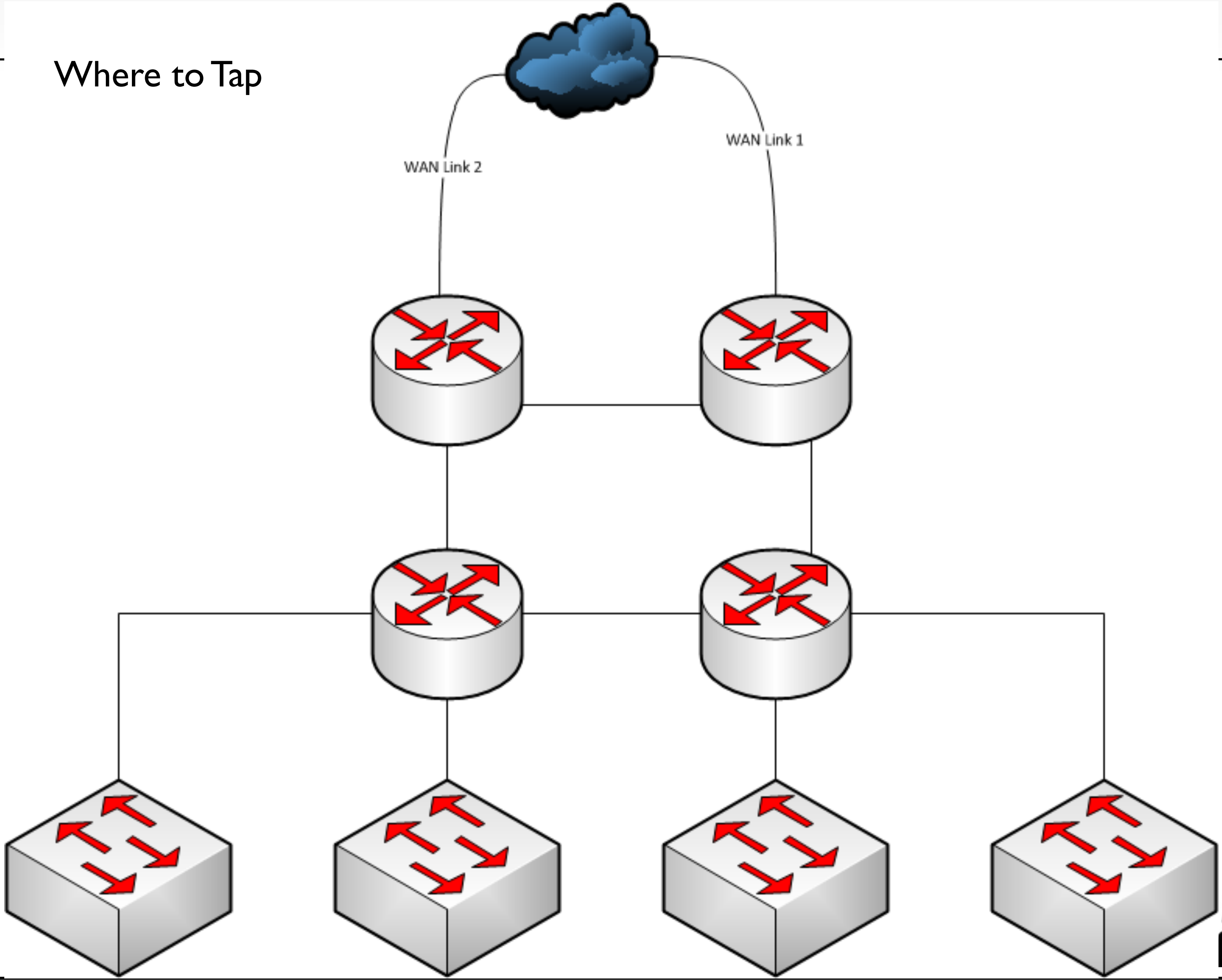
James Eyrich

Bro Workshop 2011
NCSA, Urbana-Champaign, IL

Where to Tap

- WAN or Internal
  - WAN
    - Detect intrusion attempts and out-bound misbehavior
  - Internal
    - Detect internal-internal malicious traffic
- Is there a possibility of more then one tap in the path of your flow
  - You will get duplicate packets sent to the cluster
  - Bro does not like getting duplicates
    - Separate Clusters
    - Deal with them using an external device

Where to Tap



Tap or Mirror(SPAN) port

Tap

- Cost - taps are extra hardware
- Interrupt connection to put in place.
- Light levels
  - Passive taps split the light and reduce power going to all end points – routers and the monitoring equipment
  - Find out what the minimum rx level is for router and monitoring equipment optics.
  - Pick the appropriate tap split ratio – Gigamon Support says 50/50 for 10Gbs
  - If needed there are regeneration/active taps
- Stand-alone or built-in taps
  - Built-in may lead to inflexibility of testing
  - Tied to vendor with built-in

Tap or Mirror(SPAN) port – cont.

Port Mirror (span)

- Trust the device doing the mirroring
  - Misconfiguration
  - Hardware defect
- Oh, here is an extra port!
  - When ports run tight and no one wants to buy a card
  - When the Network Engineers “need” your mirror port
- On the fly mirroring of ports to cluster members

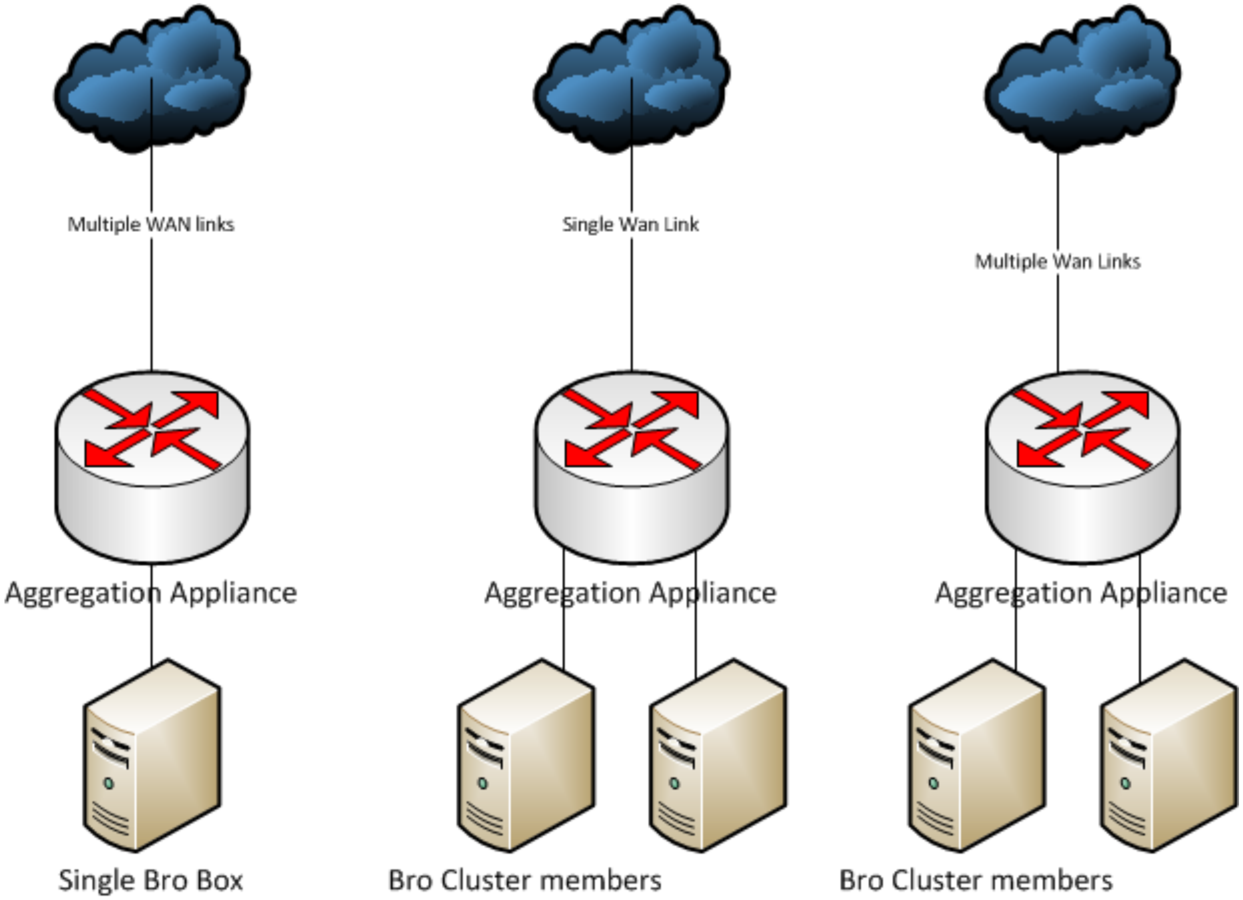
Aggregation and Load Balancing

Asymmetric Traffic

- A cluster member must receive all the packets for a particular flow
- If you don't have the possibility of asymmetric traffic you can plug taps straight into the cluster members - beware of load balancing issues.

Load balancing (LB)

- Many to one, one to many, many to many
- How many tuples is the LB algorithm using?



Bro Workshop 2011
NCSA, Urbana-Champaign, IL

Hardware Aggregation and LB

Gigamon

- Limited support when using Non-Gigamon transceivers
- GigaSmart boards can provide de-duplication
- Port only load balancing
  - Limit of 8 ports per load balance group (gigastream)
  - Our solution: uses multiple gigavue boxes in a tiered arrangement to feed part of one stream into another.

HW Aggregation and LB – cont.

Cpacket

- Have certified major transceiver vendors, will consider certifying others at customer request.
- Port and MAC address load balancing
  - MAC – use commodity ether switch for further LB.
  - Up to 48 mac addresses in a load balance group.
- Some products may offer automatic de-duplication. Support suggests using defined filters instead.

Cluster Member Load Balancing

- Take advantage of multiple cores
- Use features of NIC to load balance flows to processes running on each core.
  - Myricom – Sniffer driver – pay per NIC
  - Intel – PF_Ring and NIC's Flow Director, also NTOP drivers
- MAC based load balancing extended
  - Each Bro instance listens to a different destination MAC address

Etc

Can my external box slice packets to reduce payload from large streams (gridFTP)

- Gigamon GigaSmart cards can
- Cpacket Smart ports can