A man, a plan, an Arista, Panama?

Bob Bregant – BroCon ‘14

ILLINOIS

illinois.edu

Bro/Arista Integration

Bob Bregant – BroCon ‘14

ILLINOIS

illinois.edu

Bro Tap/Span Networking

(with Arista-specific examples)

Bob Bregant – BroCon ‘14

ILLINOIS

illinois.edu

Quick Introduction

- Bob Bregant - University of Illinois
  - Senior IT Security Engineer
    - Performed production Bro deployment at Illinois
    - Designed and deployed tap network
  - IT Security Analyst
    - Now I just use the data/scripts and try to think about how to improve that end of things

What this talk is ***not***

- Vendor talk/Sales pitch
- Something new that I've come up with
- Restricted to deployments of unusual size
- Presentation by product engineer

Campus Networking @ Illinois

- 10Gb/s core network
  - Services 320 buildings over 2.8 mi^2, nearly 55,000 users
- Multiple 10Gb/s outbound connections
  - Commodity Internet
  - Other state universities (ICCN)
- 100Gb/s connection to Internet2

What that means…

Bro @ Illinois

- Clearly can't monitor *everything…*
- Select critical points within network
  - What gets us the most "bang for our buck"
- Data fed back to central Bro cluster(s)
- This means optical taps need to be spread over a good bit of that 2.8 mi^2…
  - Cross-campus fiber isn't *that* cheap

Tap Networking @ Illinois

- Shadow campus network
  - Dedicated cross-campus fiber
- Switches at tap locations
  - Minimize light issues, minimize traffic
- Switch at Bro cluster
  - Fancy cluster traffic splitting

Aggregation

- Fiber isn't free
- Basically a big LAG
  - Lumps stuff together, amps it up, shoots it out
- Caveats
  - Don't forget to double your bandwidth
    - Unless you don't need to
  - Label everything

Aggregation

```
sw-brocon-14>enable
sw-brocon-14#config
sw-brocon-14(config)#tap aggregation
sw-brocon-14(config-tap-agg)#mode exclusive
sw-brocon-14(config-tap-agg)#config
sw-brocon-14(config)#spanning-tree mode none
sw-brocon-14(config)#no igmp snooping
```

Aggregation

```
sw-brocon-14(config)#interface Et33-36
sw-brocon-14(config-if-Et33-36)#description ResNetTaps
sw-brocon-14(config-if-Et33-36)#switchport mode tap
sw-brocon-14(config-if-Et33-36)#switchport tap default group ResNetTaps
sw-brocon-14(config-if-Et33-36)#interface Et37-38
sw-brocon-14(config-if-Et37-38)#description VPNTaps
sw-brocon-14(config-if-Et37-38)#switchport mode tap
sw-brocon-14(config-if-Et37-38)#switchport tap default group VPNTaps
```

Aggregation

```
sw-brocon-14(config-if-Et37-38)#interface Et1-4
sw-brocon-14(config-if-Et1-4)#description BroProdCluster
sw-brocon-14(config-if-Et1-4)#channel-group 10 mode on
sw-brocon-14(config-if-Et1-4)#interface Po10
sw-brocon-14(config-if-Po10)#switchport mode tool
sw-brocon-14(config-if-Po10)#switchport tool group set ResNetTaps VPNTaps
sw-brocon-14(config-if-Po10)#write mem
```

Traffic Duplication

- Cases where you want duplication
  - Test Bro cluster (partial?), other security tools
- Can also just be splitting
  - PCI to dedicated tools
- Two methods
  - Simple just uses tap aggregation
  - More complex deep-packet stuff is possible

Traffic Duplication

```
sw-brocon-14>enable
sw-brocon-14#config
sw-brocon-14(config)#interface Et5-8
sw-brocon-14(config-if-Et5-8)#description BroTestCluster
sw-brocon-14(config-if-Et5-8)#channel-group 11 mode on
sw-brocon-14(config-if-Et5-8)#interface Po11
sw-brocon-14(config-if-Po11)#switchport mode tool
sw-brocon-14(config-if-Po11)#switchport tool group set VPNTaps
sw-brocon-14(config-if-Po11)#write mem
```

Filtering

- Fiber isn't free
  - Neither is CPU time (on Bro or on switches)
- Drop early and drop often
  - Filter on ingress or egress (limits on egress)
- Justin's DumbNo flows
  - Others too: Syslog, Netflix, encrypted stuff, traffic duplication, internal VLANs?

Filtering

```
sw-brocon-14>enable
sw-brocon-14#config
sw-brocon-14(config)#ip access-list NoSyslog
sw-brocon-14(config-acl-NoSyslog)#deny udp any host 22.33.44.55 eq 514
sw-brocon-14(config-acl-NoSyslog)#deny udp any host 22.33.44.55 gt 1500
sw-brocon-14(config-acl-NoSyslog)#exit
sw-brocon-14(config)#write mem
```

Symmetric Hashing - Cluster

- A.B.C.D->E.F.G.H **must** go to the same machine as E.F.G.H->A.B.C.D
- Don't want to simply partition 0.0.0.0/0
  - It's not evenly populated or evenly popular
- Caveats
  - This cannot split a single flow
  - This does not know the load on your boxes

Symmetric Hashing - Cluster

```
sw-brocon-14>enable
sw-brocon-14#config
sw-brocon-14(config)#load-balance policies
sw-brocon-14(config-load-balance-policies)#load-balance fm6000 profile BroCon-Symm
sw-brocon-14(config-load-balance-profile-BroCon-Symm)#port-channel hash-seed 39
sw-brocon-14(config-load-balance-profile-BroCon-Symm)#distribution symm mac-ip
```

Symmetric Hashing - Cluster

```
sw-brocon-14(config-load-balance-profile-BroCon-Symm)#no fields mac
sw-brocon-14(config-load-balance-profile-BroCon-Symm)#fields ip protocol dst-ip src-ip
sw-brocon-14(config-load-balance-profile-BroCon-Symm)#config
sw-brocon-14(config)#interface Et33-38
sw-brocon-14(config-if-Et33-38)#ingress load-balance profile BroCon-Symm
sw-brocon-14(config-if-Et33-38)#write mem
```

Special Notes/Fun Facts

- Thou shalt **not** truncate the packets
  - Breaks Bro, there are better ways to cut down
- Symmetric hashing works best with 2^X
  - Seems like this is cross-vendor
- Arista hardware is running Fedora
  - And you have root. You can install software.
- There is a Web UI

Questions?

- If not, or if you come up with anything later:
  - Ask in #Bro on Freenode IRC
  - Ask on the Bro mailing lists
  - Someone will answer (probably Seth)
- Thanks!

Questions?

- If not, or if you come up with anything later:
  - Ask in #Bro on Freenode IRC
  - Ask on the Bro mailing lists
  - Someone will answer (probably Seth)
- Thanks!