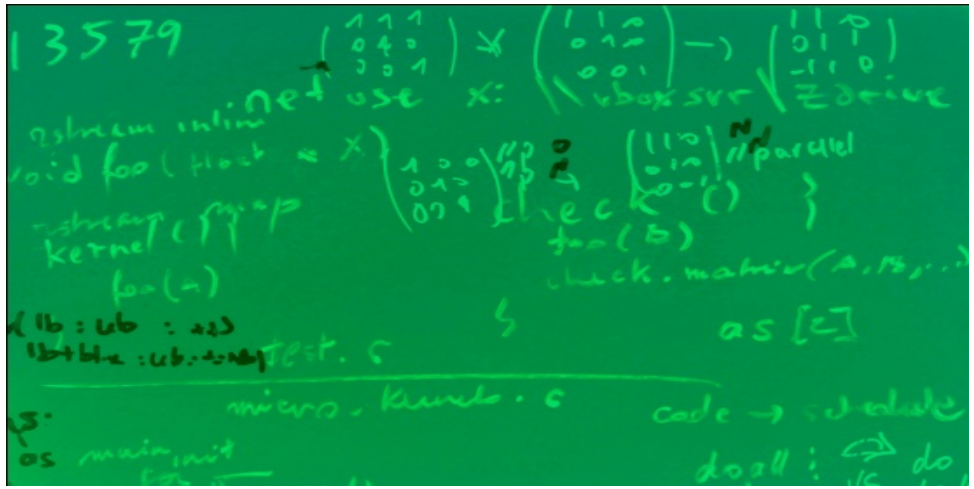
Using VLAN tags to physically map traffic flows



Dilip Madathil, Reservoir Labs
madathil@reservoir.com

Motivation

Question:

Where did this packet come from on the local network?

Our solution:

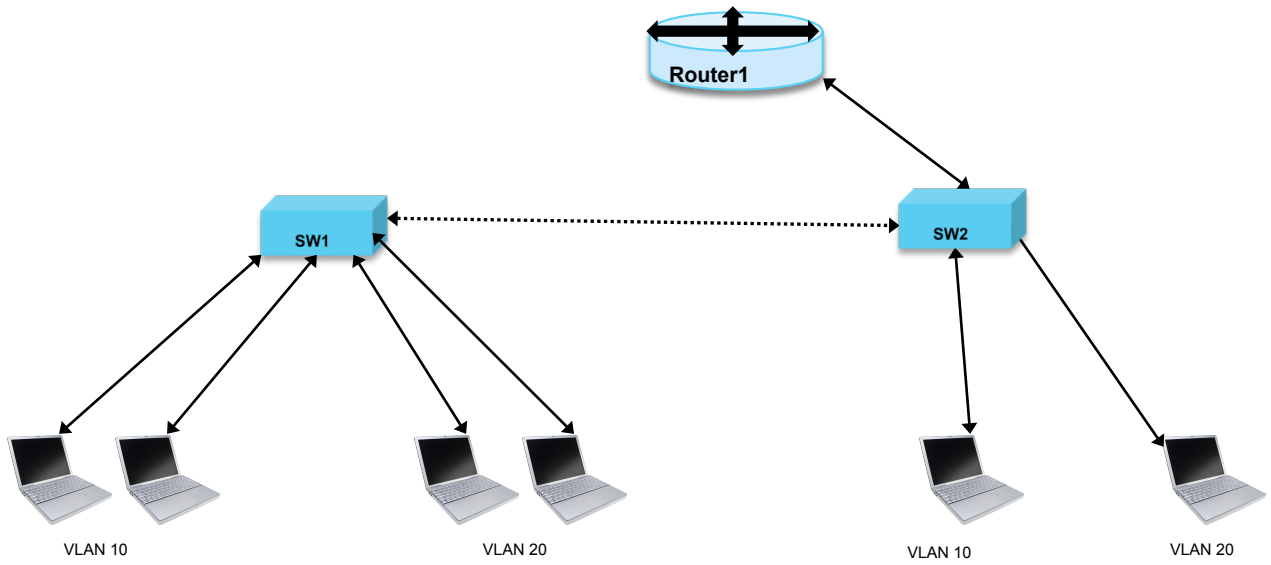
Use VLAN tags with tap/aggregation fabric to carry location information.

Use VLAN tag extraction in Bro to automate this.

Virtual LAN

What?

- Group of hosts with same broadcast domain, regardless of physical location.
- Layer 2 grouping but need not be on a single switch.
- Membership configured on a switch via software.



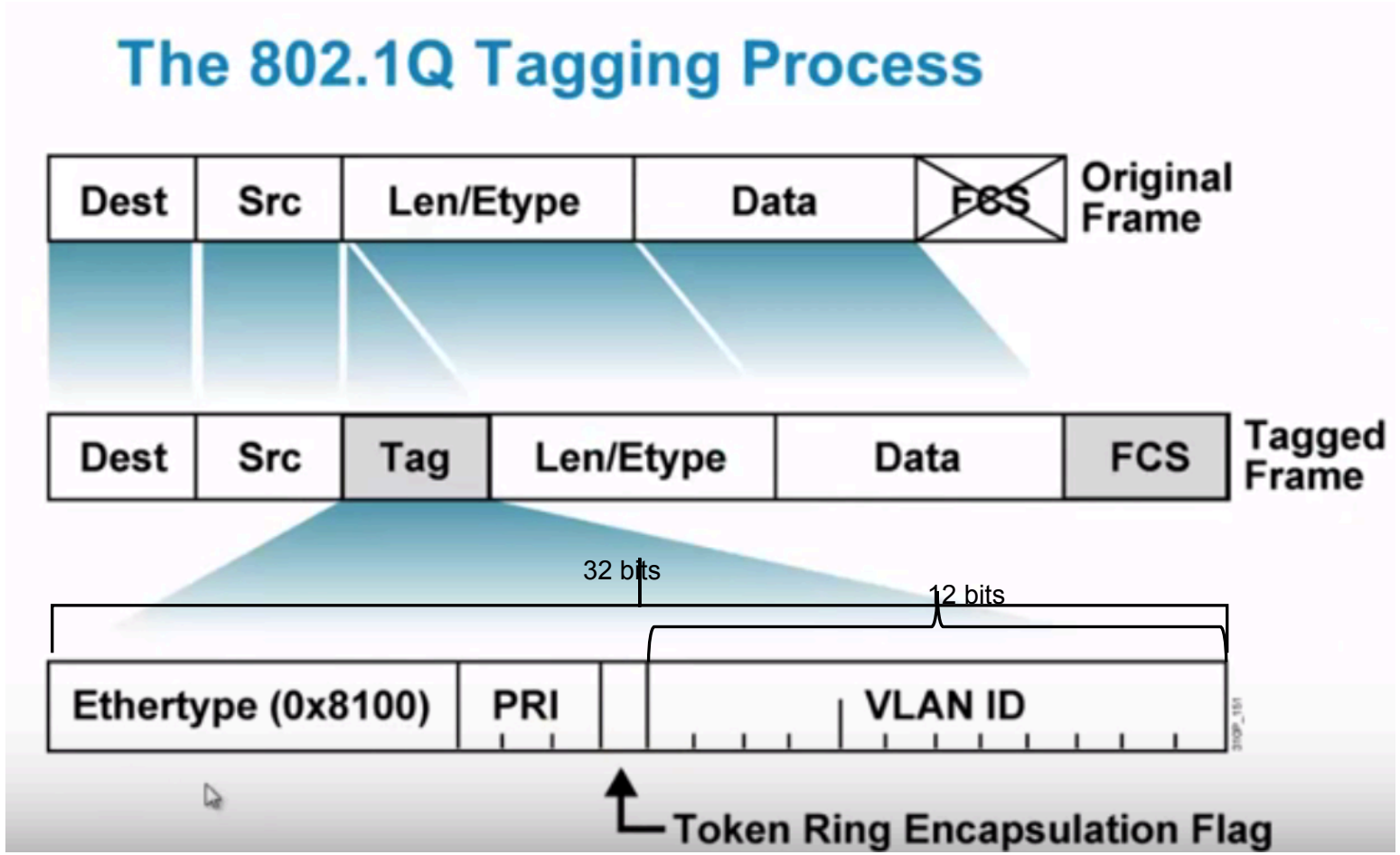
Virtual LAN

Why?

- Logical rather than physical networks
- Smaller broadcast domains
  - Fewer collisions.
  - Lesser wasted bandwidth and processing.
- Added security
  - On the same switch but communication is protected.

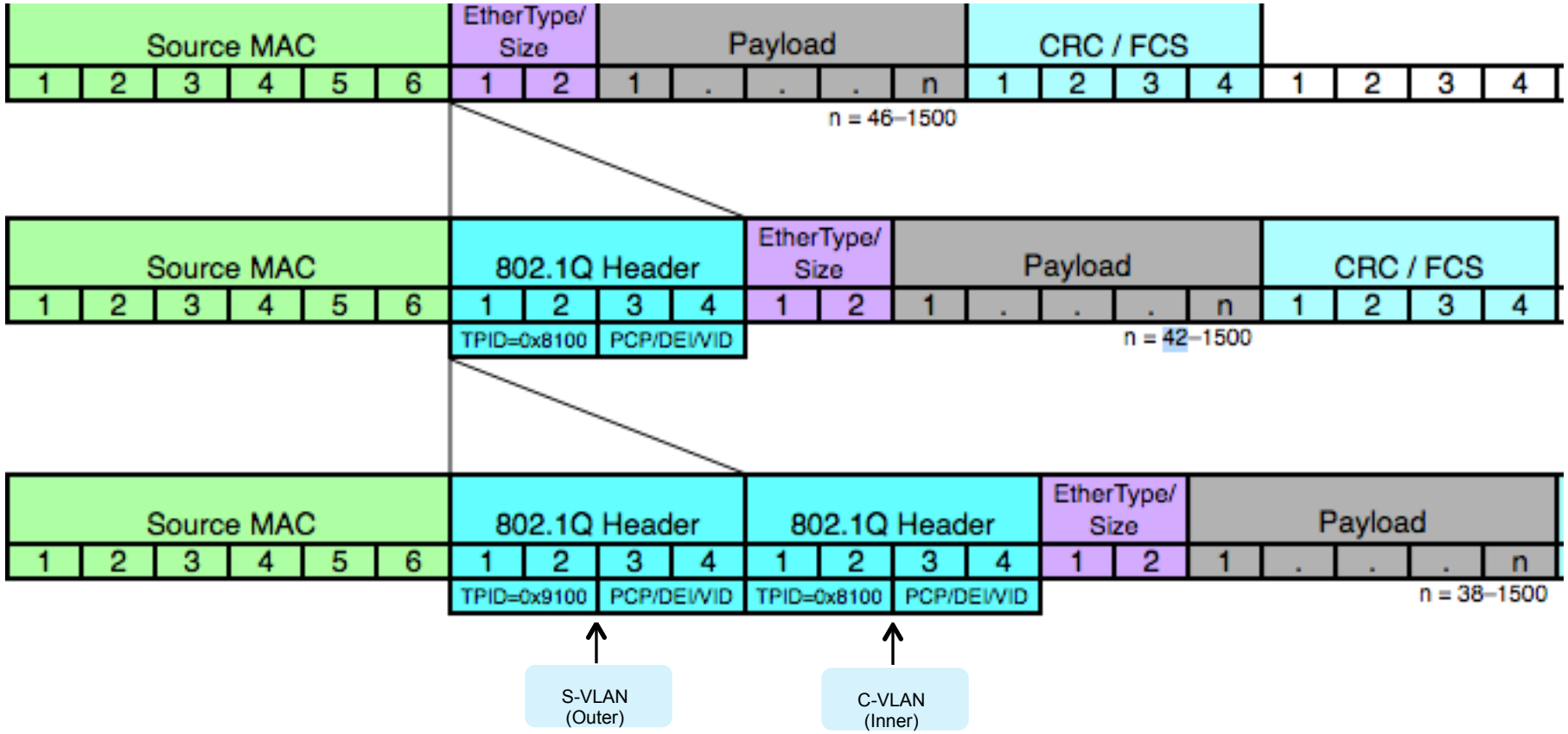
Virtual LAN

How?



https://www.youtube.com/watch?v=3RLTI7Hswz8

VLAN- 802.1ad/QinQ



TPID: 0x8100 for single tag
TPID: 0x9100 for double tag

https://en.wikipedia.org/wiki/IEEE_802.1Q

VLAN and Bro

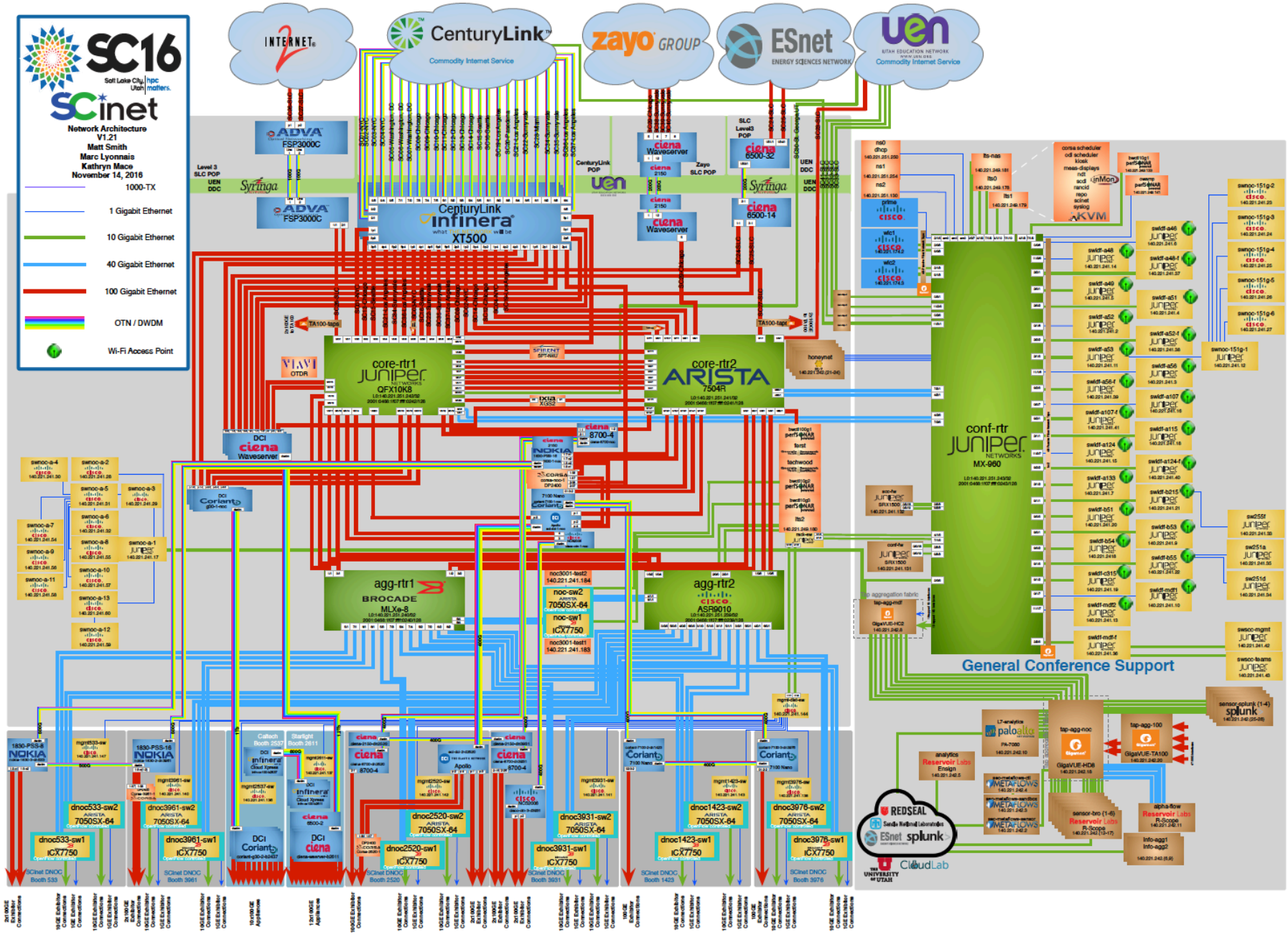
- New in Bro 2.5.
- Extract both inner and outer vlan tags.
- Adds information to connection state.
- policy/protocols/conn/vlan-logging.
- Running well in R-Scope production since Nov 2015.
- Eg output

```
[rscope-logs] /rscope_logs/logs/current# bro-cut vlan < conn.log | sort | uniq –c
    731 100
    764 101
    829 102
    236 103
```

SC16 Network

- 3.15 terabits per second.
- 56 miles of fiber deployed.
- $32 million of loaned network equipment.
- Bro used to monitor main conference network.
  - 342 exhibitors each with their own VLAN.
  - 6 Reservoir Labs R-Scope appliances.
  - 24 10Gbps ports.
  - Monitoring 36 10/1Gbps taps for border traffic and internal commodity traffic (i.e. rooms, halls, wifi, hardwired)
  - Max traffic observed 75Gbps.

SC16 Network



VLAN tags @ SC16

- VLANs used to segment the network by teams, functions and customers.
- Security team used VLAN tags and Bro to
  - Locate network end points.
  - Validate whether all taps are generating data.
- Each booth has its own VLAN tag.(inner)
- Each ingest(Tap) to a monitoring port also adds its own VLAN tag.(outer)
- Using Bro
  - Create a mapping of booth VLAN tags to
    - ip address range for the vlan.(v4 and v6)
    - A human readable description of the booth or physical location.
  - Create a mapping of the tap VLAN tag to the location where the feed was tapped from
    - Eg Conference Room A

Using VLAN tags to geo-locate packets

- Augment generated notices
  - Use hook Notice::policy(n: Notice::Info)
  - If connection information available
    - Get the VLAN tag
    - Use it to get the booth/Physical location information.
    - Tap information.
  - If connection information is not available
    - Get the destination and source address from the message and subject
    - Get the VLAN tag/booth/Tap for the destination/source from the mapping
- Additionally VLAN to physical location mapping information can also be provided to Splunk
  - Can be used gather information about traffic statistics for each VLAN using the VLAN tag in the connection logs.

Demo and Q & A

- Setup
  - R-Scope VM running on laptop.
  - Pcap with manufactured vlan data
    - 4 vlans with location information north, south, east and west.
    - 2 vlan ids for identifying tap/location information(wifi upper-level, wifi-lower-level)
  - Output
    - conn.log and notice.log augmented with location information.
    - New vlan_data.log generated with vlan information.
- Code and the test pcap will be publicly released soon.

References

- https://en.wikipedia.org/wiki/Virtual_LAN
- https://www.youtube.com/watch?v=3RLTI7Hswz8
- Code help from Michael Dopheide and Alan Commike
- http://sc16.supercomputing.org/2016/11/18/sc16-breaks-exhibits-workshop-attendance-records/