Network Tapping Technologies

Kevin A. Nassery

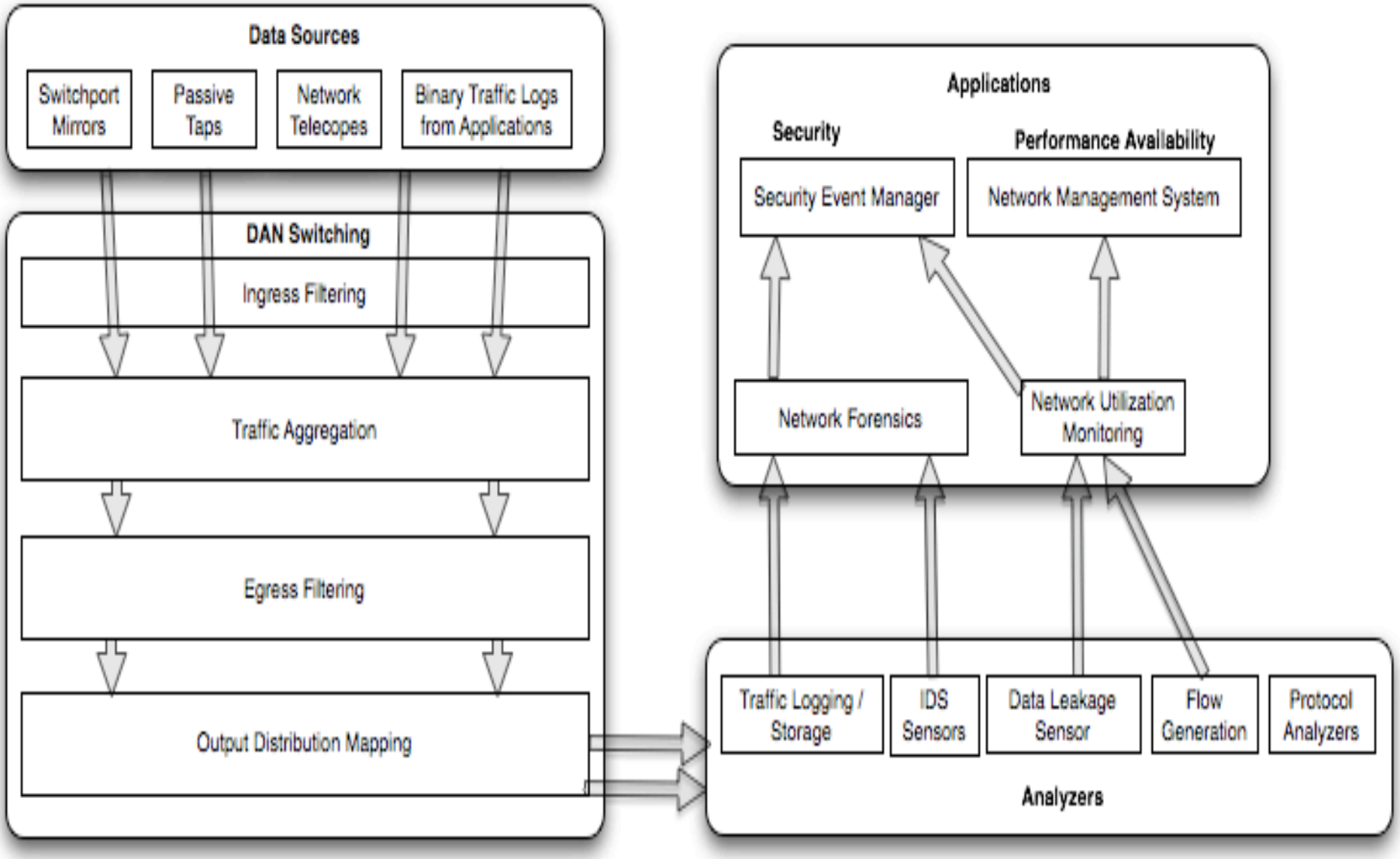
NANOG48

02/22/10

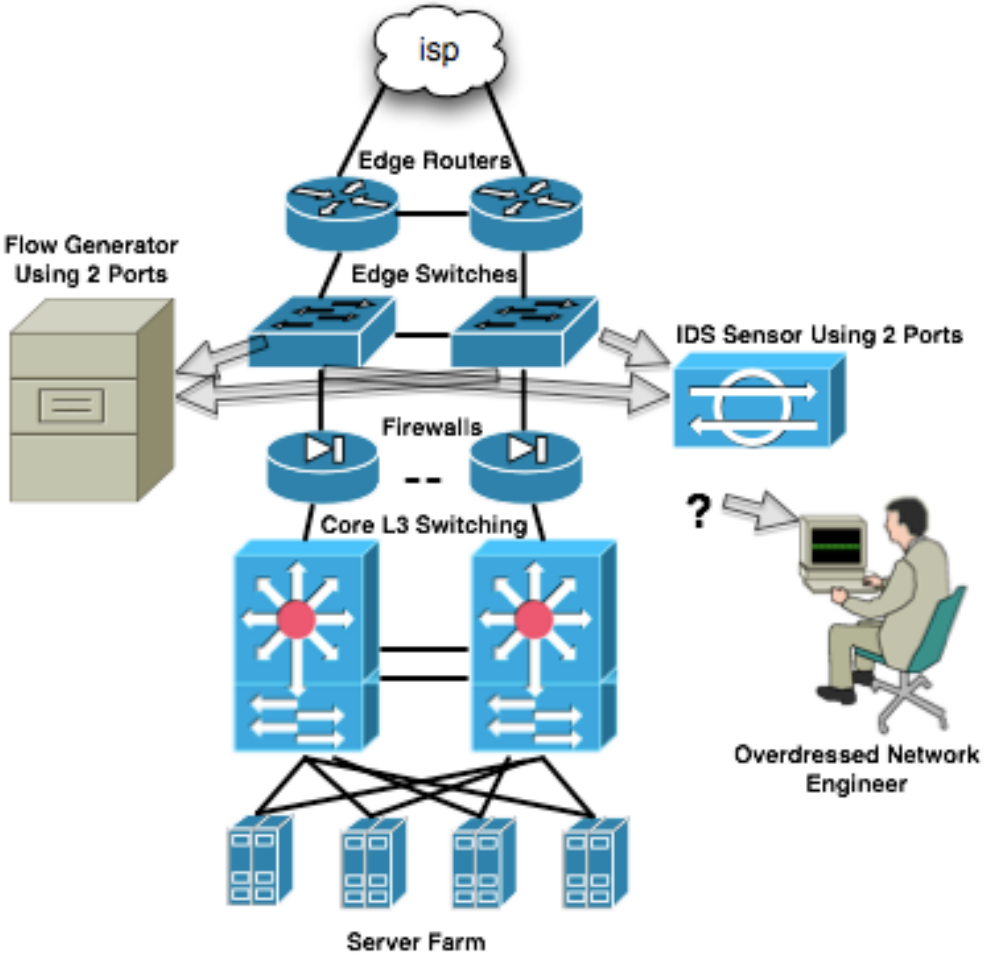
What is a Data Access Switch?

- Infrastructure designed to provide robust out of band mapping of network traffic (from taps, port mirrors, etc) to network capture and analyzer tools.
- Traditionally traffic analyzer tools have been painful to deploy due to limitations of SPAN sessions, full-duplex taps, etc.
- DAN Switches go a long way solving these issues.

Anatomy of a Data Access Network



DAN Switch Use Case #1: Public Services Network Module Utilizing Network IDS, and External Flow Generator at the network perimeter.



Without DAN Switching

•Both switches must be configured to mirror traffic from uplink ports to sensor ports.

•IDS requires 2 ports 1 for each switch & must aggregate the data in software.

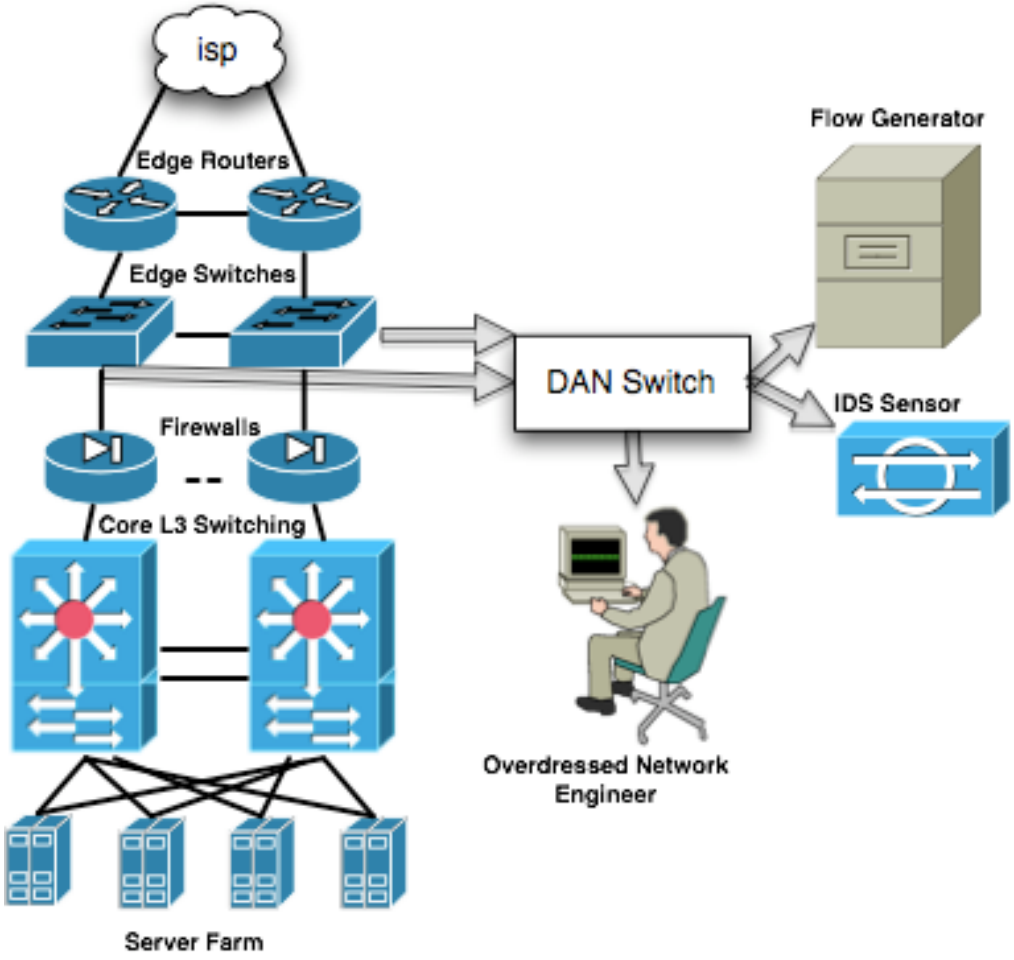
•Flow Generator and IDS are looking at the same traffic.

•Flow Generator also requires 2 ports & must aggregate data in software.

•2 SPAN session limitation on switches means Network Engineer wishing to connect portable analyzer must disconnect an active analyzer.

•Network Engineer using portable analyzer can only see half of the external traffic assuming topology is load balanced.

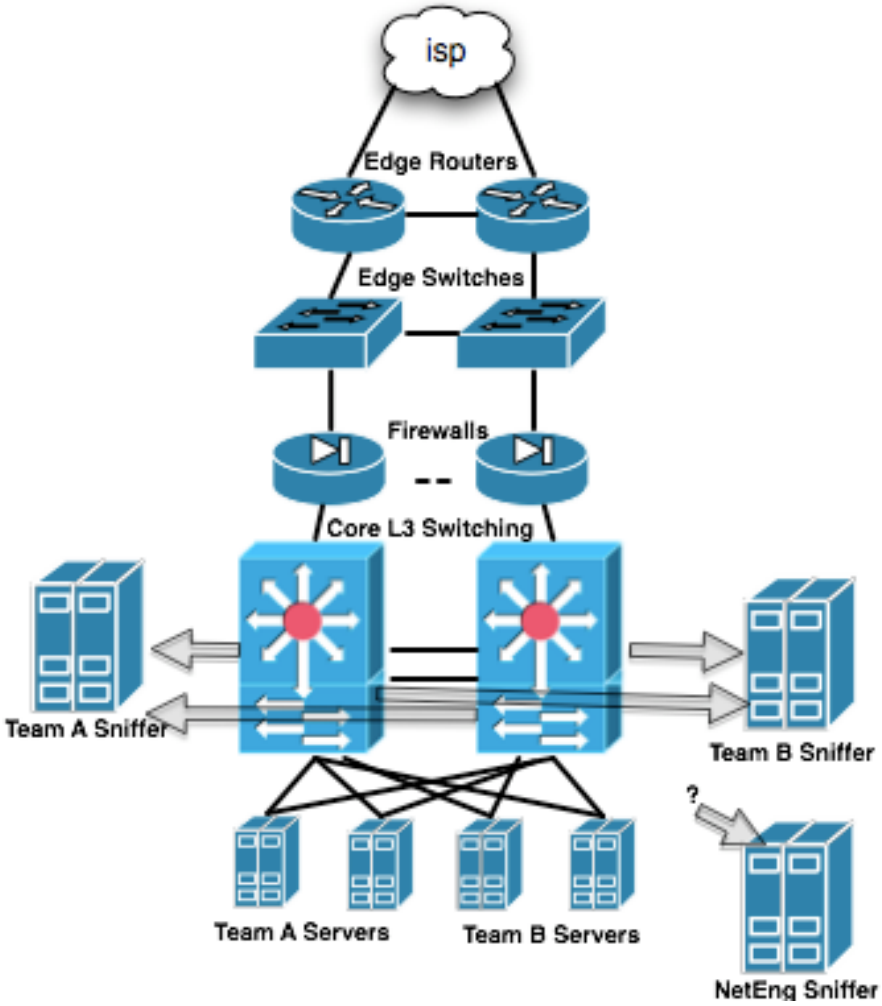
DAN Switch Use Case #1: Public Services Network Module Utilizing Network IDS, and External Flow Generator at the network perimeter.



With DAN Switching

- 1 SPAN port per switch is used.
- Switch SPAN ports are aggregated by DAN switch.
- DAN switch output to IDS sensor is 1 port.
- DAN switch sends the same output stream that the IDS sensor is using to the Flow Generator.
- Neteng now has choice of using free'd SPAN ports, or better yet, using a new output port on the DAN switch for his portable analyzer.
- If IDS or Flow generator are overloaded specific traffic can be excluded from stream (Ipsec VPN traffic perhaps).

DAN Switch Use Case #2: Server Admin Teams want Network Level Visibility into their servers, and *only* their servers.



Not using DAN Switches:

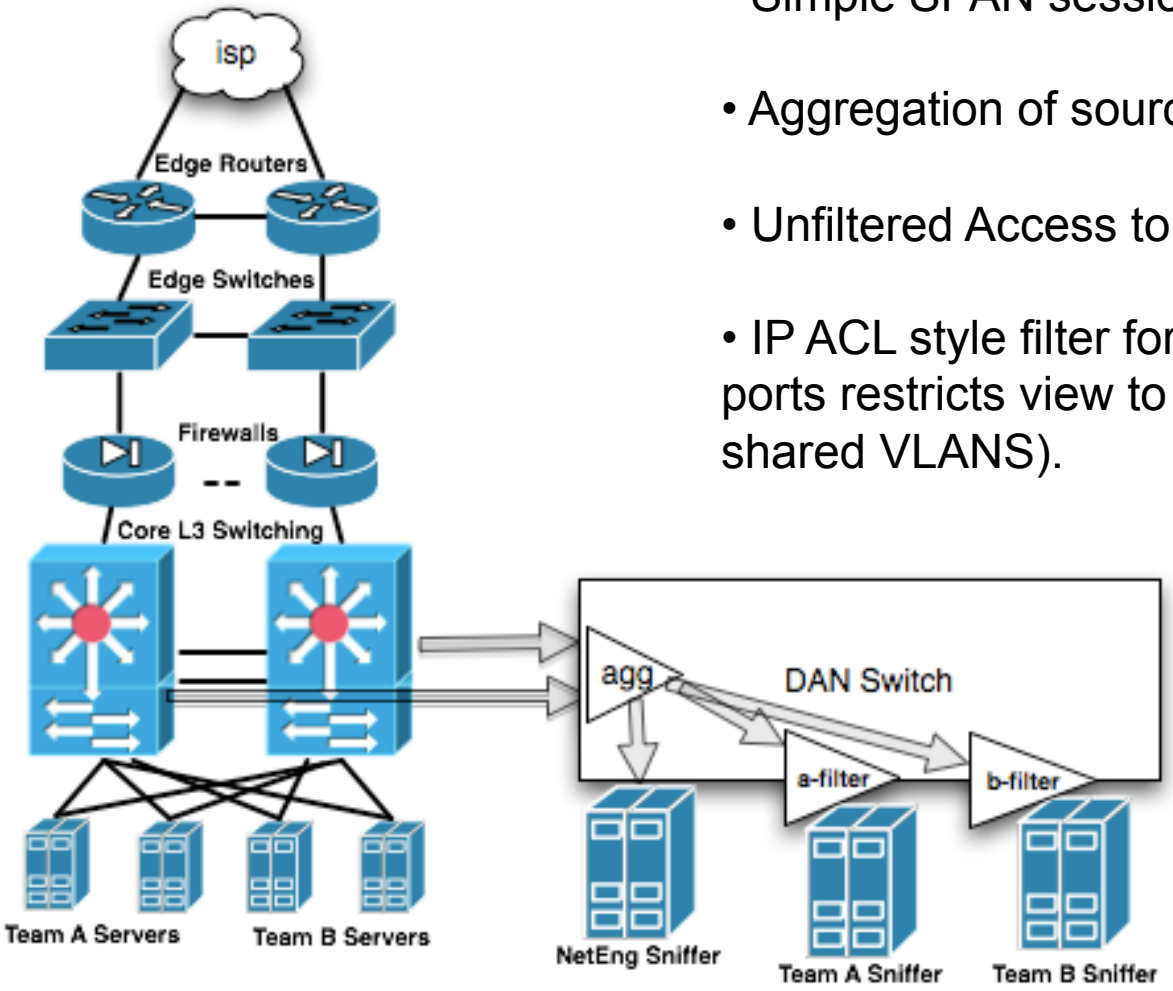
•SPAN ports (potentially with VACLS) must be configured for each switch to each sniffer.

• Servers must aggregate data together using software.

• Does not scale for >2 number of groups.

• Additional access switches require additional server ports.

DAN Switch Use Case #2: Server Admin Teams want Network Level Visibility into their servers, and *only* their servers.



Using DAN Switches:

- Simple SPAN sessions for relevant VLANS.
- Aggregation of source ports (could be 10gE).
- Unfiltered Access to NetEng Sniffer.
- IP ACL style filter for Team A, Team B output ports restricts view to their servers (even in shared VLANS).

My Background

- Been using DAN devices for a few years.
- Recently advised on an effort where 10gE connections were being monitored and converted to flows at the edge.
- It seems like vendors are in a GUI feature war in this space, rather than making these things more usable in the real world.

The good

- Flexibility over traditional taps, port mirrors, aggregation and regeneration.
- Performance advantages of being able to filter traffic before it gets to your tools.
- Avoids the complexity of distributed sniffers and RSPAN.
- Easy to use, and to manage remotely.
- Aggregate multiple source ports
- Filter that input data
- Distribute the input data to output ports
- Filter that output data

The Bad #1: No Truncation

- Tools which only need headers get whole frames.
  - limits our ability to oversubscribe tool-ports.
- For example looking at headers of a 10gE link in production ~5% of information was headers.
  - Even with link saturation, truncated headers could be monitored with a gigE tool port.

The Bad #2: No custom PDU offsets

- Filters can be written for basic protocol properties like TCP port, but cannot have filters on arbitrary offsets like TCP[0] to indicate the first byte of a TCP header.
- Typically we only get frame offsets which is too difficult to use consistently (for example dot1q variance, or IP options change TCP[0]).

The Bad #3: Limited ability to leverage 802.1q VLAN filters.

- Many switches strip VLAN tags off SPAN ports.
- This means DAN device must be inline dot1q links.
- Limitation of switch not DAN itself.

The Bad #4: Source ports must be from single network layer.

- If src ports are combined from access, distribution, core, and perimeter networks packets are duplicated to the tool port at ever point they are seen confusing most tools.

The Cure

- In-line frame truncation
- Tcpdump style PDU offsets for major protocols.
- Switch vendors need to support mirroring 802.1q VLAN tags to SPAN ports.
- IP TTL De-duplication (using TTL variances to separate distinct routing layers and eliminate duplicate frames).
- Input ports should be able to be labeled with arbitrary 802.1q tags so that tool ports can filter different access layers.
- Statistical sampling mode (send me 1/20 packets).

Q & A