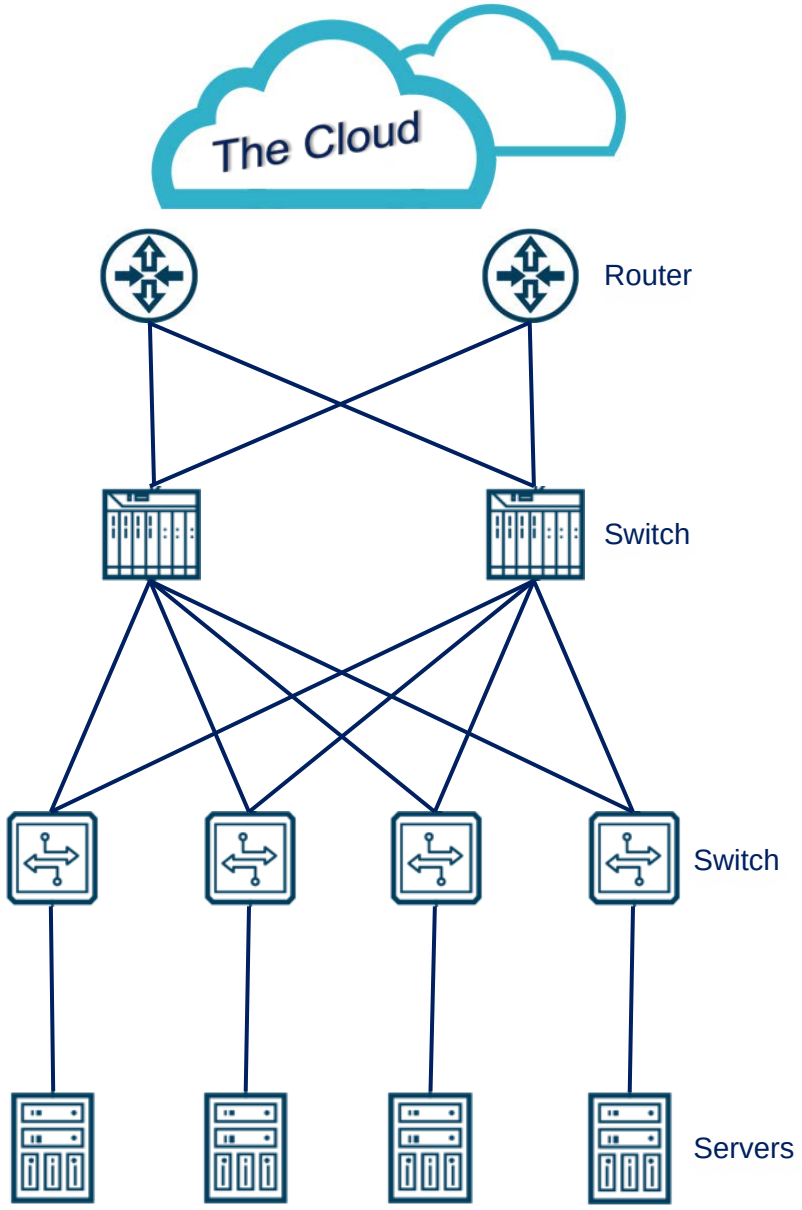
ARROW SOMMERFEST 2018

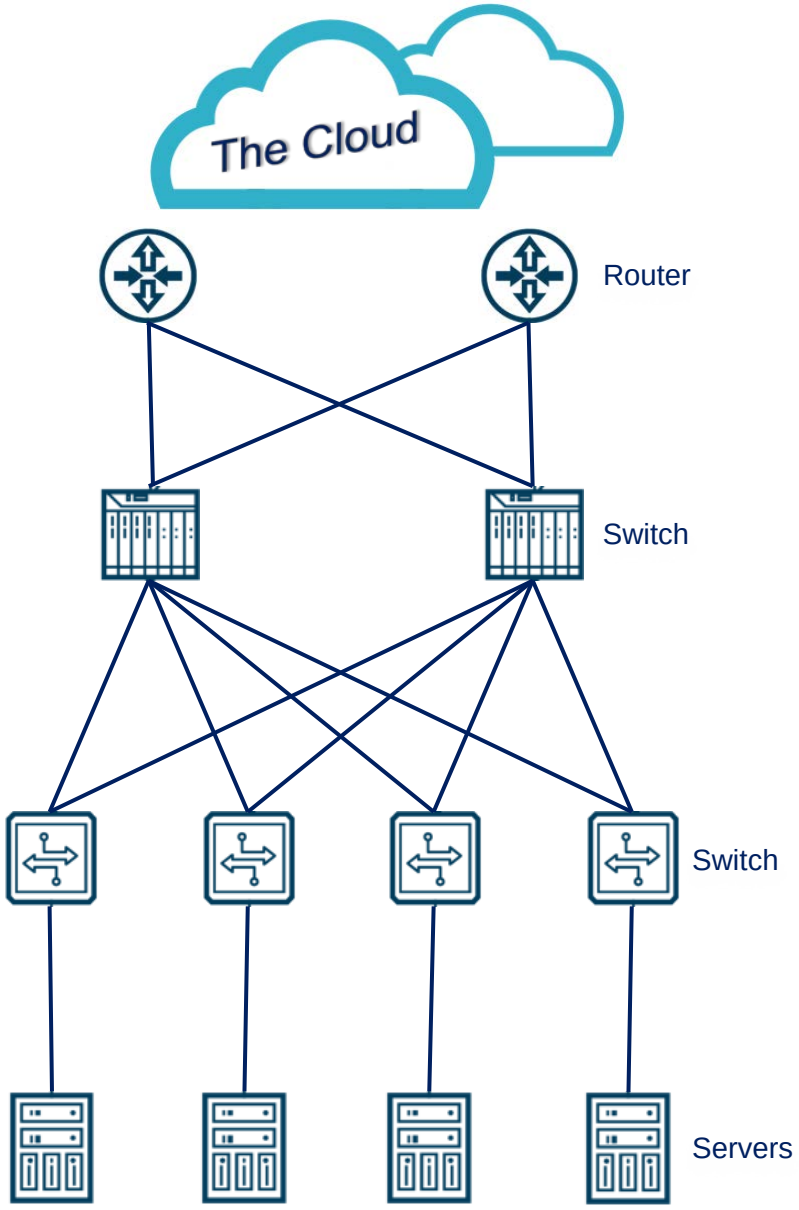
Christian Reuling, System Engineer

EXAMPLE NETWORK INFRASTRUCTURE



ixia

WHAT DO YOU WANT TO KNOW

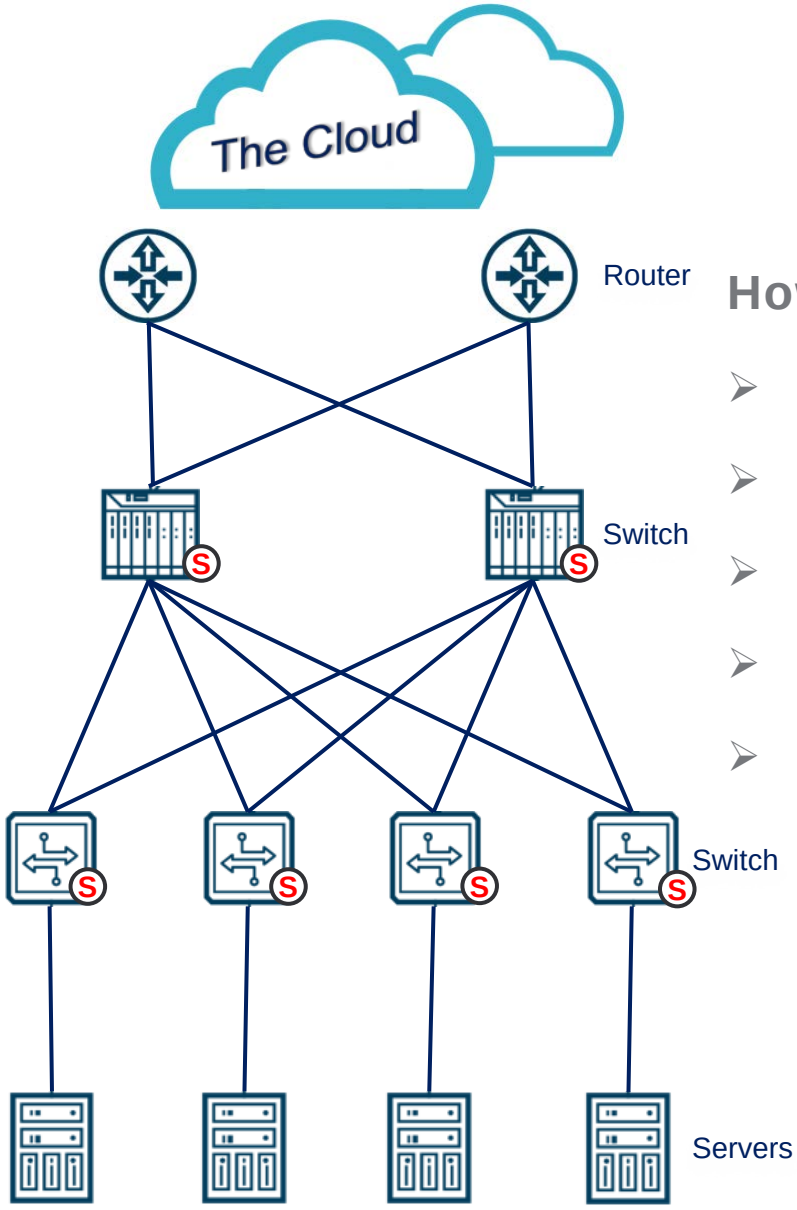


How do they make sure that the millions of Dollars that has been spent are paying off in terms of:

- **Availability:**
  - meet SLAs
- **Security:**
  - Potential threats, data loss prevention, vulnerabilities
- **Compliance:**
  - Sarbanes-Oxley, HIPPA, PCI-DDS
- **Performance:**
  - End user experience, troubleshooting, root cause analysis
- **Trends:**
  - Capacity planning and scalability

ixia

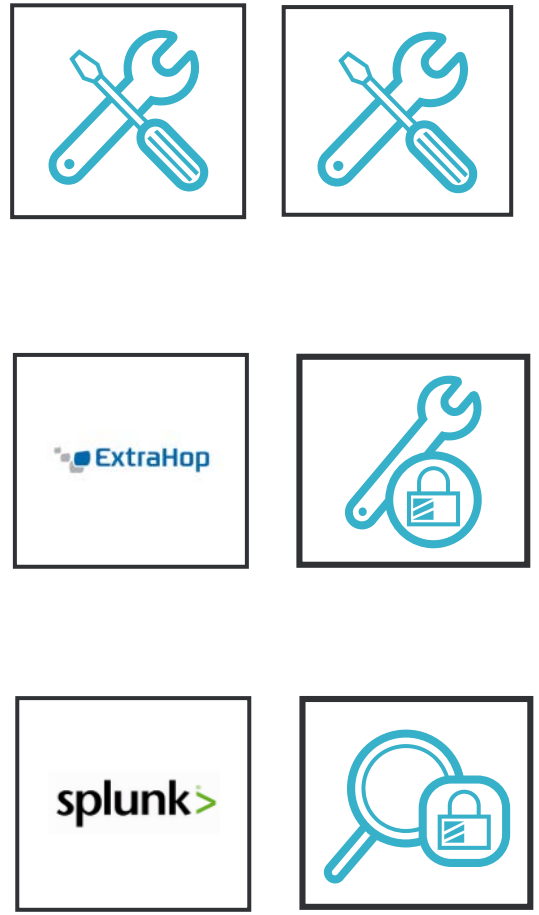
SOLVE PROBLEMS WHEN USING TOOLS



How to connect the tools to the network:

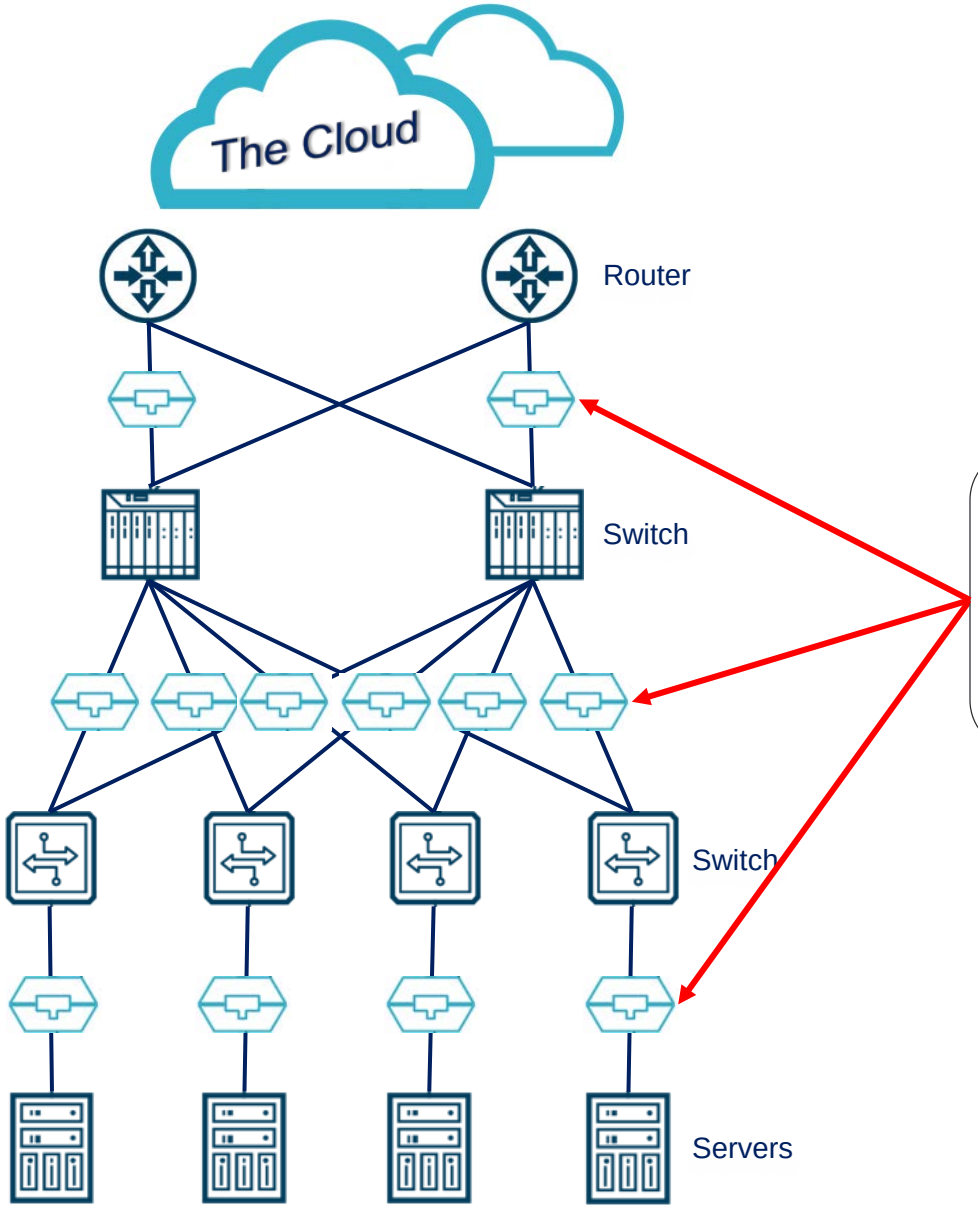
- Different tools are competing for the data
- Poor data quality with SPAN ports
- Different link speeds/standards in the network
- Possible too much data for the tool
- Tunneling protocols maybe in place (VxLan / VnTag)

Tools Farm

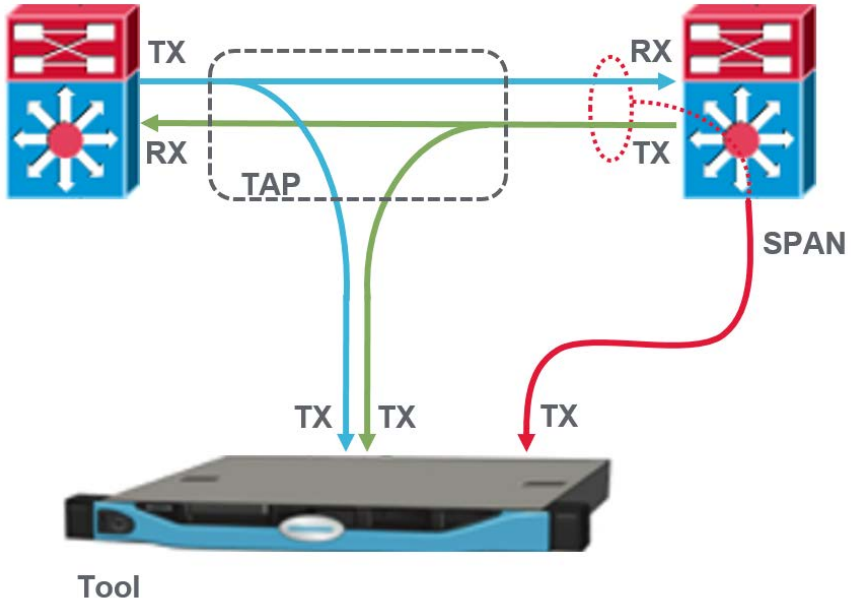


ixia

STEP 1: DEPLOY TAPS



Deploy Ixia TAPs within your network architecture providing you full visibility



ixia

TAP VERSUS SPAN

TAP

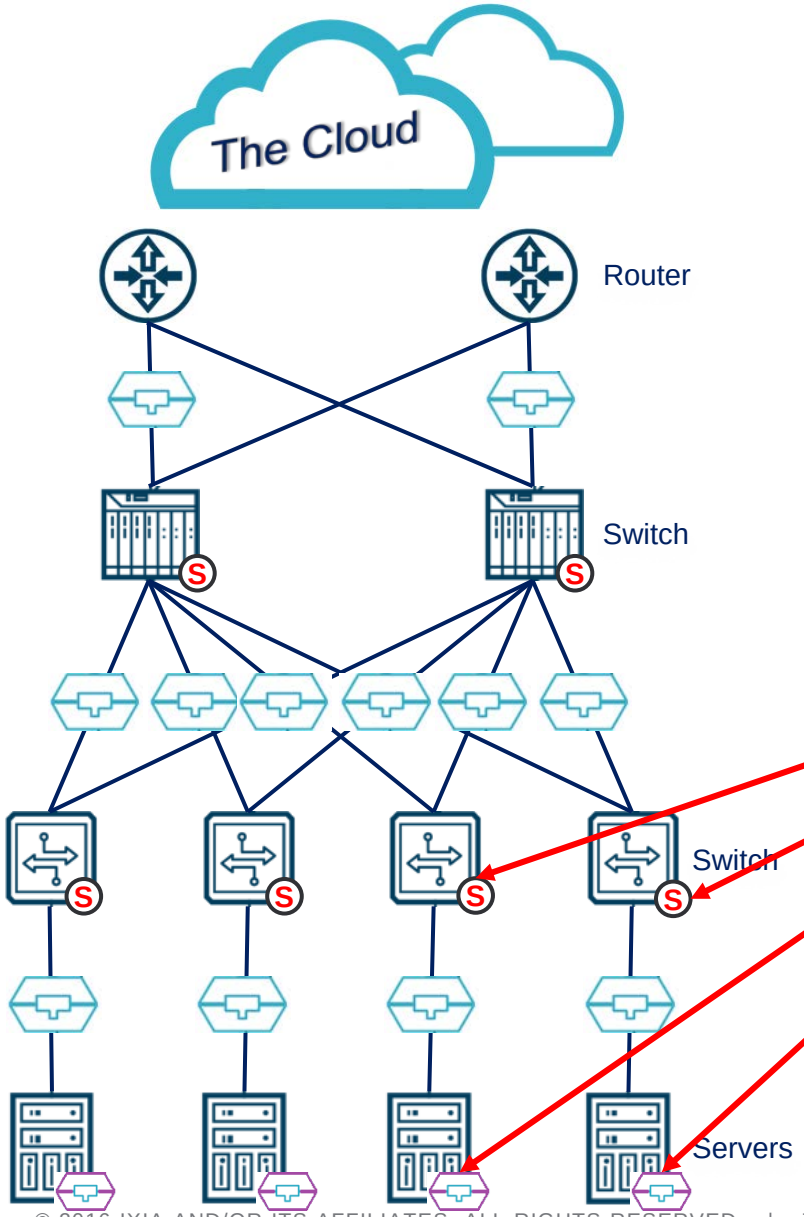
- Full Duplex Taps
  (no packet loss due to aggregation)
- Simplest optical TAPs are safe as houses
  and grow with the Network from GE to 100GE
- Copper TAPs are fail safe even when the power is lost
- Available for all media types:
  Copper: 10M, 100M & 1G
  Optical: Single Mode 1G till 100G
  Multi Mode 1G till 100G
  Cisco Bidi

SPAN

- Limited number of SPANs leads to compromise
  (Multiple tools cannot be used at the same time)
- Have to be configured and maintained
  (Danger working on Production Network)
- Load depended behavior
  (tend to lose packets already at lower processor load)

ixia

STEP 2: DEPLOY CLOUDLENS

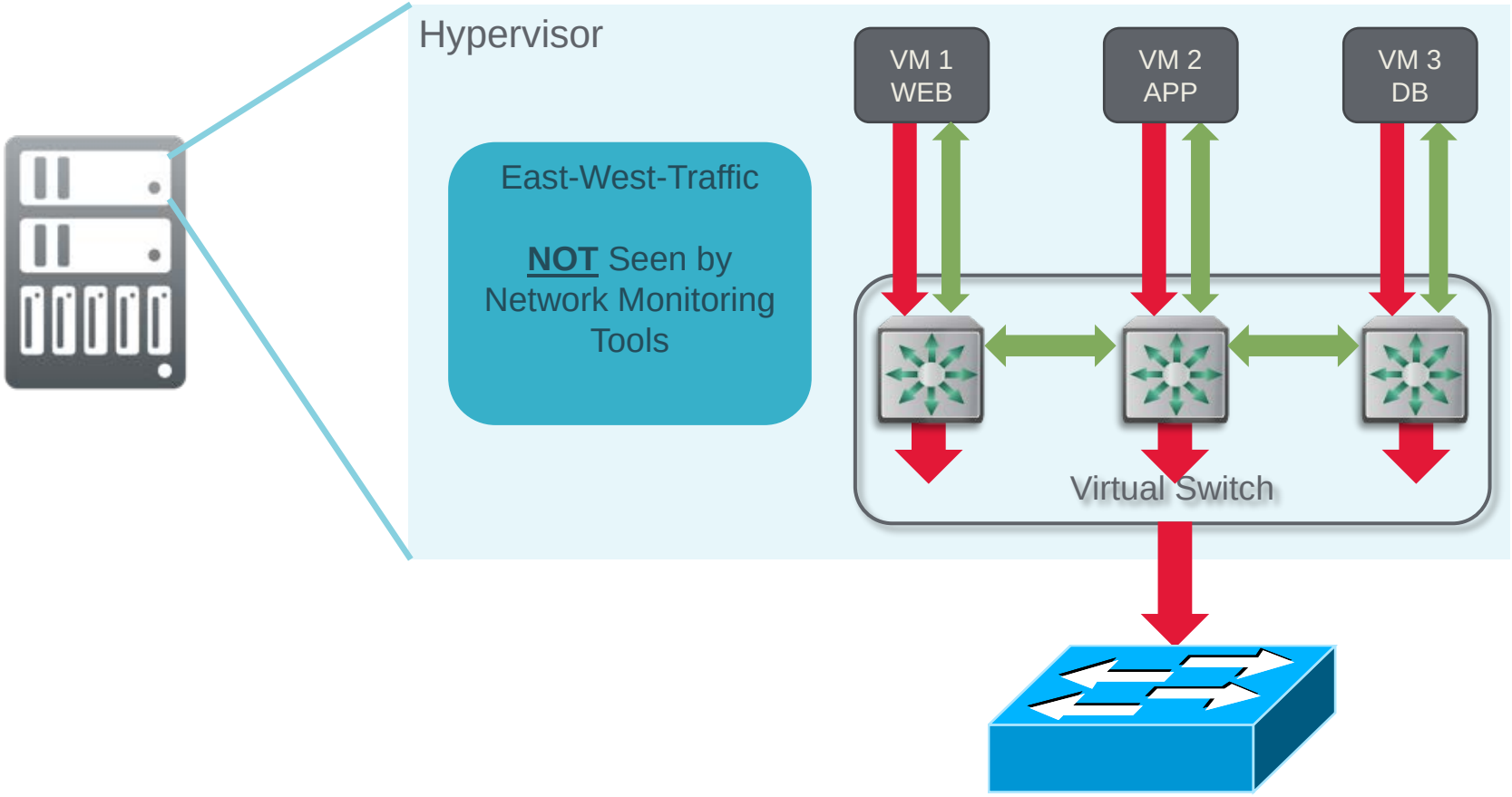


Deploy Ixia CloudLens private solution as virtual Tap

Use SPAN ports as needed

ixia

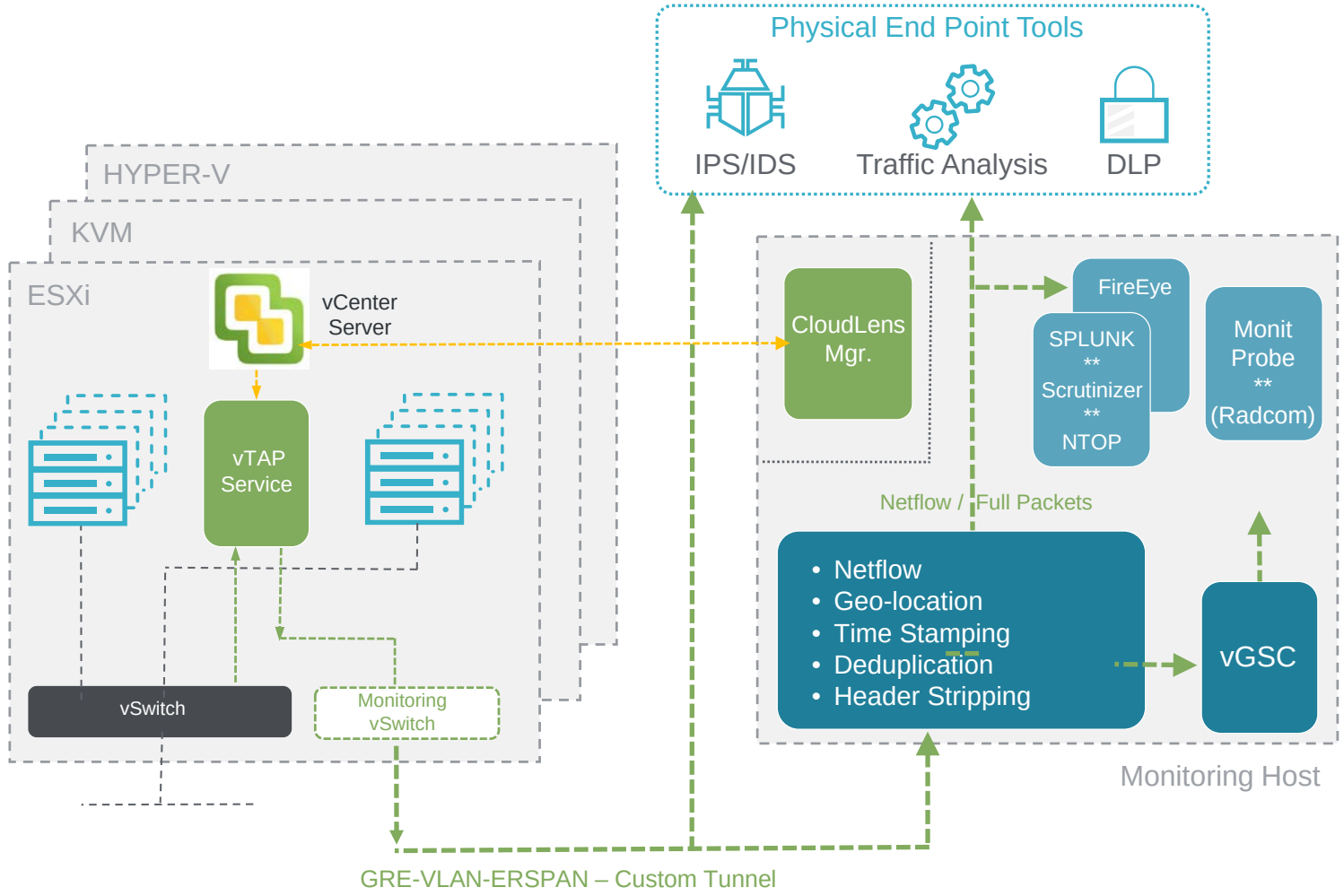
VIRTUAL NETWORKS



ixia

CLOUDLENS PRIVATE

Virtual Datacenter Visibility

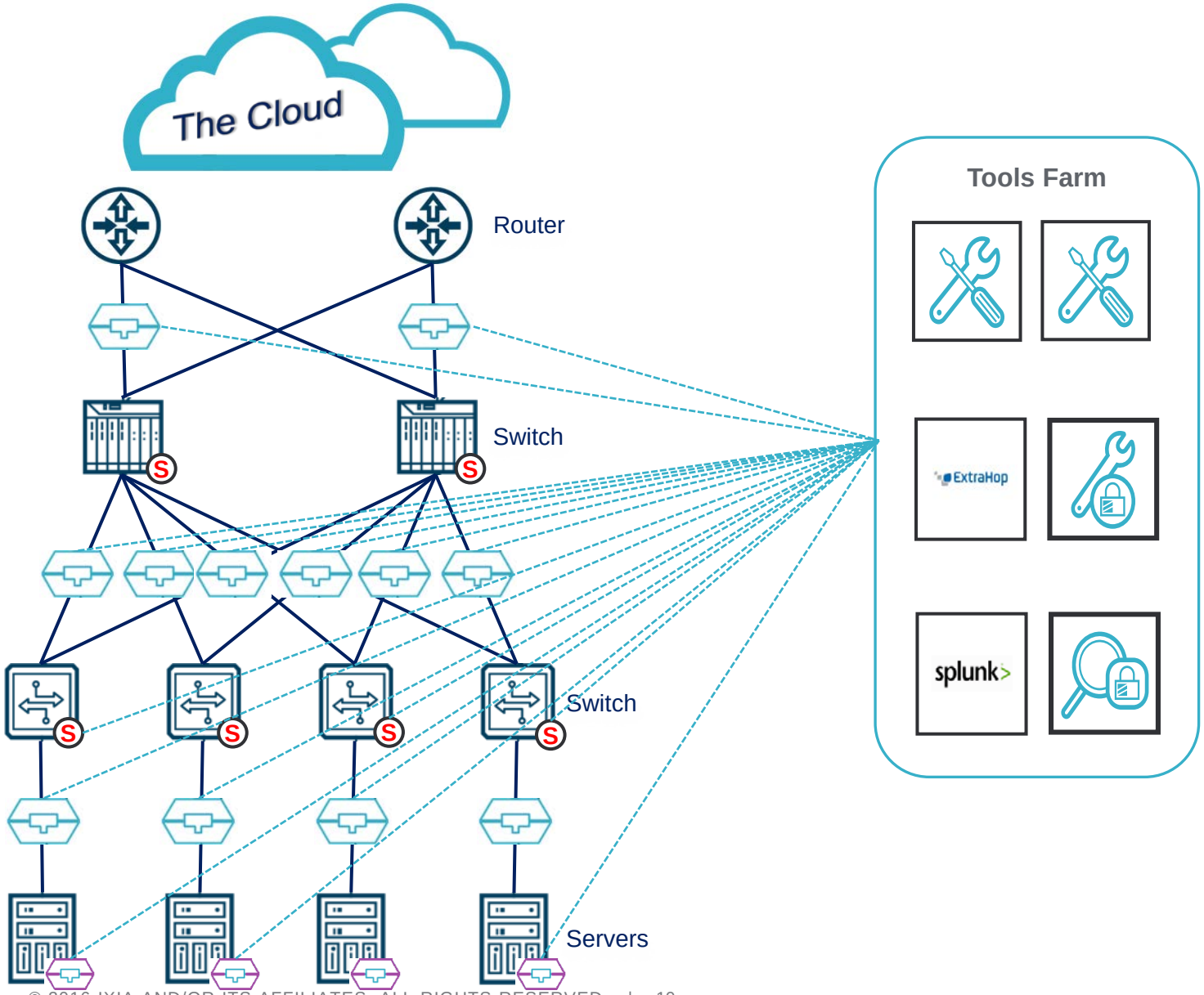


Virtual Traffic Visibility

- Inter-VM Traffic Monitoring
- Multiple Hypervisor Support (ESXi, KVM, Hyper-V)
- GRE – VLAN – ERSPAN Protocols
- Centralized Management

ixia

STEP 3: SOLVE ANOTHER PROBLEM



Granularity can become very costly due to:

> Every TAP requires two tool ports (A>B & B>A)

> Link speed dictates tool speed and performance (very costly for 40G/100G)

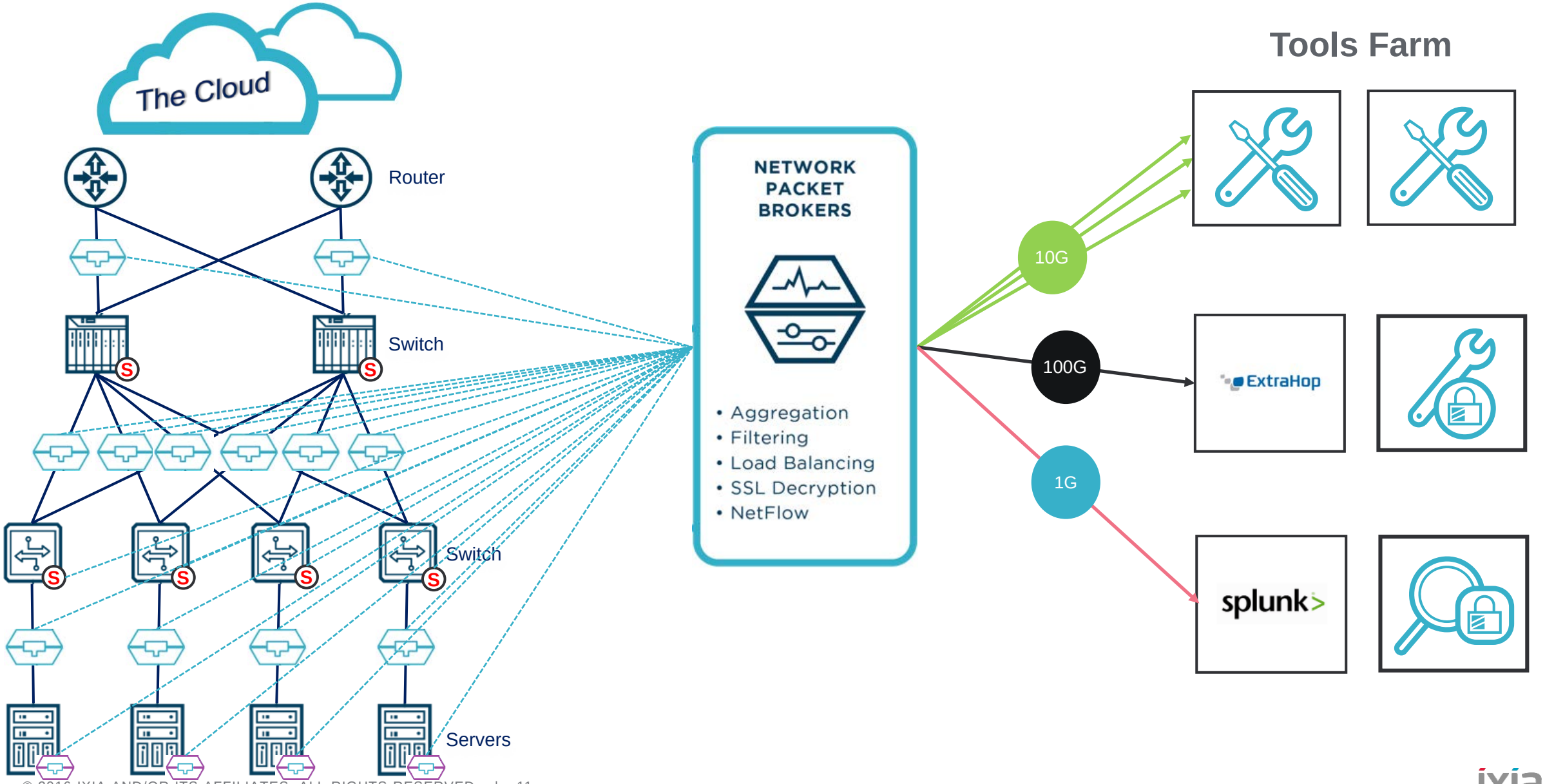
> Different tools are competing against the same TAP or SPAN port

> If not as much tool ports as TAP or SPAN are available engineers need to change ports. (Problems with access control/rights & distance)

> Tools are flooded with unnecessary data

ixia

STEP 4: ADD A PACKET BROKER

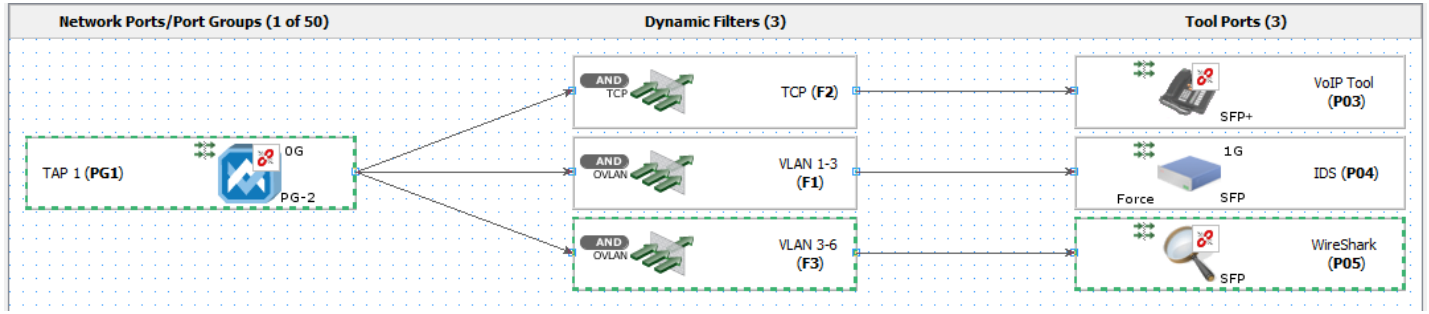


ixia

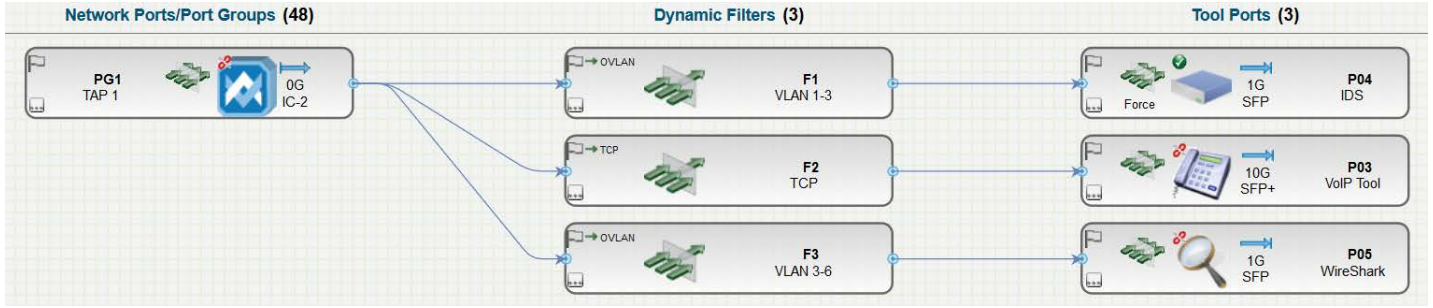
GRAPHICAL USER INTERFACE

The Easy Way (Ixia NTO)

Java



HTML 5



The Hard Way (Other)

Sample Commands – Multi-Rule Filters (VLAN & Ports)

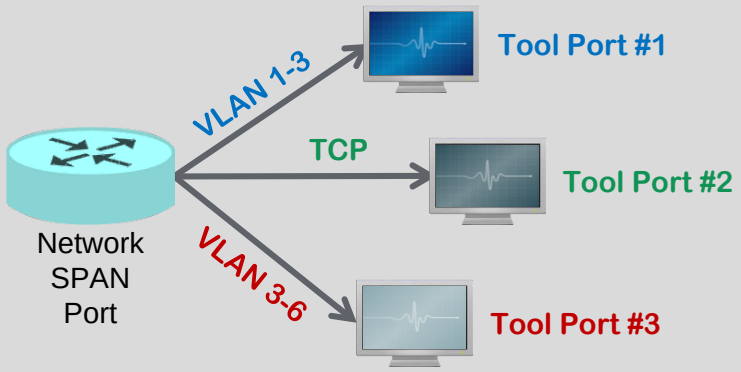
```
# Define Port 1 thru 4 as egress ports (tool ports)), all others are ingress ports by default
config port-type 1 2 3 4 tool

# Define a cross-box "container" named "crossBoxMap"
config xbmap type mt alias crossBoxMap

# Define a multi-rule map filter, first four is for different VLAN ranges
# Tool port 1 & 2 of GigaVUE-1 is for NAC 1A & 1B
config map-rule crossBoxMap rule vlan 100..199 tool 1-1 1-4
config map-rule crossBoxMap rule vlan 200..299 tool 1-2 1-4

# Tool port 1 & 2 of GigaVUE-2 is for NAC 2A & 2B
config map-rule crossBoxMap rule vlan 300..399 tool 2-1 1-4
config map-rule crossBoxMap rule vlan 400..499 tool 2-2 1-4

# Tool port 3 of GigaVUE-1 is for AppMon 1A (which gets traffic for NetBIOS protocols)
config map-rule crossBoxMap rule portsrc 137..139 tool 1-3
config map-rule crossBoxMap rule portdst 137..139 tool 1-3

# Tool port 4 of GigaVUE-1 is for AppMon 1B (which gets everything except protocols)
config map-rule crossBoxMap rule collector tool 1-4

# This designates the ingress ports for the map (Switches 1A, 1B, 2A & 2B)
config xbmapping net 1-19 1-20 2-19 2-20 map crossBoxMap
```


ixia

IXIA'S AUTOMATIC RULE ENGINE COMPILER

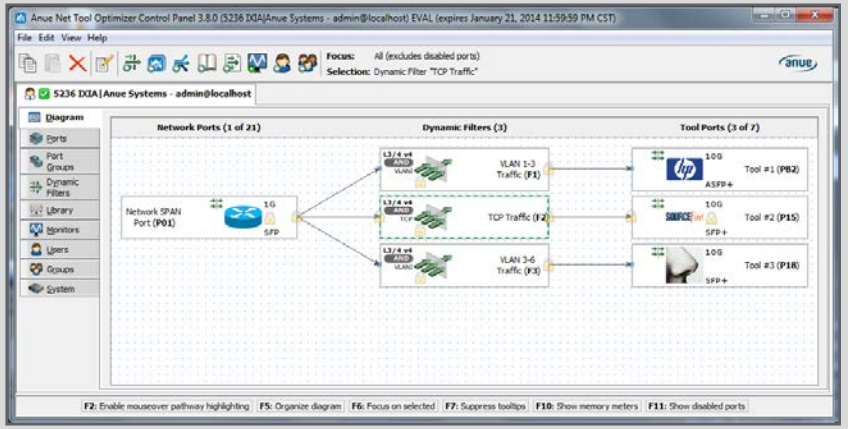
1. What you want

Traffic multi-casted from one SPAN port to 3 tools



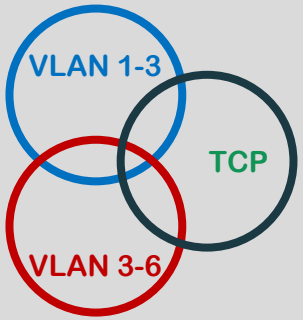
2. What you do

Enter 3 simple filters in the Network Tool Control Panel



3. What Automated Rule Set Compiler does

Automatically calculates filter overlaps, and creates rules



No.	Criteria	Action
0	VLAN 3 + TCP	Tool 1, 2 & 3
1	VLAN 1-3 + TCP	Tool 1 & 2
2	VLAN 4-6 + TCP	Tool 2 & 3
3	VLAN 3	Tool 1 & 3
4	VLAN 1-2	Tool 1
5	VLAN 4-6	Tool 3
6	TCP	Tool 2
7	Null	Drop

4. Why is this a big deal

- Automatically resolves overlapping rules. Greatly simplifies getting to what you need.
- Hitless changes – no packets dropped
- Concurrent changes by different admin users
- Simple to integrate with external provisioning systems – automated service provisioning

ixia


ixia
THANK YOU