Taking Wireshark to the Future Networks

June 15, 2011

Patrick P. Leong
CTO | Gigamon

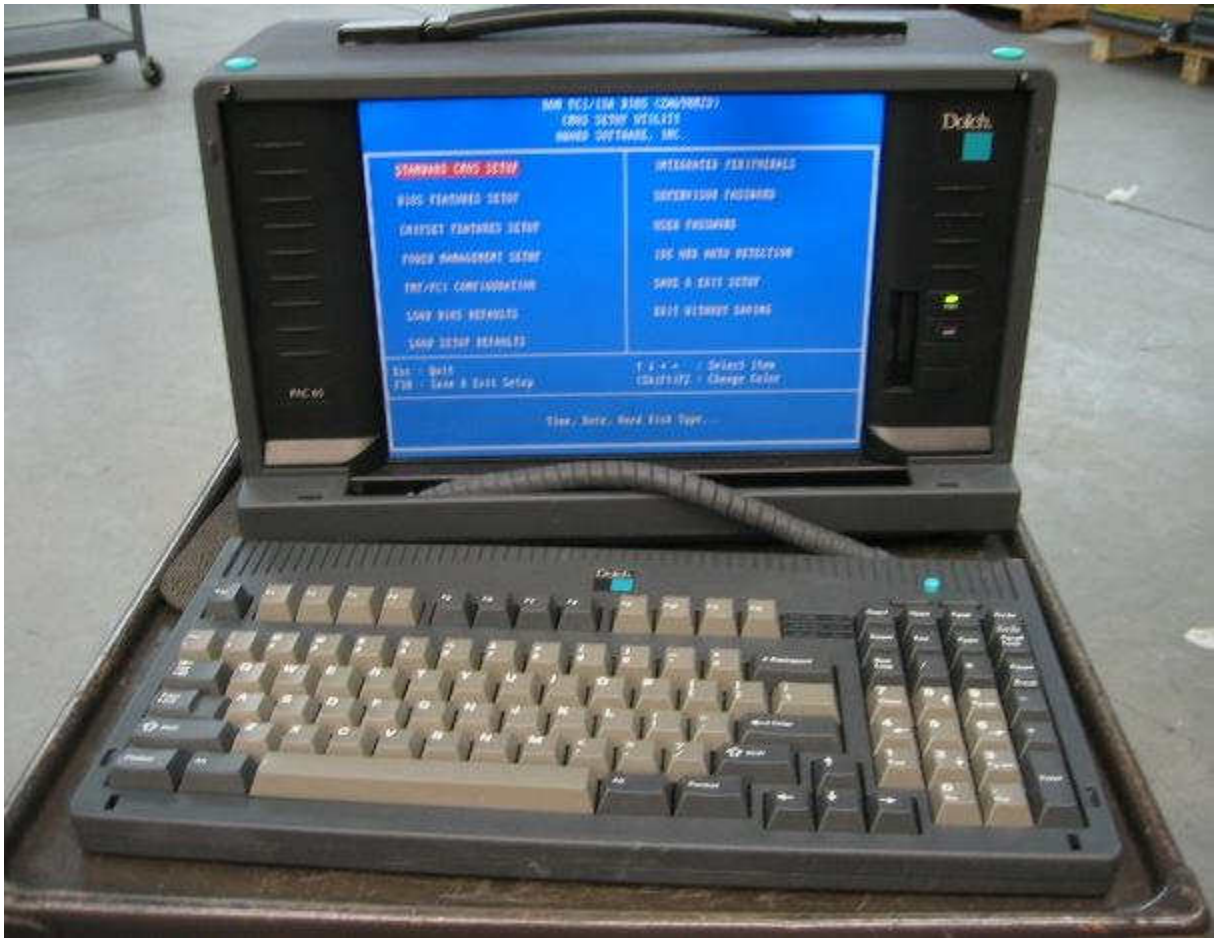
SHARKFEST **'11**
Stanford University
June 13-16, 2011

Outline

- Wireshark --- Perspective from a DOS Sniffer Developer
- New Trends in Network Monitoring & Security
- Challenges facing a Wireshark type of device
- Where we can go from here
- Summary

A Little Bit of History

Network General DOS Sniffer
1986-1997



Some Highlights of DOS Sniffer

- Multiple Network Interfaces:
  10/100, Token Ring, WAN (T1, E1, HSSI), ATM
- Purpose-Built PC (Dolch boxes)
- Traffic Generation Capability
- Expert Analysis and Statistics
- Distributed and Standalone Systems
- Service & Support
- $$$

In 1998, Network Associates started migrating DOS Sniffer to the Windows-based SnifferPro.

Wireshark (formerly Ethereal)

- Started in 1998
- Open Source
- Runs on Windows, Linux, Solaris, FreeBSD and other operating systems
- Supports many capture file formats
- Rich set of decodes
- FREE!

The Network—Now & Then

- Speed: 10M, 100M, 1G, 10G, 40G, 100G…
- Duplex: Half to Full
- From Hub to Switch, and Asymmetric links
- Ethernet dominates, with a lot more traffic
- Virtualization
- More Regulations and Compliances (SOX, HIPPA, PCI etc.)
- Security is a Must-Have
- *There are always problems with the Network*

Network Problems Getting Worse…

Difficult to Access Crucial Data at the Right Time

Fragmented, Complex, Expensive, and Inefficient

Visibility

- Lack of visibility – fragmented monitoring approaches provide network engineers limited access to particular points in the network for multiple tools

Cost

- Significant management overhead and monitoring costs – high CapEx and OpEx given fragmented configuration and layout of tools

$$$$

Utilization

- Lack of centralized data capture leads to inefficient utilization of tools – tools in low volume areas are undersubscribed while those in high-volume areas are oversubscribed

Scalability

- Lack of scalability – requires multiple expensive devices to be deployed across network boundaries, creating complexity, performance and management issues

Network Operator's Toolbox

- Wireshark: Great for packet level sniffing
- Application response time monitors
- Customer experience monitors
- Intrusion detection systems
- Intrusion protection systems
- Forensic recorders
- Other specialized monitors

Challenges

Disclaimer:

Wireshark is a great tool!

The challenges listed here are mainly discussions from a technical/architectural standpoint. It applies in general to any PC-based analyzer.

Challenges

#1: Throughput due to PC based architecture

Example:

10G pipe going to a 1G laptop interface:

May randomly drop packets due to over-subscription

Solution:

Some kind of hardware-based pre-filtering

Challenges

#2: Lack of aggregation capability

Example:

Capturing traffic from an asymmetric link

Solution:

Aggregation taps, data access switches

(But watch out for bandwidth over-subscription as we aggregate, use hardware pre-filtering)

Challenges

#3: Coarse time-stamping (msec resolution)

This is constrained by the clock resolution of the underlying OS running inside the PC hosting the Wireshark

Solution:

Hardware-based time-stamping (nsec resolution) with interpretation by Wireshark

e.g. Gigamon's GigaSMART blade (GPS, PTP, timestamp decode supported by Wireshark)

Challenges

#4: Handling of Duplicate Packets

Wireshark can do some post-capture de-duplication via `editcap -D`

- But what is considered a duplicate?
- Can this be done in real time?

Solution:

Hardware-based de-duplication engine with line rate processing capability

Challenges

#5: Competing for span port access

Tool many tools, not enough span ports

Too many span sessions degrades the switch or router's performance

Solution:

External taps (dump taps)

Intelligent data access switches

Challenges

#6: Lack of visibility due to Virtualization

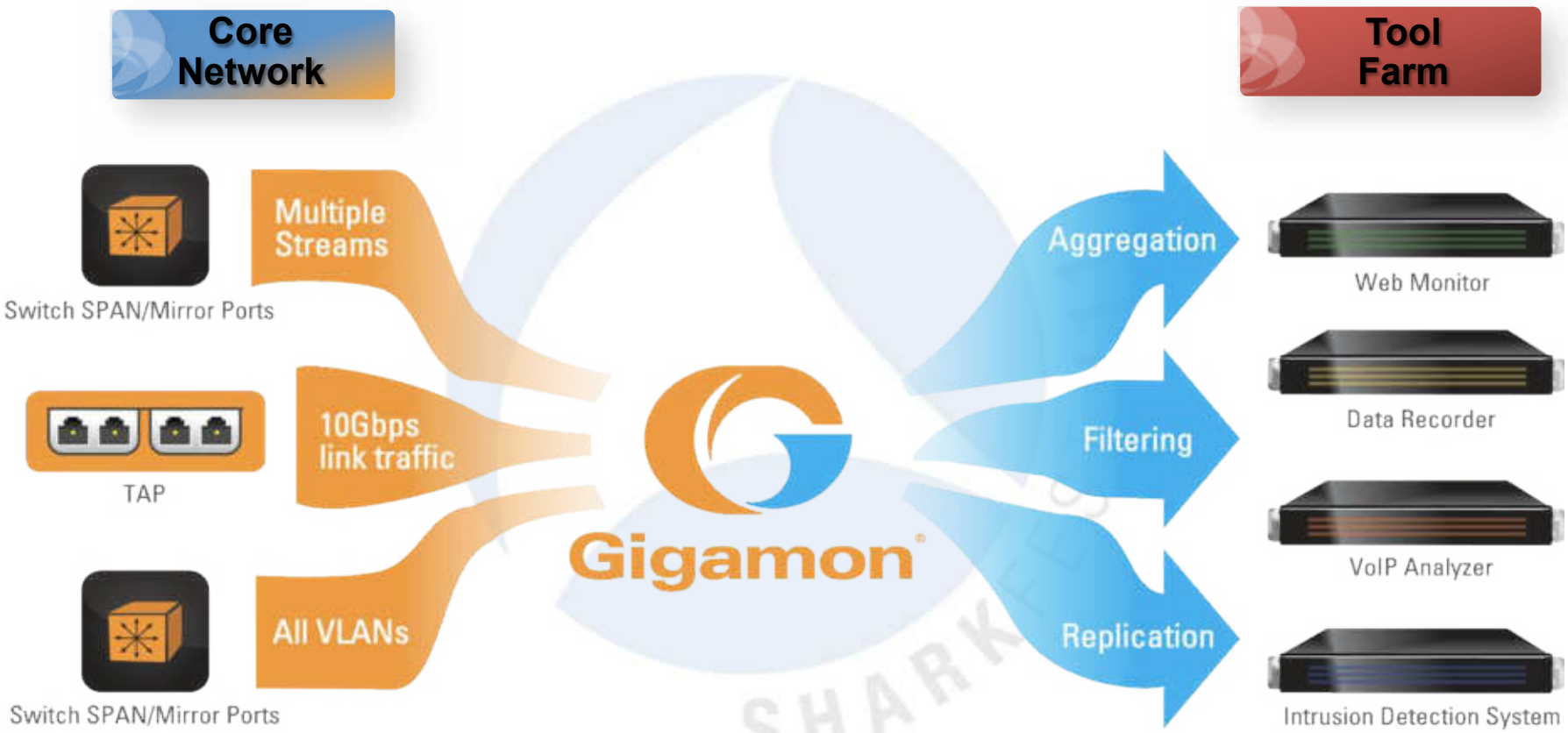
Traffic between virtual guest machines within the same physical host is generally invisible to the outside

Solutions:

Specialized switches that can span virtual traffic out to the physical world

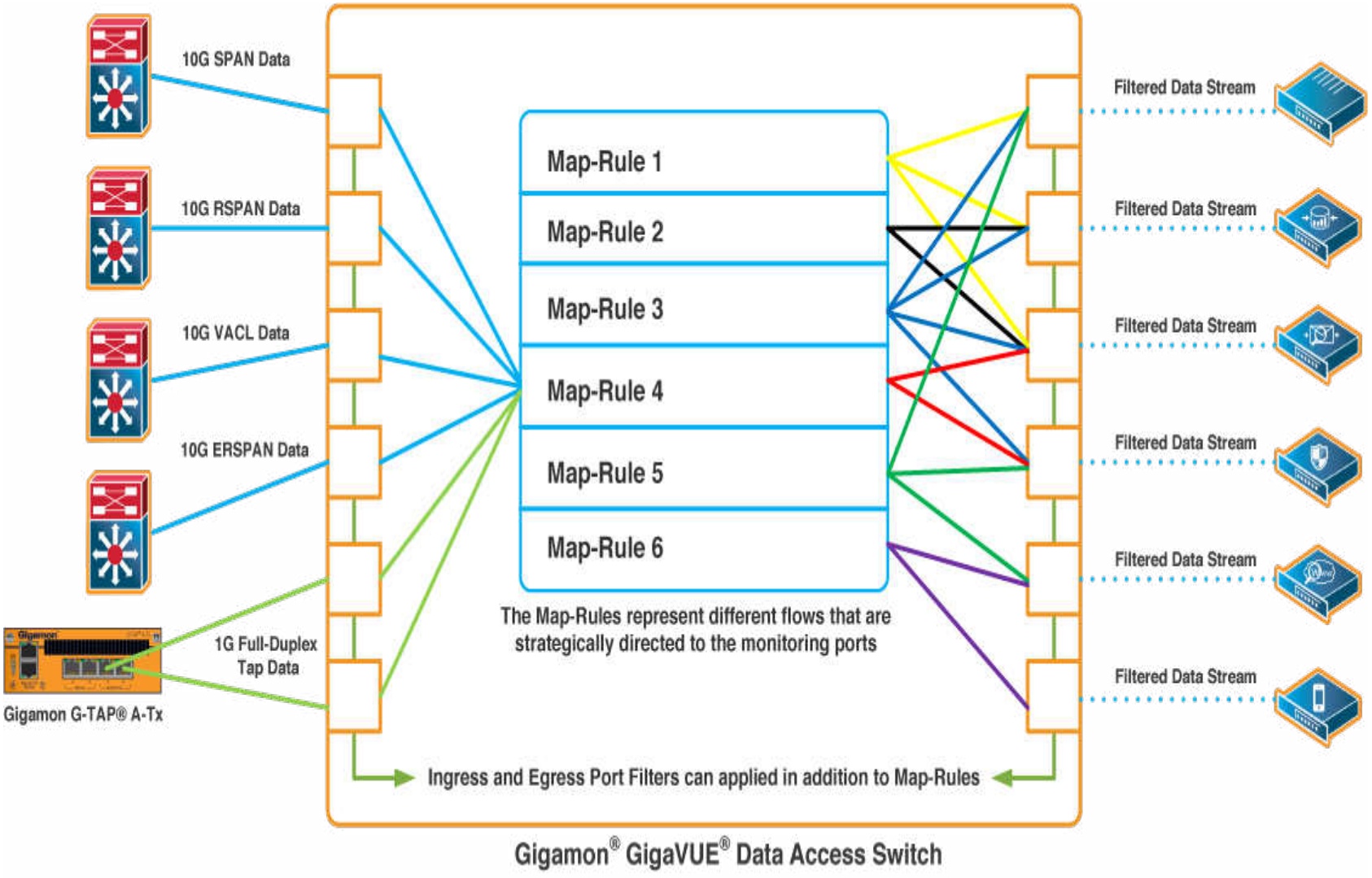
Thin layer of spanning software at hypervisor

Intelligent Data Access Switch



Flow-Mapping®

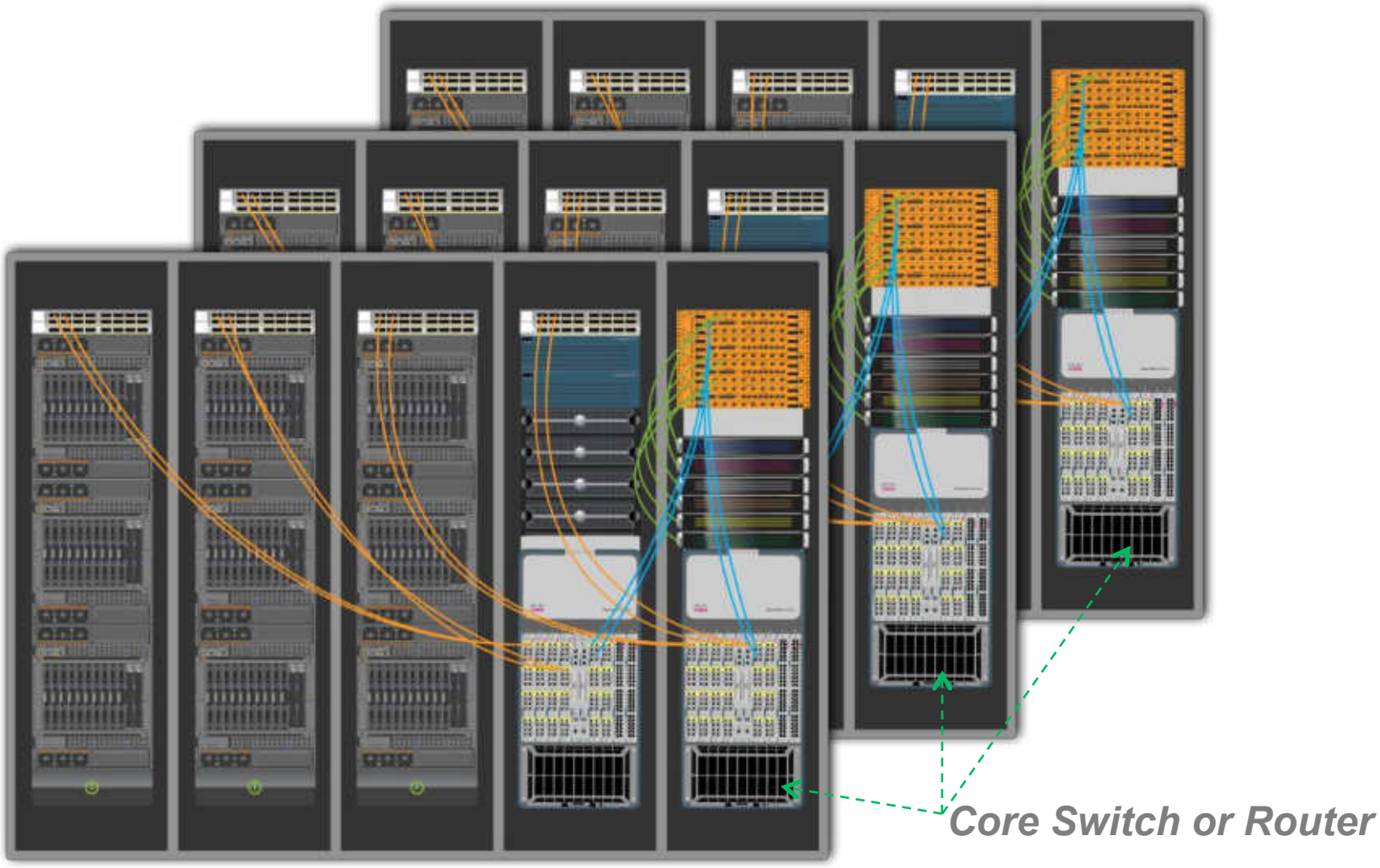
Smoothing out the line speed transitions on network and tools



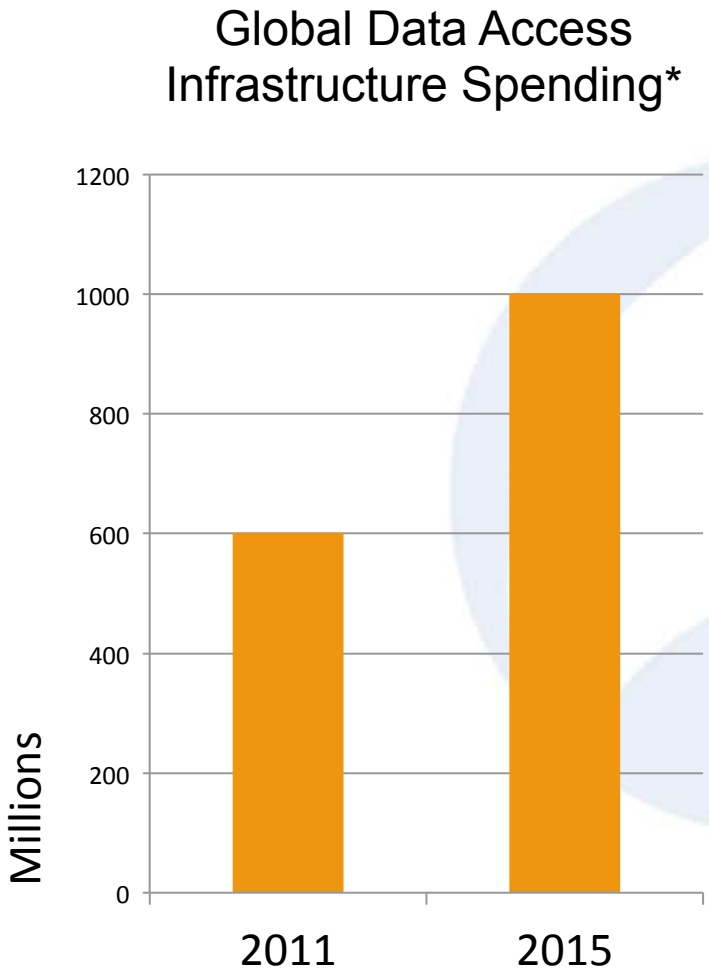
Intelligent Data Access Switches

- No more competition for span port access
- Hardware-based ingress and egress filters
- Flow-Mapping
- Built-in taps, with failover protection
- User access control (can be authenticated by a AAA server
- Load-balanced outputs to tools
- SNMP traps and syslogs
- Flexibility of adding new tools with no traffic disruption

Deployments in Data Centers



Rapidly-Growing New Market



Driving Forces

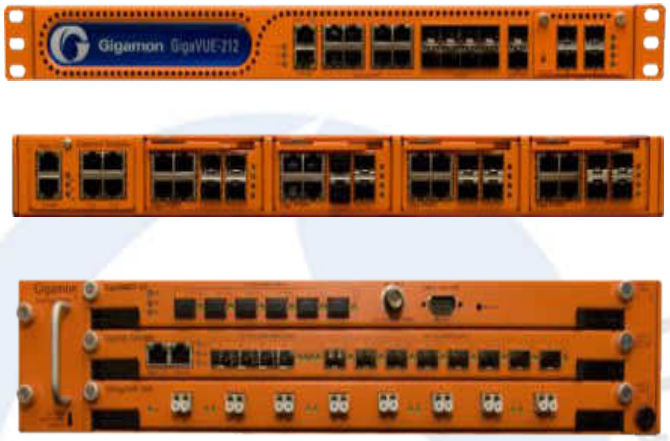
- **Explosive Growth of Data**
  Too Many Packets (double every 2 years)
- **Fast Adjacent Market Growth**
  An 'Enabling' Technology
- **Accelerated Innovation**
  10/100 -> 1G → 10 G → 40 G → 100G
- **Cloud Computing**
  Rapid Data Center Build-outs & Consolidation

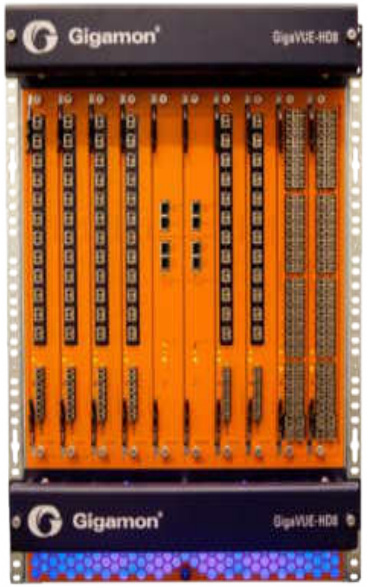
*Source: estimates came from Gigamon internal research

Intelligent Data Access Switches

GigaVUE 212/420/2404 HD-8

Intelligent Data Access Appliances

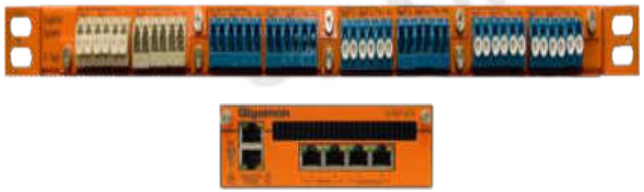




GigaSMART

DPI & Packet Modification Blade

GTAP & GTAP-A



Scalable & Intelligent Passive/Active TAPs

Some Possibilities

- Enhanced capture file format for handling hardware-based timestamps and other hardware-based tags on a per packet basis

- For virtual environment, an open source libpcap engine running in the hypervisor?

Summary

- New networks and data centers require 24x7 monitoring and security
- Providing traffic access for tools is an issue
- User-control over traffic access for security and compliance
- Differences between network line rate and tool capacity needs hardware scope-down
- Virtualization is a challenge but not a dead-end
- Data Access Switch provides a viable solution

Thank You

Contact information

Gigamon
589 Gibraltar Drive
Milpitas, CA 95035
408.263.2022
info@gigamon.com