SHARKFEST '13

Wireshark Developer and User Conference

Enabling Visibility for Wireshark across Physical, Virtual and SDN

Patrick Leong, CTO Gigamon

Agenda

- A review of the network then and now
- Challenges in network monitoring and security
- Introduction to Traffic Visibility Fabric
- Virtualization and its visibility implications
- SDN
- PCAP-NG file format

About Gigamon

- Founded in 2004, HQ at Milpitas, California
- Creator and Leader in Traffic Visibility Fabric
- 1000+ End Customers
- 60 of Fortune 100, 50 of Top 100 Global Service Providers
- Went public on June 12, 2013

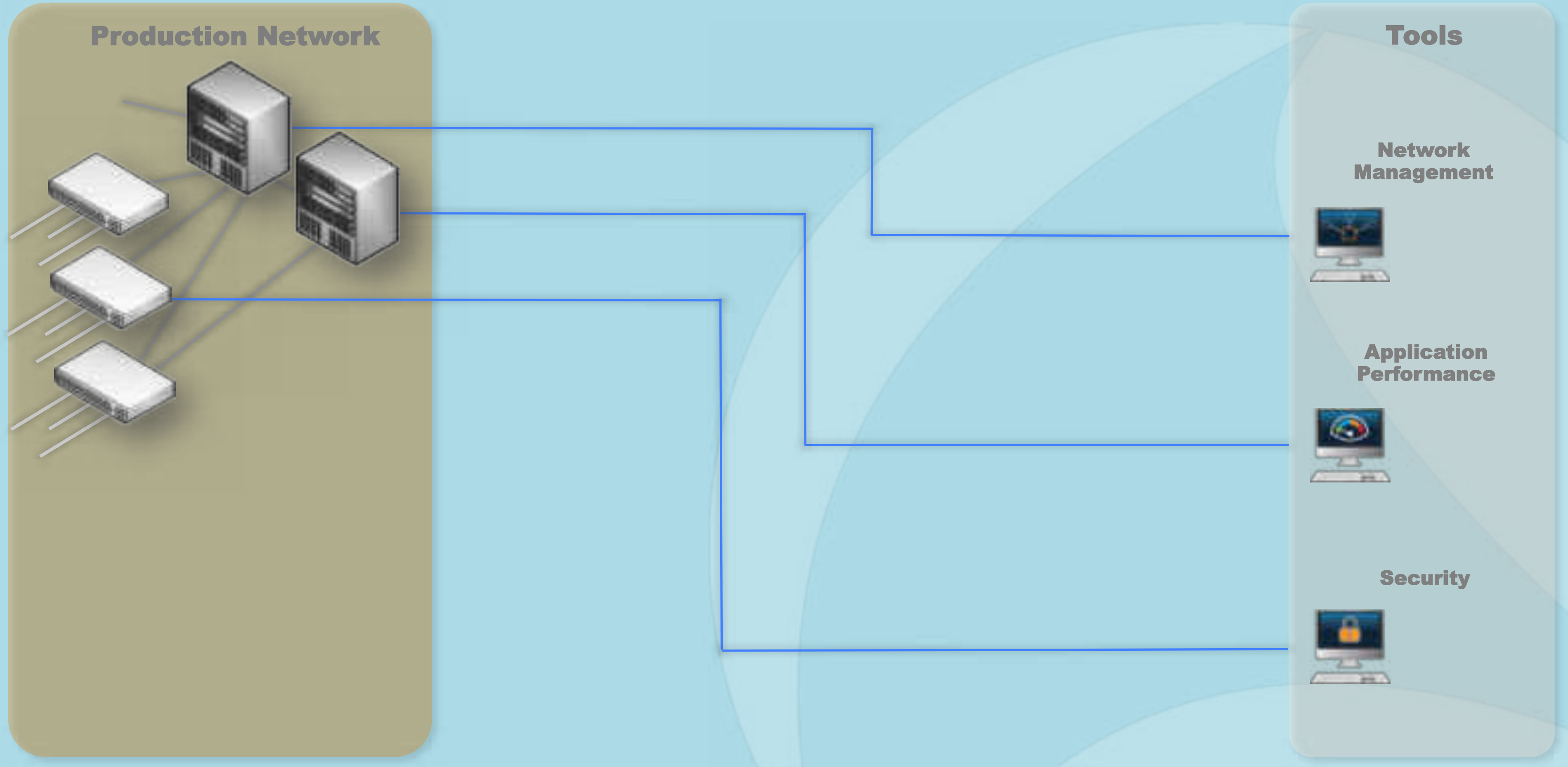
The Network – Then and Now

- Speed: 10M, 100M, 1G, 10G, 40G, 100G…
- Duplex: Half to Full
- From Hub to Switch, and Asymmetric links
- Ethernet dominates, with ever increasing traffic
- Big Data, Mobility, Virtualization, and SDN
- More Regulations and Compliances (SOX, HIPPA, PCI etc.)
- Security is a Must-Have
- *There are always incidents with the Network*
- *Network downtime is increasingly costly*

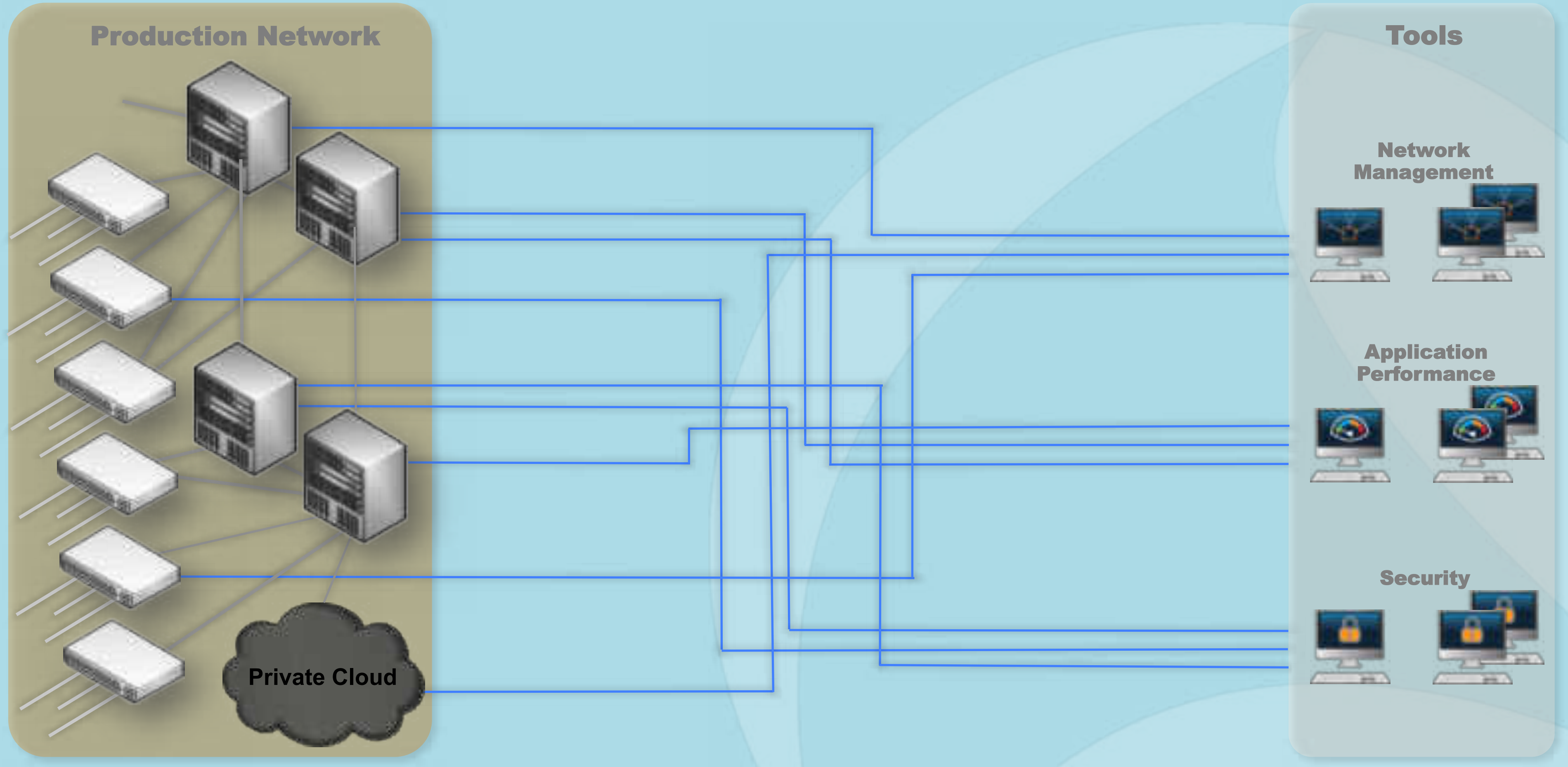
A Network Operator’s Toolbox

- Wireshark: Great for packet level sniffing, and it’s free!
- Application response time monitors
- Customer experience monitors
- Intrusion detection systems
- Intrusion protection systems
- Forensic recorders
- Other specialized monitors

Traditional Network Monitoring Setup



As the network becomes more complex



Issue: Multiple Tools Completing for Span Port Access

- Too many tools and not enough span ports
- Each tool may want a different view of the same traffic
- A switch cannot provide too many span sessions
- Spanning is not the primary function of a switch or router

Issue: Signal Strength Budget for Deploying Multiple External Taps

- A few external taps over a link is enough to degrade the signal strength
- Rack space issue with too many external taps
- Many external taps have no management interface
- Security issue

Issue: Throughput Limitation of the Tools

- Many tools have a PC-based architecture due to the complexity of performing packet analysis
- Subject to driver (e.g. Winpcap, Libpcap) throughput, DMA throughput, disk writing throughput etc.
- Processing throughput of a tool can be lower than its interface throughput
- Random dropping of packets when a tool cannot catch up with big pipe traffic
- Happens over and over again as network speed increases and tool throughput is usually lacking behind

Issue: Lack of Aggregation Capabilities

- Aggregation of network traffic from multiple ingress points to a single tool
- Capturing traffic from an asymmetric link
- Serving situations where a tool is under-utilized
- Aggregation can be extended across a traffic visibility fabric
- Aggregation and multiplexing go hand-in-hand

Issue: Coarse Time-Stamping Precision

- PC-based time-stamping is constrained by the clock resolution of the underlying OS of any PC-based tool
- Millisecond resolution is typically the best resolution for PC-based time-stamping
- Need higher precision (nano-second resolution) and higher accuracy (GPS, IEEE 1588 synced) time-stamping for high speed networks
- Need hardware-based time-stamping as close to the production network as possible

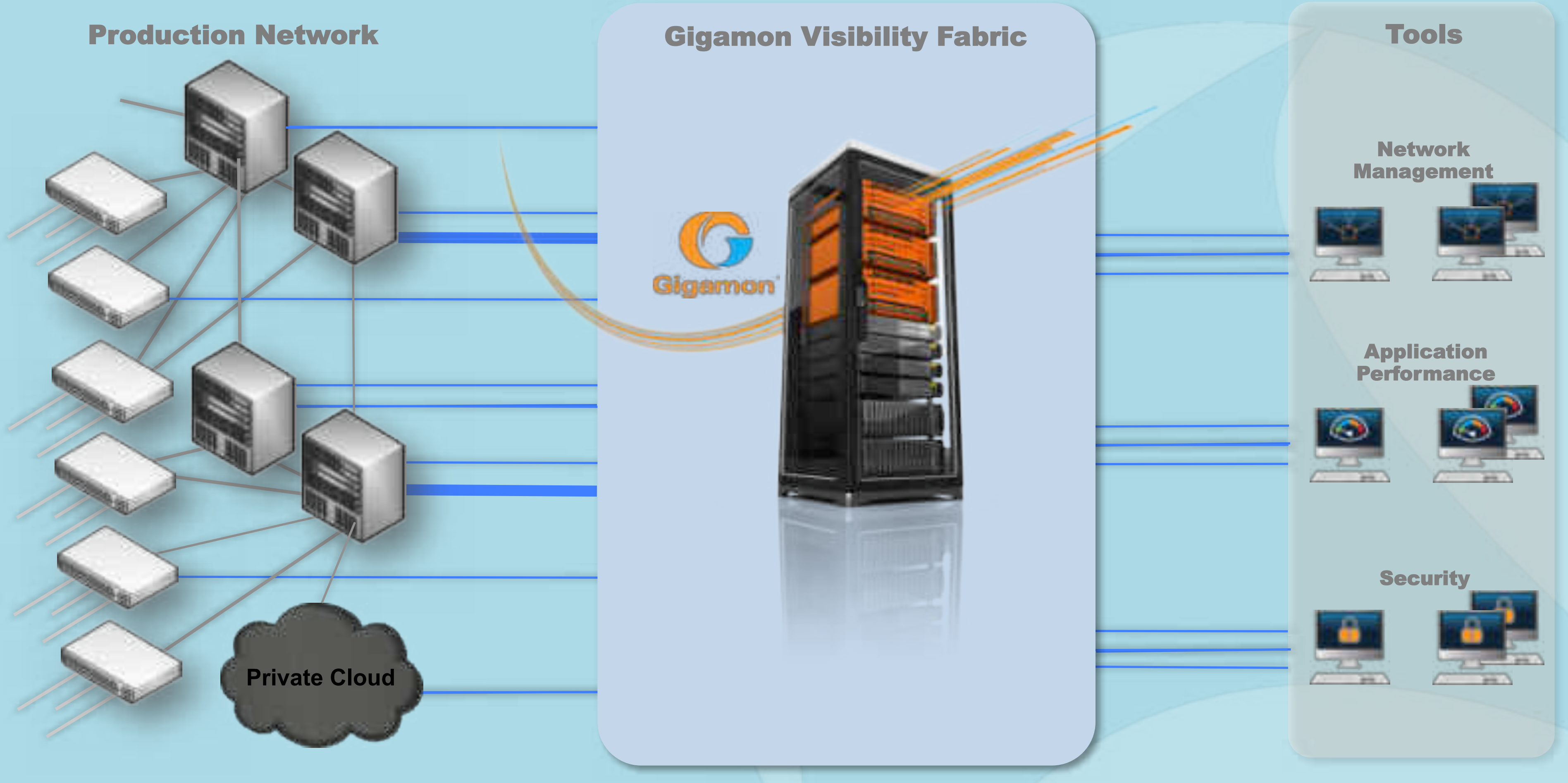
Issue: Multiple User Tenancy

- Large organizations usually have multiple teams: e.g. Network, Security, Compliance, User Experience Teams
- Different teams may have different tools that all need to have access to the same traffic
- Different teams may want a different view of the same network traffic
- Teams stepping into each other is a common issue

Issue: Inability to handle duplicate packets for some tools

- Duplicate packets may come from:
  - Ingress and egress span session of a switch
  - A packet being tapped as it traverses across multiple links
- Duplicate packets usually show up within a small time window (< a few milliseconds)
- Some tools get confused when seeing duplicated packets
- Need line rate de-duplication function with adjustable time window
- May also need to replicate all packets to other tools

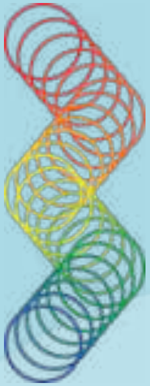
Traffic Visibility Fabric



Traffic Visibility Fabric Requirements

- Enable departments to centralize their tools and bridge data to the tools across disparate islands of physical, virtual and SDN worlds

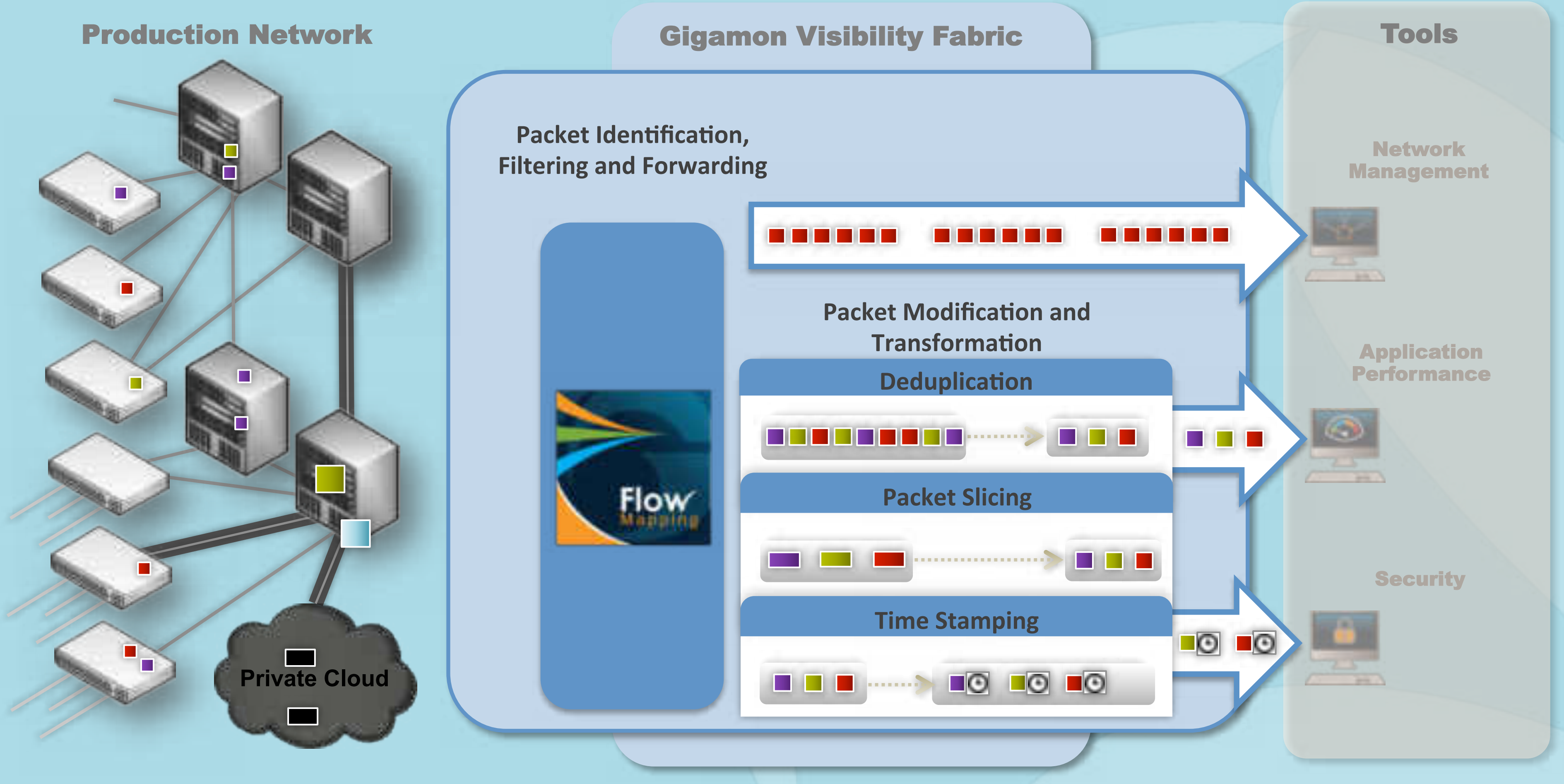
- Ability to normalize and optimize traffic to the tools across the islands of users, virtual machines, devices and applications to enable tool optimization
- Ability to offer a flexible policy engine that enables parallel monitoring policies to serve multiple departments simultaneously
- Enable just-in-time tuning of the visibility fabric in response to real-time events within the network through automation and programmability



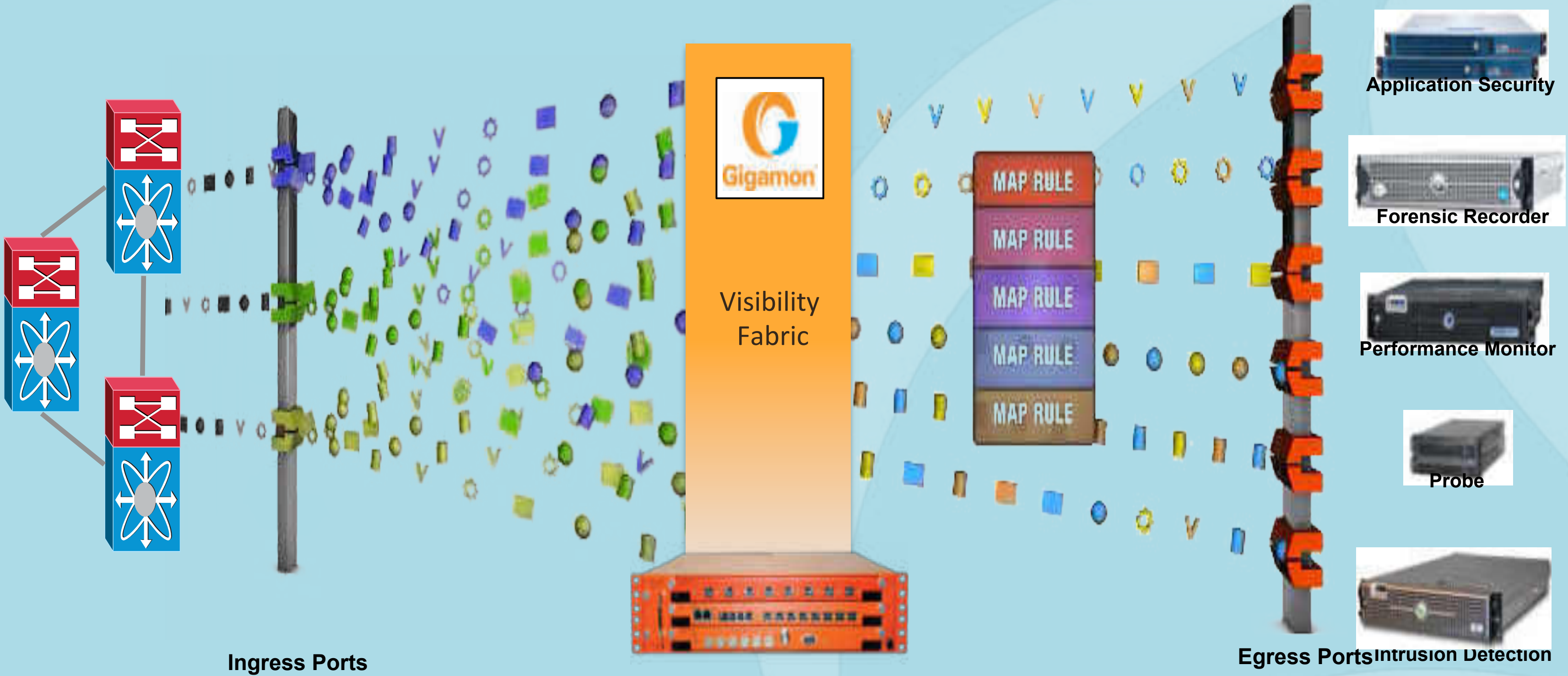
Traffic Visibility Nodes: Building blocks of a Traffic Visibility Fabric

- Hardware-based aggregation and multiplexing of packets from network to tool ports
- Hardware-based time-stamping (nanosecond resolution, GPS and IEEE 1588 synced)
- Intelligent Flow Mapping
- Special packet processing and modification
- Scalable into clusters
- Support Multi-User Tenancy

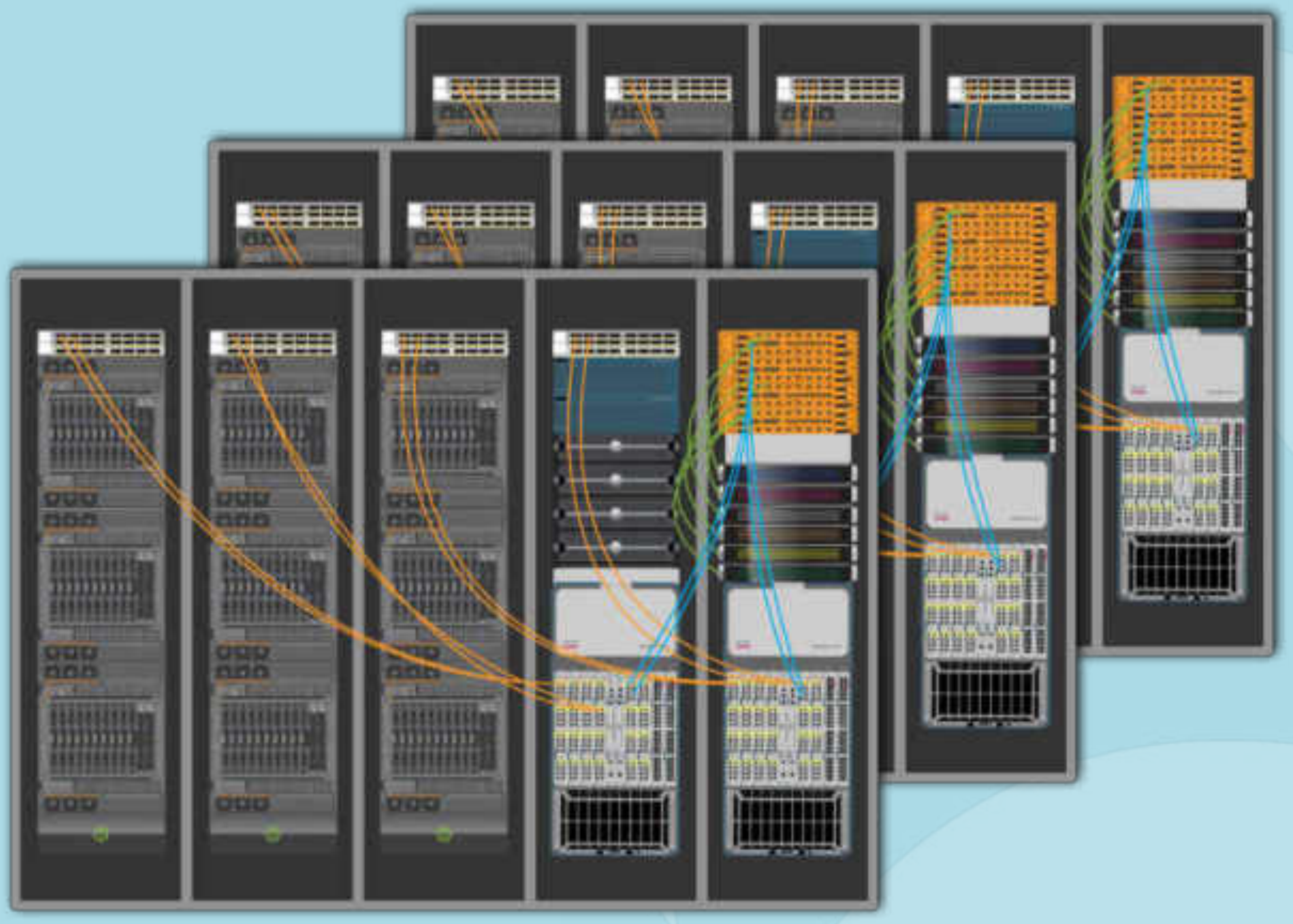
The Heart of Gigamon Traffic Visibility Fabric



Flow Mapping



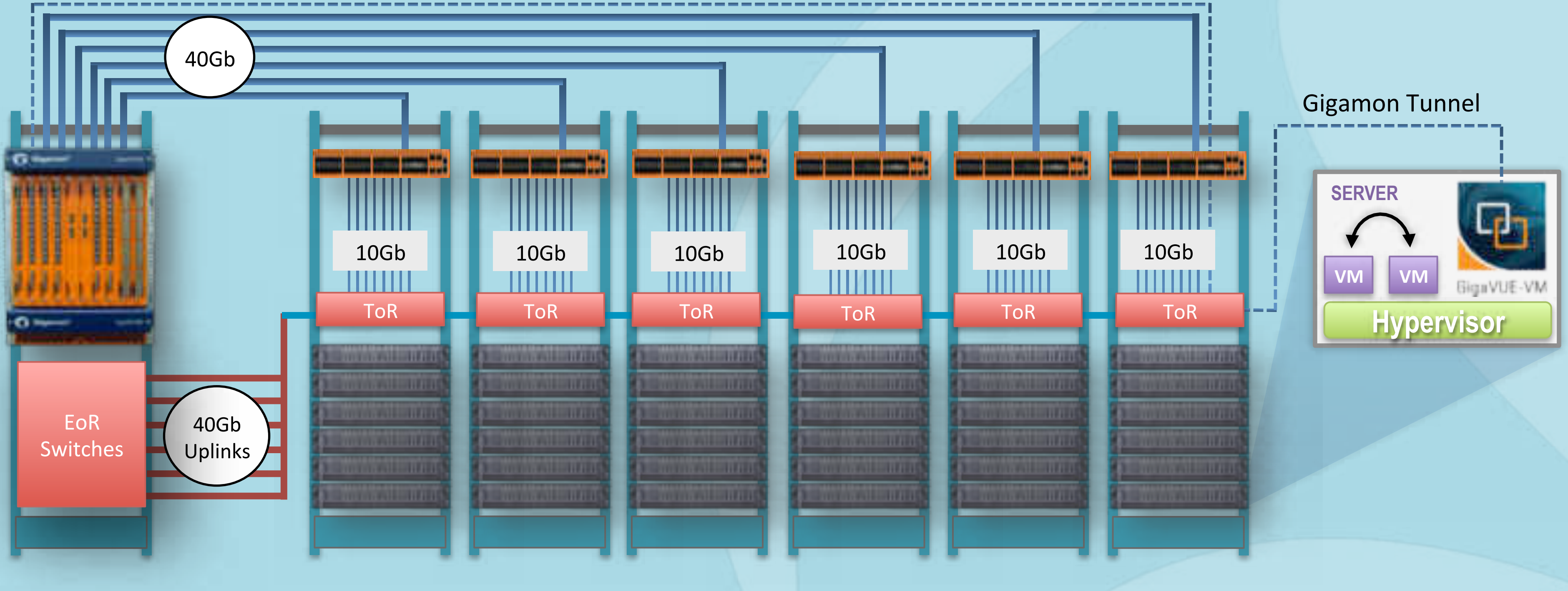
Top of Rack Deployment of Visibility Nodes



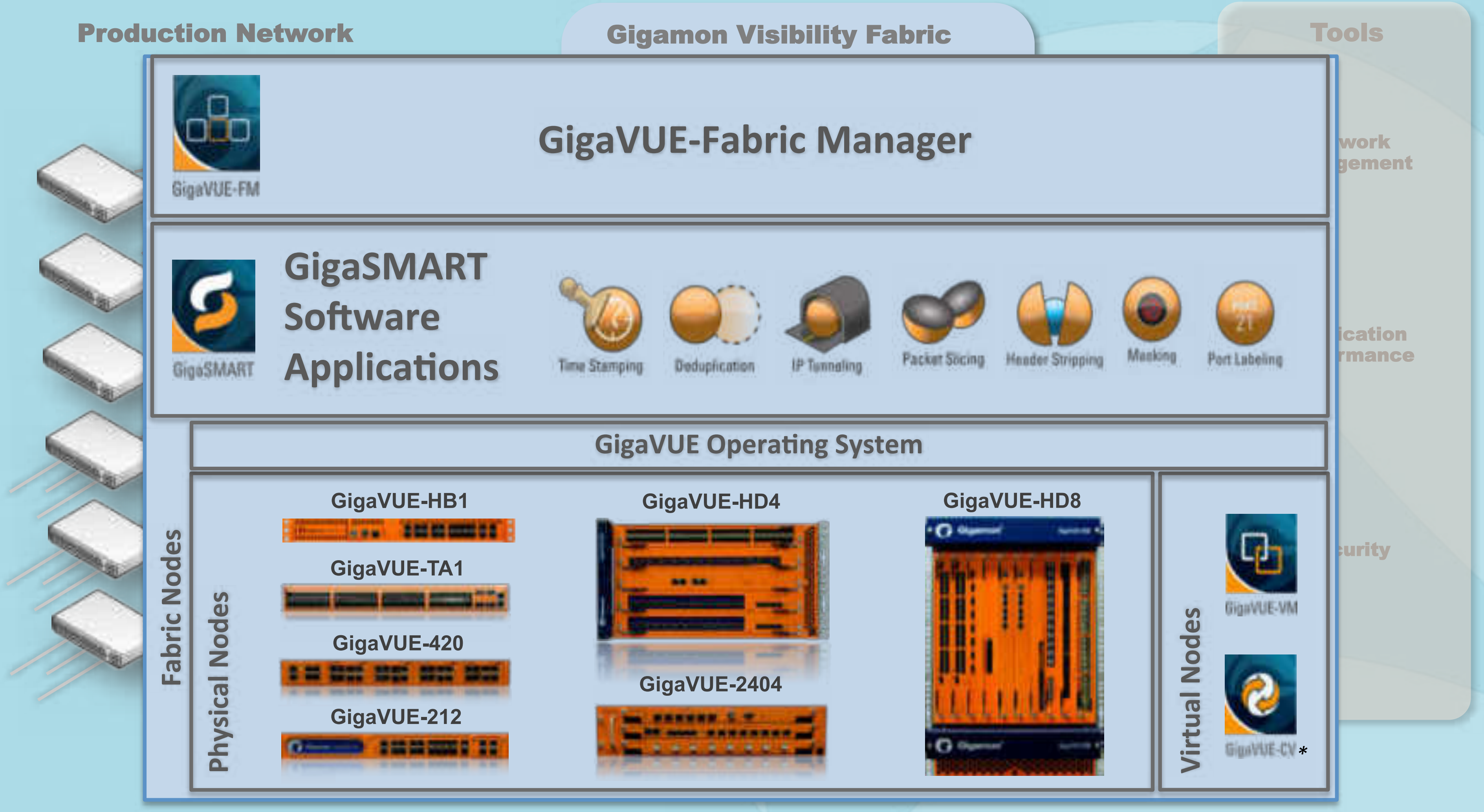
Virtualization and Network Visibility

- Traffic between virtual machines within a physical host is not visible to the outside
- Re-deployment of a virtual machine from one physical server to another brings along networking issues
- Virtualized networks introduce new encapsulation headers (e.g. VxLAN, NVGRE) that some tools may not understand
- Allow user to enforce a high level monitoring policy

GigaVUE-VM: Bringing the gap between physical and virtual worlds



Gigamon Traffic Visibility Fabric Portfolio



Production Network

Gigamon Visibility Fabric

Tools

GigaVUE-Fabric Manager

GigaSMART Software Applications

GigaVUE Operating System

Fabric Nodes

Physical Nodes

GigaVUE-HB1

GigaVUE-TA1

GigaVUE-420

GigaVUE-212

GigaVUE-HD4

GigaVUE-2404

GigaVUE-HD8

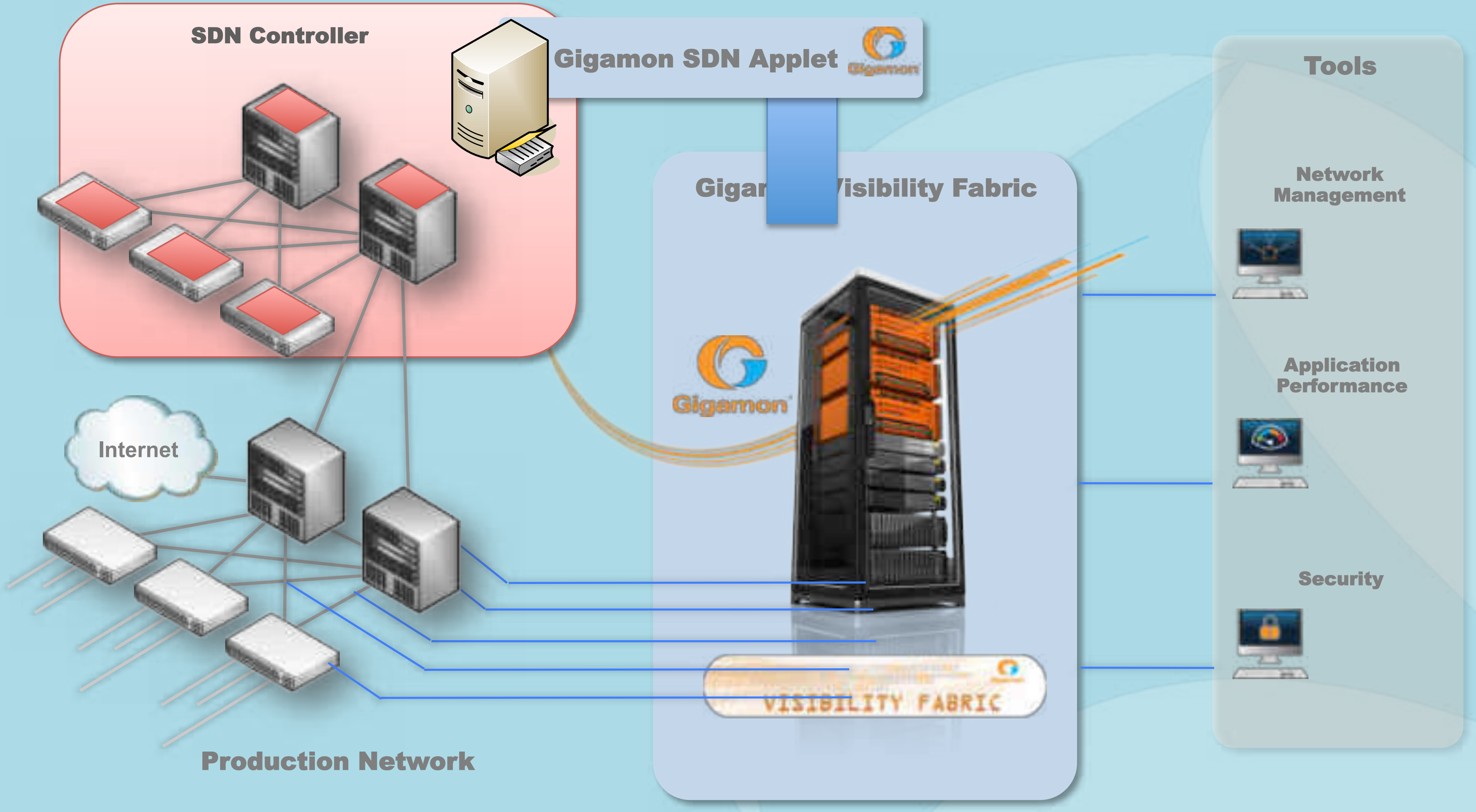
Virtual Nodes

** Proof of Concept Technology*

Software Defined Network (SDN)

- Promise of flexibility and automation to the network
- SDN is different from OpenFlow
- Enterprise has not actively deployed SDN yet
- Visibility is critical to a SDN production network
- Need a close-loop verification between the applications running on the controller, the controller and the open flow switches, and monitoring of the traffic surrounding the open flow switches.
- *All software has bugs*

Visibility for SDN



PCAP-NG Capture File Format

- New default file format for Wireshark
- Starting with version 1.7
- Very flexible file format
- Consists of blocks, with optional data within each block
- Allow interface descriptions, interface statistics and other meta-data to be associated with a capture file

Summary

- Traffic visibility is critical to modern day networks
- A Traffic Visibility Fabric (TVF) delivers visibility to the physical, virtual and SDN networks
- TVF brings ROI to existing and future tools
- TVF enables different groups within an organization to have their only view of the same traffic
- TVF allows the remote fetching of traffic to a centralized tool farm where experts are located

Thank You