Pervasive, Programmable Network Visibility for Carrier-Grade Network Monitoring

The growth of video, social media, and the Internet of Things (IoT) is pushing networks to their breaking point, forcing Mobile Network Operators (MNOs) to rethink their network architectures and business models.

As network traffic continues on an exponential growth curve, the business impact of network outages, service degradation, and security breaches is also growing rapidly. Network monitoring and security tools have therefore become increasingly central to the effective operation and monetization of mobile networks.

Monitoring and security tools depend on a network visibility infrastructure to receive replicated and curated traffic flows from the network for out-of-band analysis. As MNOs increasingly embrace Software-Defined Networking (SDN) and Network Functions Virtualization (NFV)-based architectures for networking infrastructure, their network visibility and monitoring infrastructures must follow suit. This creates a challenge, however, as legacy network visibility solutions are typically rigid, monolithic, and inadequate to support the billions of IoT connections and the tsunami of 5G traffic that will soon hit mobile networks.

Extreme, the leader in enterprise cloud and service provider data center infrastructure, offers a next-generation network visibility solution for pervasive monitoring of both physical and virtual mobile networks. The Extreme® solution delivers the benefits of both SDN and NFV network visibility, enabling diverse deployment scenarios for the world's largest mobile networks.

A Next-Generation Network Visibility Solution

The Extreme next-generation network visibility solution (see Figure 1) combines industry-leading hardware and software packet brokers with a scalable, software-based session director deployed on Commodity Off-the-Shelf (COTS) servers.[1] It also features Extreme Visibility Manager, an intuitive, single pane of glass management interface for all related hardware and software elements.

Core and Edge Aggregation Network Packet Brokers

Extreme MLXe and Extreme SLX® Packet Brokers offer comprehensive, wire-speed visibility into core and edge networks.

MLXe Packet Brokers

Extreme MLXe Packet Brokers are industry-leading, high-performance network packet brokers that offer a rich set of advanced traffic optimization functions, such as timestamping, packet slicing, port labeling, protocol stripping, and stateful filtering.

In addition, Extreme MLXe Packet Brokers are available in 4-, 8-, 16-, and 32-slot form factors to support diverse deployment needs (see Figure 2).

They offer up to 64 100 Gigabit Ethernet (GbE) ports, 128 40 GbE ports, and 640 10 GbE ports, as well as up to 15.36 Tbps switch fabric capacity in a single chassis.

Extreme MLXe Packet Brokers are ideally suited for centralized visibility architectures that demand high performance, scale, and advanced traffic optimization features.

SLX Packet Brokers

Extreme SLX Packet Brokers—including the Extreme SLX 9140, 9240—are suited for high-density traffic aggregation (Figure 3).[2] These packet brokers also offer a range of interface capacities, as shown in Table 1.

Maximum Interface Capacities for Extreme SLX Packet Brokers

SLX 9140	SLX 9240
100 GbE (6)	100 GbE (32)
40 GbE (6)	40 GbE (32)
25 GbE (48)	25 GbE (128)
10 GbE (48)	10 GbE (128)
1 GbE (48)	1 GbE (N/A)

Industry-First Virtual Packet Broker

Extreme offers the industry's first full featured virtual network packet broker. Extreme Virtual Packet Broker (Extreme vPacket Broker) brings the scalability, agility, and flexibility of NFV to network visibility, providing flow aggregation, replication, load balancing, filtering, and traffic optimization capabilities with a hardware-independent architecture.

Extreme vPacket Broker is deployed in a Virtual Machine (VM) environment on COTS servers and is built to meet the scalability and performance requirements of IoT and 5G networks. Its NFV-based scale-out architecture enables operators to acquire new features on demand, eliminating long purchase and deployment cycles.

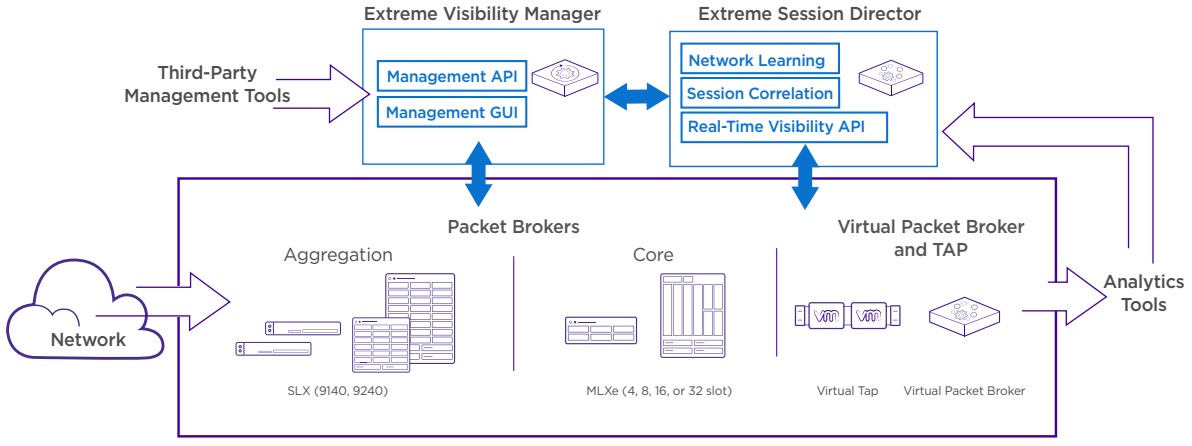

Figure 1: *The Extreme Networks visibility solution.*

[1] COTS servers are external to the packet broker hardware.

Figure 2: MLXe Packet Brokers (4-, 8-, 16-, and 32–slot models) for core network monitoring.

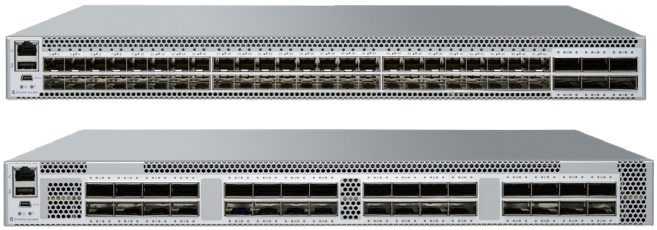

Figure 3: SLX Packet Brokers for aggregation (SLX 9140) (SLX 9240)

Extreme Networks Virtual TAP

Extreme Virtual TAP is a traffic replication, filtering, and optimization function deployed alongside Virtual Network Functions (VNFs) in a multi-tenant virtual Evolved Packet Core (vEPC) environment. Extreme Virtual TAP inspects inter-VM traffic and replicates relevant flows, forwarding them to a physical or virtual network packet broker for further processing.

The Extreme Virtual TAP and Extreme vPacket Broker functions can be deployed individually or collectively as an integrated virtual network monitoring solution.

Intelligent Session Controller for Stateful Traffic Forwarding

Extreme Session Director brings the power of SDN to network visibility, creating a separation of mobile control and bearer flow processing for enhanced network intelligence, real-time programmability, and scalability. Key functions of Extreme Session Director include:

Session Correlation - Mobile networks, unlike fixed networks, have added layers of complexity due to the presence of control traffic and the diversity of network protocols. When forwarding mobile network traffic to monitoring tools, the control and bearer traffic associated with each session needs to be correlated and forwarded to the same instance of the tool, to ensure that the tools gain complete session visibility.

Extreme Session Director performs stateful session correlation, allowing tools to redeploy the compute cycles (that they would otherwise need to allocate for session correlation) for their core monitoring functions.

Real-Time Programmability - Extreme Session Director exposes a tool-facing Application Programming Interface (API) that out-of-band monitoring and security applications can leverage to reprogram traffic flows that are bound to them in real-time (under 1 millisecond).

With real-time programmability, Extreme Packet Brokers become truly service-oriented visibility nodes, enabling MNOs to realize the full potential of their monitoring tool investments.

Automated Network Learning - The automated network learning feature of Extreme Session Director provides network operations staff with a holistic, dynamic, and graphical view of the network's topology by statefully inspecting and correlating traffic across multiple mobile control interfaces.

Automated network learning empowers operations staff with real-time network intelligence, enabling them to define flow forwarding rules on Extreme Packet Brokers, based on a rich and diverse set of criteria.

Single Pane of Glass for Physical and Virtual Packet Brokers

Extreme Networks Visibility Manager is an intuitive, Graphical User Interface (GUI)-based management application that provides a "single pane of glass" for configuring, maintaining, and troubleshooting both physical and virtual Extreme Packet Brokers. Key functions of the Extreme Visibility Manager function include:

Role-Based Access Control (RBAC)- Extreme Visibility Manager supports differential access privileges based on the defined role of the user. With (RBAC) - administrators can define device- and port-level access privileges for a

role, profile, or group. This provides administrators with significant control, as well as flexibility in the administration of Extreme Packet Brokers.

Simplified Software Upgrades - Extreme Visibility Manager provides a central point of management, allowing administrators to upgrade the software on any Extreme Networks physical or virtual packet broker through an easy-to-use GUI.

Alarms and Notifications - Administrators can define triggering criteria for automated alarm generation and email notifications from Extreme Visibility Manager when specific events occur.

Automated Configuration Backup - Extreme Visibility Manager enables administrators to automatically back up device configurations on a periodic basis to ensure service continuity in the event of system malfunction.

Diverse Deployment Scenarios for Physical and Virtual Networks

Extreme Packet Brokers support both centralized and distributed visibility architectures for pervasive monitoring of physical and virtual mobile packet cores (see Figure 4).

In a centralized visibility architecture, Extreme SLX Packet Brokers are deployed at the edges or aggregation layers of the network, where they collect and filter traffic before forwarding relevant flows to the centrally deployed Extreme MLXe Packet Brokers. Alternatively, SLX Packet Brokers at the aggregation layer can forward traffic directly to the Analytics Engines.

For virtual networks, Extreme Virtual TAPs (deployed in a VM within the hypervisor environment that hosts VNFs) intercept inter-VM traffic and forward relevant traffic flows to centrally deployed physical or virtual network packet brokers for further processing.

In a distributed visibility architecture, different regions or functions within the network operate independent visibility and monitoring infrastructures. Extreme SLX, Extreme MLXe, and Extreme Virtual Packet Brokers can be used to forward traffic flows to locally deployed monitoring tools.

With these different deployment options, MNOs can further ensure that their mobile networks are ready to support IoT and 5G traffic.

Learn More

Extreme Networks partners with companies of all sizes to deliver innovative solutions that help organizations maximize the value of their most critical information. To learn more, visit www.extremenetworks.com.

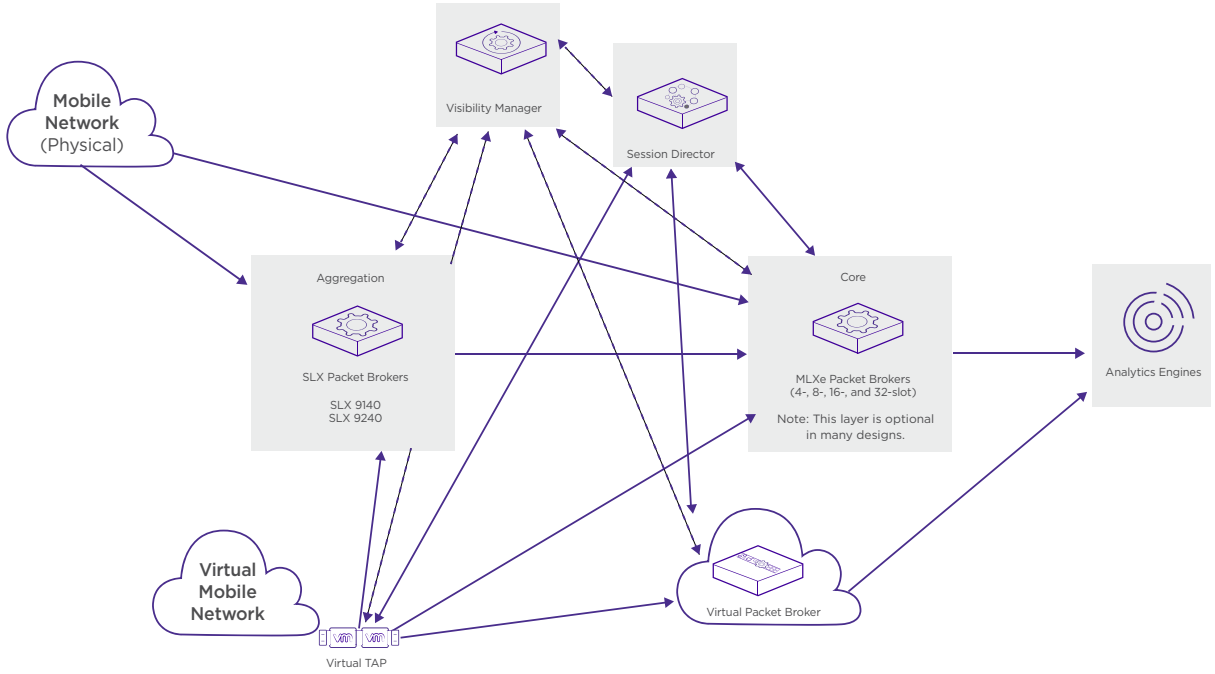

Figure 4: Deployment alternatives for physical and virtual network visibility.