SOLUTION GUIDE

Improving Visibility and Monitoring with SDN for Carrier Networks

Building a Visibility Fabric with Luxar, Pica8, and Rohde & Schwarz Cybersecurity

Network Traffic Visibility

The network is the lifeblood to a telecommunications service provider's (carrier) business. It provides the transport for the revenue-generating applications and services to their end customers, and when it's down, it has a direct impact to their revenue stream. When a carrier knows what traffic runs through its network, the carrier can optimize the use of the network infrastructure, identify any leakage of revenue, gather market intelligence, and provide better or new value-added services. Visibility of network traffic is the fundamental enabler. Extracting packets from the carrier network and analyzing them provides this visibility. However, dealing with high volumes of traffic can be difficult to scale.

Today, with SDN technology, carriers can now build a scalable traffic analytics farm. Luxar Tech (Luxar), Pica8, and Rohde & Schwarz Cybersecurity (Rohde & Schwarz) have partnered to provide a visibility fabric built with SDN technology that provides the pipelines for extracting, grooming, aggregating, and distributing the traffic to an analytics tool for analytics and performance management.

Visibility Fabric for Analytics and Reporting: An Overview

A visibility fabric enables packets to be copied from the carrier network without intrusion or adding risk of disrupting the carrier network traffic. Packets can be copied using passive optical splitters placed at various extraction points of the carrier network. The copied packets can be aggregated to packet brokers for speed conversion, filtering, load balancing, slicing, time-stamping, header-stripping, and header modification. The packet brokers send the tapped traffic to a fabric of spine and leaf Ethernet SDN switches to which a cluster of servers are connected that host the applications that provide traffic analytics and reporting for the network operators to consume. In a nutshell, the visibility fabric comprises a layer of optical splitters and packet brokers, connecting to an Ethernet switch fabric, that feeds the traffic into various analytics appliances.

This solution guide describes how to build this fabric with components from Luxar, Pica8, and Rohde & Schwarz. Luxar offers optical splitters and packet brokers, along with an SDN (Software-Defined Network) controller that works with Pica8 PicOS-driven switches to form a multi-purpose Ethernet switch fabric called LuxeFabric™. Traffic is fed from LuxeFabric to the R&S®NetReporter 2 toolset for analytics and reporting.

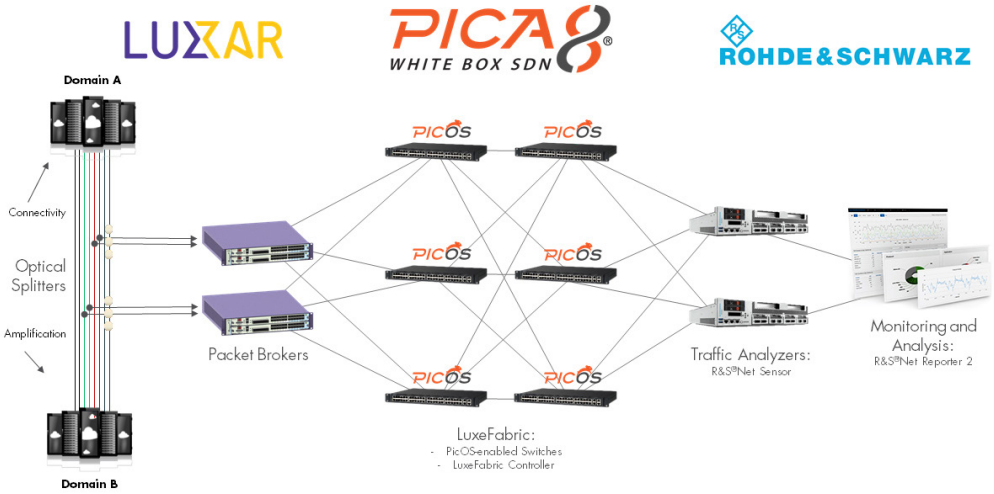

Figure 1. Network traffic visibility architecture

Solution Components

Optical Splitters

An optical splitter is a passive network element to be inserted onto an optic fiber to make a copy of the optical signals by splitting some optical energy from the original optical signals. The original communication is not affected. By using optical splitters at various extraction points of a network, traffic can be tapped for analysis.

Packet Brokers

A packet broker is a purpose-built device for traffic-tapping applications. It can serve various functions such as:

- Converting traffic from one speed to another
- Converting traffic from one medium to another
- Filtering uninteresting traffic so that uninteresting traffic would not consume analytics appliance bandwidth
- Slicing packets for bandwidth efficiency or privacy compliance
- Load balancing traffic to multiple instances of an analytics tool
- Replicating traffic to multiple analytics tools.

Luxar offers a variety of packet brokers that serve different deployment scenarios.

LuxeFabric Controller

LuxeFabric controller is an SDN controller based on OpenDaylight. LuxeFabric controller instructs the LuxeFabric switch hardware with forwarding rules in the data plane. Meanwhile, it presents REST interfaces for applications to program the controller and hence the fabric. It is built with open networking technologies such as OpenDaylight and OpenFlow. It can be installed on a physical server or a virtual machine. It also supports active-standby redundancy.

LuxeFabric provides all the benefits of an OpenFlow-based SDN. It offers a flexible network automation and management framework, which will enable rapid service introduction, reduce operational overhead, and decrease network instability introduced by operator error.

LuxeFabric encompasses the benefits of both a traditional L2 network and a traditional L3 network yet without the drawbacks of either. The LuxeFabric controller has built-in equal-cost-multi-shortest-path forwarding intelligence. With none or a few configurations, you have a network whose redundant paths are fully utilized. Also, LuxeFabric controller makes no assumption about network topology. Therefore, you are not limited to a spine-leaf Clos network topology. More importantly, the network can be scaled out as needed. On the other hand, LuxeFabric is able to interoperate with a traditional L2/L3 network.

LuxeFabric can serve multiple purposes, some relevant to visibility fabric. First, it enables tapped packets to be forwarded and load-balanced from the packet brokers to the analytics server cluster. Secondly, it enables the analytics server to exchange messages among themselves and the main database or other data storage systems (e.g., as in a Hadoop cluster). Thirdly, it can be connected to a traditional L2/L3 network for a remote client to retrieve analytics reports from the analytics server cluster.

LuxeFabric Switch Hardware

LuxeFabric switches are OpenFlow switches qualified by Luxar to ensure compatibility and integrity. Luxar has qualified PicOS-driven switches. Pica8 provides PicOS, the network operating system running on and managing the switch hardware.

LuxeFabric Switch Operating System Software

The LuxeFabric switches run PicOS, a market-leading network operating system software for white box switches. PicOS eliminates vendor lock-in by delivering open, hardware-agnostic networking. Built on Linux, PicOS incorporates a full Layer-2 and Layer-3 feature set with support for OpenFlow, OVSDB, and other key SDN protocols.

R&S®Net Sensor – intelligent, network agnostic IP probe

Deployed in the network at statistically relevant spots, R&S®Net Sensor is the element that processes all user and control plane network traffic at full line speed. It classifies traffic into applications and extracts information such as RADIUS, GTP-C or DHCP messages to support transparent subscriber resolution in R&S®Net Reporter 2. Nonintrusive installation of the probe via a network ensures short deployment times. When installed, the R&S®Net Sensor is agnostic to the type of monitored network and can process plain network traffic as well as the GTP-encapsulated traffic seen on Gn/Gp or S5/S8 interfaces. A single probe can simultaneously handle traffic from different access type networks. By providing the full classification vector for layer 3 to layer 7 and above, R&S®Net Sensor provides full traffic awareness and consistent performance reporting capabilities.

R&S®Net Reporter 2

R&S®Net Reporter 2 receives network data records from multiple R&S®Net Sensor probes deployed throughout the network and automatically aggregates and stores application classification information. When hooked into additional databases (subscriber DB, CRM, TAC), the application classification is supplemented with additional information such as subscriber, device, location and data plan. An easy-to-use, intuitive user interface provides a wide variety of views, filtering and drill-down options on the underlying data. Examples include application visibility for the entire network, specific access network segments, mobile gateways and specific subscriber, device and location. Open APIs provide direct access to the underlying analytics database. R&S®Net Reporter 2 can be customized to operator needs and connected northbound to big data and other third-party systems to provide specific data based on a customized setup. R&S®Net Reporter 2 can run on dedicated hardware or in common virtualization environments.

Deployment

The visibility fabric has been deployed to fit monitoring needs of various scale. An exemplary deployment comprises Luxar LTV8250 packet brokers, one instance of a controller, a fabric of three spine switches and three leaf switches, and over a hundred servers, where each server can contain multiple instances of traffic analyzers.

LTV8250 is a 100GE packet broker. The 2RU device provides two 100GE interfaces and twenty-four 10GE interfaces. One of its functions is to convert the 100GE tapped traffic into 10GE traffic towards the spine switches of the fabric. It also supports 128K filtering rules for selecting or de-selecting specific packet flows to be forwarded to the analytics tools. An important one of its functions is to ensure that a conversation of two end-nodes, i.e., traffic from IP A to IP B and vice versa, always lands on the same instance of an analytics tool through the fabric so that the traffic analysis can be most effective. The packet brokers are located at the traffic extraction points.

Figure 2. LTV8250 packet broker

In the exemplary deployment, there are three spine switches and three leaf switches co-located with the analytics server cluster and the controller machine in a data-center-like environment. The spine switches and the leaf switches are interconnected in a Clos network topology, prepared for future expansion of the network. The switches are Pica8's P-5101. They are the typical 1RU Broadcom Trident 2-based switches, but most importantly, they are driven by PicOS. The controller talks to PicOS using the standard protocol OpenFlow 1.3. A P-5101 switch provides four 40GE ports and forty-eight 10GE ports. LTV8250 devices are connected to the spine switches through the 10GE ports. The 40GE ports are used for interconnecting the spine switches and the leaf switches. The 10GE ports of the leaf switches are used for connecting to the servers. The management ports of the switches are connected to the controller machine through an out-of-band Ethernet network.

Figure 3. Pica8 P-5101 OpenFlow switch

The controller machine hosts the controller software. The controller software runs on Ubuntu 14.04 Linux OS and is based on OpenDaylight. The LuxeFabric logics are implemented as a plugin collaborating with some basic OpenDaylight components.

The network topology can be observed using the OpenDaylight DLUX web GUI.

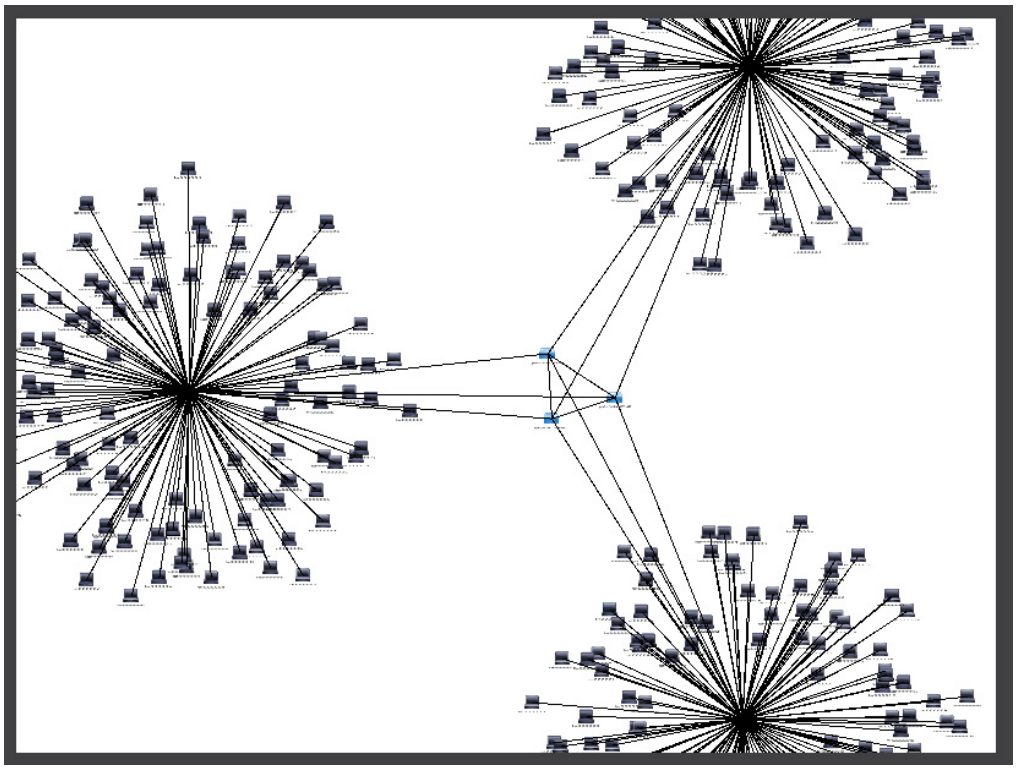

Figure 4. Network topology as shown in DLUX web GUI

The controller provides REST interfaces for configurations and scripting. In the visibility fabric use case, an application script of the fabric controller pushes the configurations using HTTP to the REST interfaces of the controller. The application script manages the forwarding rules and controls the associations between the hash values assigned to packets and the instances of the analytics tool according to the liveness and the work load of the instances of the analytics tool.

The controller automatically learns about the liveness and the port locations of the instances of the analytics tool through ARP packets. When an instance of the analytics tool is migrated from one port location to another, the controller learns the new location through the ARP requests from the instance. In that case, the script does not need to do anything. When there is no ARP request nor ARP reply from an instance, the controller timeouts the learned port location, and the script may consider the instance dead and modify the forwarding rules and push the new forwarding rules to the controller.

One instance of a controller may be sufficient because the switches can keep forwarding traffic while the controller is being restarted. An active-standby controller pair is called for when there is a concern about the availability of the control plane.

In the present deployment scenario, R&S®Net Reporter 2 receives data from the array of R&S®Net Sensors and aggregates the information into relevant reports and flexible exports into any other data storage systems.

Using Rohde & Schwarz's leading application classification engine R&S®PACE 2, R&S®Net Sensor delivers high accuracy application and protocol detection. The detection list covers the most used 2000 applications and protocols from all geographical regions and across various business fields. By providing the full classification vector for Layer 3 to Layer 7 and above, R&S®Net Sensor delivers full traffic awareness and allows building consistent performance reporting capabilities.

Figure 5. Reports of Net Reporter.

Conclusion

Telecommunications service providers need to optimize the use of their networks and gather intelligence about traffic types and patterns to generate new revenues and services. Carriers can now deliver a more flexible, cost-effective solution to gain network visibility using SDN technology. Luxar, Pica8, and Rohde & Schwarz have provided an integrated solution that enables traffic visibility, analytics, and reporting in a scalable and cost-effective fashion.

About Luxar Tech

Luxar Tech develops industry-leading network visibility and optical connectivity solutions for service providers and large enterprises. Its software-defined visibility fabric enables building scalable traffic analytics farms. Its bleeding-edge fiber monitoring system provides exceptional precision identifying fiber faults. Its DWDM transport systems offer highly cost-effective data center inter-connectivity. For more information, visit www.luxartech.com.

About Pica8

Pica8 is breaking barriers to truly customizable application performance through open networking. With its Linux-based PicOS™ network operating system, Pica8 enables custom traffic engineering and empowers white box and brite box switches to integrate easily with existing Layer 2/Layer 3 networks and deliver unlimited SDN scalability through OpenFlow. Since 2009, Pica8 has pioneered new open networking technologies such as Linux-based networking, CrossFlow networking, vASIC® and Table Type Patterns. Through ongoing innovation, Pica8 is a trusted brand that unlocks the potential of made-to-order networking, offering a mainstream alternative to legacy proprietary systems.

About Rohde & Schwarz

Rohde & Schwarz Cybersecurity is an IT security company that protects companies and public institutions around the world against espionage and cyberattacks. With around 400 employees, the company develops and produces technologically leading solutions for information and network security. Development of the trusted IT solutions is based on the security-by-design approach for proactively preventing cyberattacks.

Pica8, Inc.
Corporate Headquarters

1032 Elwell Court, Suite 105
Palo Alto, California 94303 USA
650-614-5838 | www.pica8.com

Produced in the United States 12/16.