Assuring the promise in Edge Computing

Horst Fellner, Leader EMEA 5G Solutions
horst.Fellner@spirent.com
https://www.linkedin.com/in/horstfellner/
General considerations
Spirent’s 5G thermometer

**What’s HOT**
- 5G Core: First deployments
- 5G Edge Cloud: Build outs starting
- Automation: Cost savings then agility
- 5G Security: Risk assessment

**What’s WARM**
- Open RAN & IAB
- New Players: FAANGS | MSOs | Towers
- Supply Chain & Security
- Private Networks
- Non-Terrestrial Networks

**What’s NOT**
- Consumer ARPU: Flat or low for 5G
- Corona Virus: Supply chain
Today: Individual Clouds

Disintegrated clouds with vertical implementation

- O-RAN Fronthaul
- Backhaul
- Access
- Edge Datacenters
- Aggregation Network
- 5G Stand Alone
- Core Datacenters
- EPC
- IMS

RAN   Fronthaul   Backhaul   Edge DC   Aggregation & Core DC
Challenges for Edge Compute deployment

- Edge Cloud Availability
- Virtualization and cloud migration
- Proliferation of Security Functions
- Limited Visibility
- Fault remediation

- Validate
- Assure
- Automate

- Infrastructure
- Security
- Visibility and Assurance

Virtual stack

APPLICATION
SERVICE
VIRTUALIZATION
INFRASTRUCTURE
Vertical clouds from Telco perspective

**Core Cloud** – Cloud architecture for the new Core including edge disaggregation. Mostly being built by the CSPs with partners like VMware.

**Private Edge Cloud (or Private MEC)** – For private networks where the Core and relevant apps are hosted in the customer pre. This is a mixture of CSP self build and partnerships (i.e. Azure).

**Public Edge Cloud (or Public MEC)** – This is the most common in the media where the CSPs are partnering with the hyper-scalers. Telco network functions are not hosted in the Public MEC and the focus is mostly on apps including CDNs, AI/ML processing and content accelerators.

**vRAN Edge Cloud** – Specialised design of the edge cloud for hosting the baseband unit and new splits. Currently the vRAN cloud is proprietary due to the need for hardware accelerators (i.e. FPGA, GPUs, smart-NICs) to handle the lower layer radio processing and due to no common industry architectures.

**Enterprise Edge** – Evolution of CSP enterprise offerings including vCPEs, vFW, vGi functions.
Infrastructure validation
Challenges

- Need to accelerate market adoption of SD-WAN services
- Lack of standardization in SD-WAN industry
- Rapidly evolving, complex technology, challenging to deploy
- Migration into cloud and native services complexity

MEF addressing with standardization
Virtualization: Breaking Up Network Functions …

The Original “Network Functions”

Vendor A

Network Function Virtualization Infrastructure

Virtual Network Functions

APPLICATION

VIRTUALIZATION

INFRASTRUCTURE

SERVICE

Hardware

Application

Application

Application

Container

Cloud
Spirent SD-WAN Solutions

- SD-WAN Testbed Automation and Orchestration
- SD-WAN Application/Validation
- SD-WAN Product Validation (and MEF Certification)
- SD-WAN NFV/Cloud Validation

- DESIGN
- ONBOARD
- DEPLOY
- OPERATE
- MAINTAIN
**NFVI Validation**

Determine maximum CPU work when compute host is filled to full capacity with a specified VM flavor.

Determine network data plane frame loss and latency between two compute hosts.

Determine aggregate memory bandwidth and latency when compute host with specified number of VMs of a specified flavor.

**Diagram:**
- CPU
- Memory
- Storage
- Network
- Hypervisor
- vSwitch
- Operation System
- Hardware Accelerator
- Network Interfaces
Spirent SD-WAN Test Package Testbed Configuration
Security validation
Security Challenges 1/2

**DDoS Attack**
Resource exhaustion | Data Breach

**NFV Software**

**NFV Infrastructure**

**NFVi Attacks**

**Multi-Vendor Weakness**

**Edge Distribution Attacks**

**Ethernet Layer 2 Attacks**
VLAN Hopping | DHCP/MAC Spoofing

**Ethernet Fronthaul Attacks**

**Security Gateway Attacks**
Resource Exhaustion | Spoofing

**Security GW Attack**

**Device Vulnerability Attack**
Botnet DDoS | Malware | Fraud

**Massive IoT Attacks**

**Man-in-the-Middle Attack**
Packet-injection | Data Breach

**C-RAN MEC**

**CORE Enterprise**
Security Challenges 2/2

Network Slice Attacks
- Slice Attack
  - Slice Faking
  - CUPS Hijacking

Rouge Base Station
- Man-in-the-Middle Attack
  - DoS
  - Identity Theft
  - Spying

New Core Attacks
- IP Attacks
  - DoS
  - Tunnel Flooding

Subscription Attacks
- Orchestrator & Controller Attack
  - Command & Control

Roaming Threats
- Hybrid Network Attacks
  - SS7 & Diameter

Common Services
- Time, Location & DNS Attacks
  - DoS
  - Spoofing
  - Hijack
  - Floods
Security(SASE) Solutions

SD-WAN Testbed Automation and Orchestration

SASE User Experience Management

Assess/Benchmark CSF

Security Efficacy
Configuration
Functional
Performance/Scale

CSF SRT

SD-WAN & SASE
Assurance

Security Efficacy
Configuration
Functional
Performance/Scale

APPLICATION

SERVICE

VIRTUALIZATION

INFRASTRUCTURE

Assess/Benchmark
SD-WAN VNF/SFCs

Certify SD-WAN
Assess/Benchmark
SD-WAN VNF/SFCs

SD-WAN SRT

Assure SD-WAN

Benchmark NFVi for
SASE/SD-WAN

Onboarding & LCM
CSF

Change Mgmt. & Troubleshooting

Onboarding & LCM
CSF

Cloud Turn-Up & SAT

Troubleshoot/Isolate

Qualify NFVI

Onboarding & LCM NFs,NSs

Validate WAN
Underlays

Underlay SAT

DESIGN

ONBOARD

DEPLOY

OPERATE

MAINTAIN

Edge Computing World, Berlin

Proprietary and Confidential
Assessing Security Efficiency in Cloud Environments
Validate Security

**Current State**
- Pre-Deployment Validation Relying on Vendor Testing
- Vulnerabilities discovered after attacks

**Desired State**
- Pre-Deployment Validation w/ **Realistic** Security Testing
- Vulnerabilities pro-actively detected and mitigated

**Goal:** Improving security and proactive reducing risks
Operational assurance
Challenges

Each network has own visibility and management

Missing easy and full overview

Difficult fault-finding localization and isolation

High complexity when changing architecture or introducing new
Coverage: E2E Visibility

**Current State**
- Individual networks
  - Own visibility and management
- Disaggregated view as “island” solution
- Difficult new service introduction

**Desired State**
- One network view
- Automated operations
- Decreasing complexity for changes or new service introduction
Network operations (live) concept

- **KPI's**
  - Availability
  - Delay
  - Latency

- **Service Assurance Controller**
- **Active data**
- **5G Stand Alone**
- **Passive data**
- **Service Activation Tests**
- **E2E Tests**
- **VTA**
- **Embedded Test Function**

- **Access**
- **Aggregation**
- **OP Center/Management Factory Floor**
- **Latency**
- **Delay**
- **Availability**
Gaining E2E Visibility

Current State

Multiple solutions/networks with dedicated view

<table>
<thead>
<tr>
<th>Tools</th>
<th>Triage Time</th>
<th>Trouble Tickets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor A</td>
<td>60%</td>
<td>75%</td>
</tr>
<tr>
<td>Vendor B</td>
<td>75%</td>
<td>90%</td>
</tr>
</tbody>
</table>

Desired State

Aggregated visibility and operation

<table>
<thead>
<tr>
<th>Tools</th>
<th>Triage Time</th>
<th>Trouble Tickets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor A</td>
<td>60%</td>
<td>75%</td>
</tr>
<tr>
<td>Vendor B</td>
<td>75%</td>
<td>90%</td>
</tr>
</tbody>
</table>

Goal: Reducing complexity, accelerating time-to-market and optimizing user experiences
Summary
Unleashing the Flexibility of SD-WAN with Active Assurance

CHALLENGE

• Tier-1 service provider was preparing to launch SD-WAN
• Needed to activate services faster at significantly lower cost and ensure IP mesh network was ready for SD-WAN

SOLUTION

• Spirent Active Assurance for virtual and physical networks
• Deployed Ethernet & IP virtual test agents to more than a thousand of the client’s points of presence

IMPACT

• Automated manual service activation, SLA monitoring and troubleshooting workflows, saving millions of dollars each year
• Provider saved $10 million by deploying virtual test agents in lieu of physical test heads as it upgraded 1G links to 10G
Challenges

What keeps you awake at night?

Network readiness
Will your network perform and avoid post-deployment problems w/ 5G, SD-WAN, cloud and Wi-Fi migrations?

Security threats
How can you stay ahead of threats and keep your network secure? Are you proactive or reactive?

Improving resources
How do you.security in-house talent to support and develop further?

Cloud migrations
How can you ensure your clouds will perform in real-world conditions while avoiding higher Opex?

Technology adoption
How can you be sure of a successful migration from various sources? Are end-users experiencing promised QoE?

Data ownership
Security and GDPR when using 3rd vendors for hosting and operationalizing company data.

Solving the challenges and improving the outcome for successful Cloud deployments
Benefits we provide to our customers

Accelerate time to market

Reduce complexity and cost

Harden cybersecurity defenses

Optimize user experience

We’re with you every step of the way