Anomaly Detection in Software-Defined Networks

Christian Liß
InnoRoute GmbH

11 July 2018

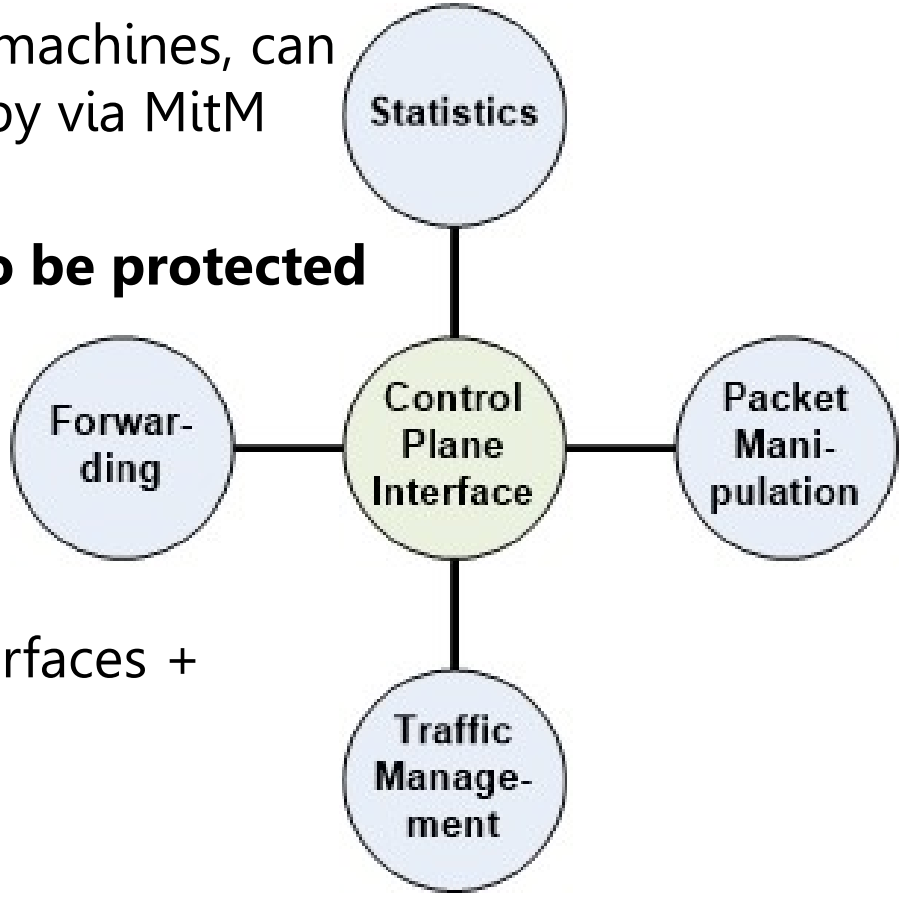
NETWORK SECURITY – AN ARMS RACE

- Security is a **hygiene factor** & it's **non-binary** (no simple yes or no)
  - it's **complex**: hard to benchmark, not common knowledge
    → even if you know what happens, do you know how to react?
  - it takes **resources**
  - for most products it **isn't the main feature**
- More and more attacks are **remote**, network-based & **fully automated**
- Pure number of botnet nodes opens new, interesting **businesses for cybercrime**
- The pace of the arms race is going faster and faster, as new **technologies evolve**, which can be **used by both sides**
- More and more **devices get connected** + **networks converge**:
  fixed-mobile in access networks, IT & OT in industrial networks,
  Enterprise & cloud, … → **more devices affected + affected by similar attacks**

By Leena Snidate / Codenomicon (http://heartbleed.com/heartbleed.svg) [CC0], via Wikimedia Commons

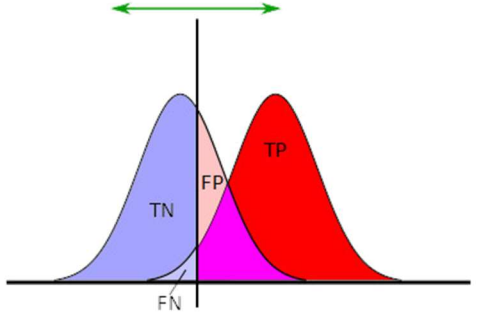
SOFTWARE-DEFINED NETWORKS – FLOW-BASED NETWORK OPERATION

- **Productivity** = f(network availability)
- **Each network element**, like printers and virtual machines, can be used to attack other systems, step-by-step, spy via MitM
- Each device can be hardened,
  but also the **network** as a complex system **has to be protected**
- Not always possible **by design**,
  → constant **monitoring** and **maintenance**
- Flexible networks (SDN) **increase the power** of its owner, of the admin or the attacker
- First **targets**: south-bound and north-bound interfaces + network as a whole during reconfiguration
- SDN: **flow-based X** → easily auditable paths, performance KPIs, and more



NETWORK ANOMALY DETECTION

- Important technology to **keep up with** rapidly developing & diverse **threads**
  → Sometimes buffer overflows might be triggered by a single packet,
  but vulnerable hosts have to be identified via scans first …
- Heavily **softwarized datacenter networks**: yet another software-based service
  SDNs: use existing SDN infrastructure
  Everything else: dedicated hardware
- False positives: lower productivity + lead to
  disabled/insensitive detection services
  → must be highly **selective** and **report precisely**
- Two European 5G-PPP research projects:
  Mobile access networks based on vNFs, connected via SDN
- Biggest weakness: **SDN control channel**, which could be
  guarded by special protection and **fallback to defined paths**



TP	FP
FN	TN

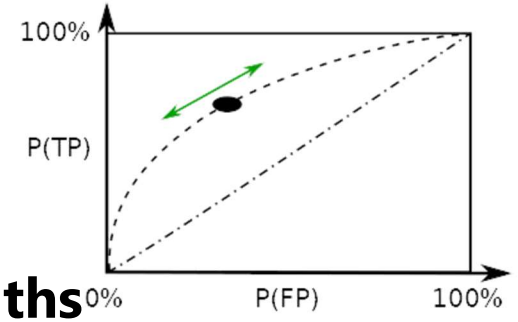
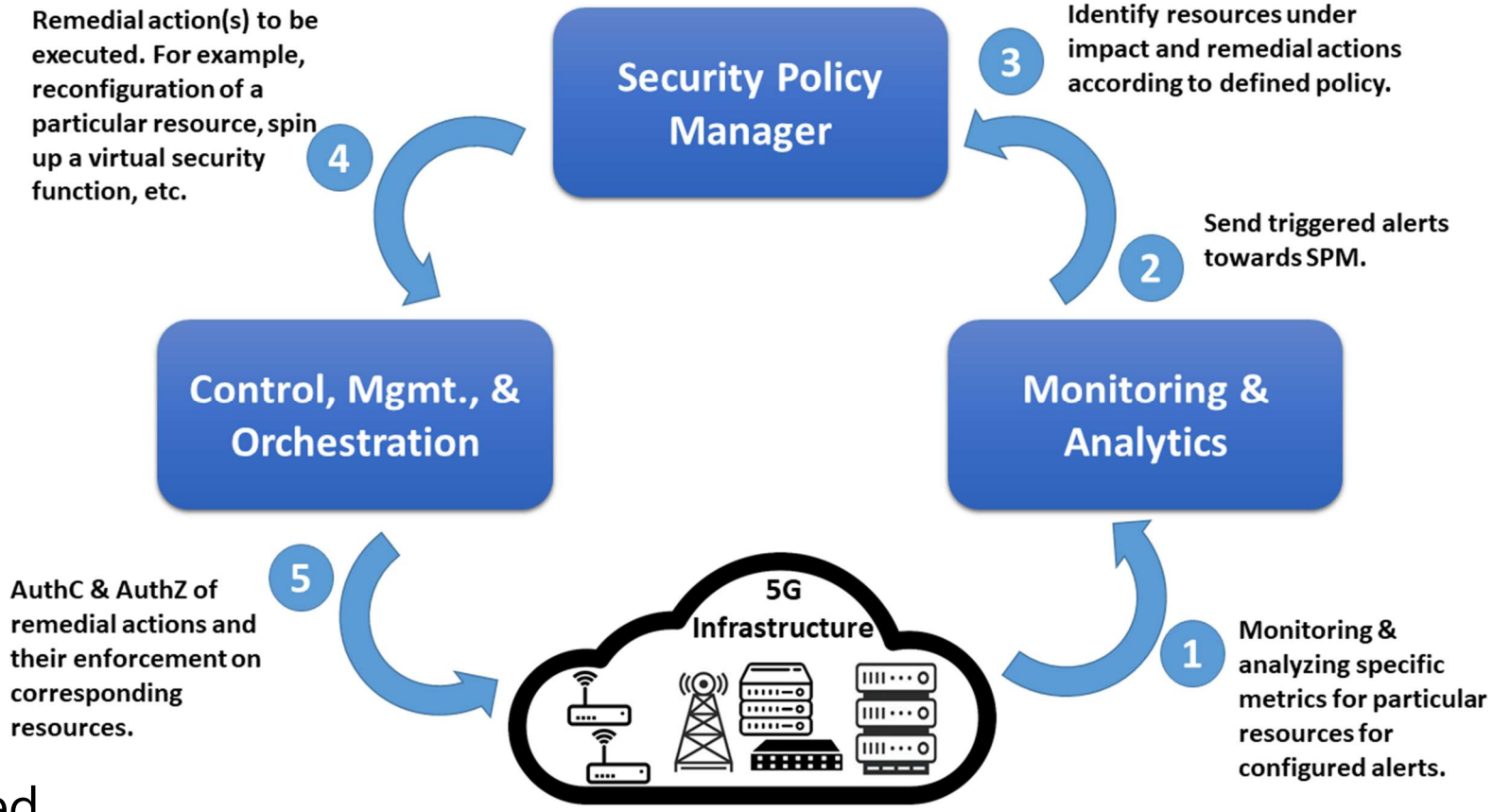


Image: By Sharpr [CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0)], from Wikimedia Commons

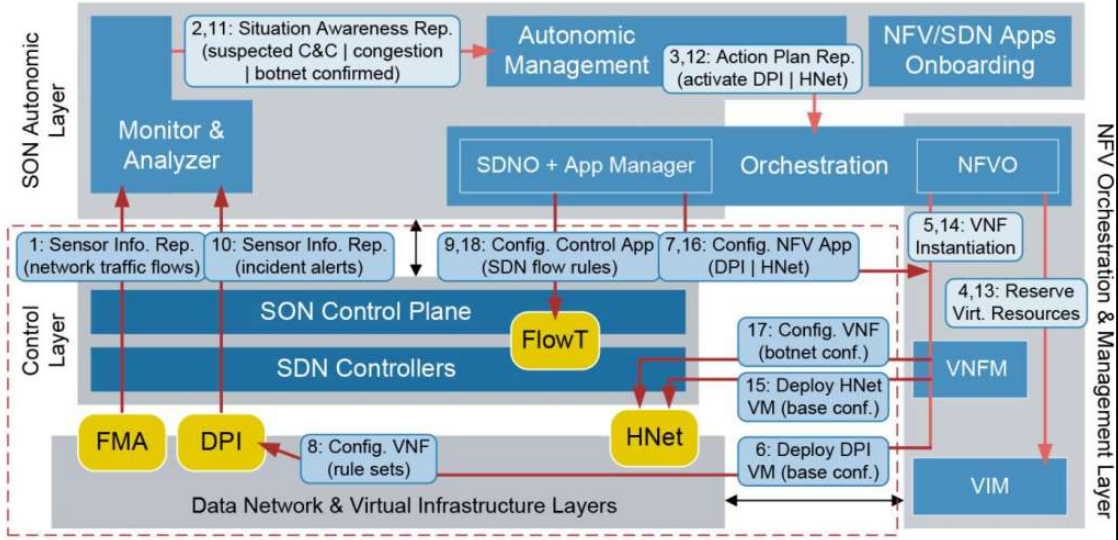
CHARISMA SECURITY SOLUTION

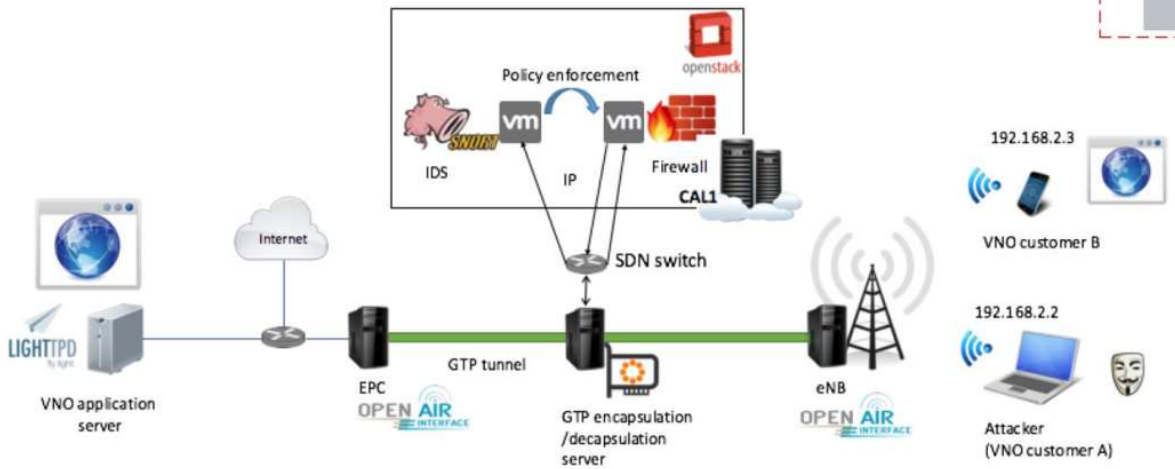
- 5G **subscribers as zombies** for DDoS, C&C, …
- Distributed network sensors supply information to **autonomous management unit**
- **Targeted blocking** through automatically deployed **virtual Firewall** next to compromized 5G subscriber

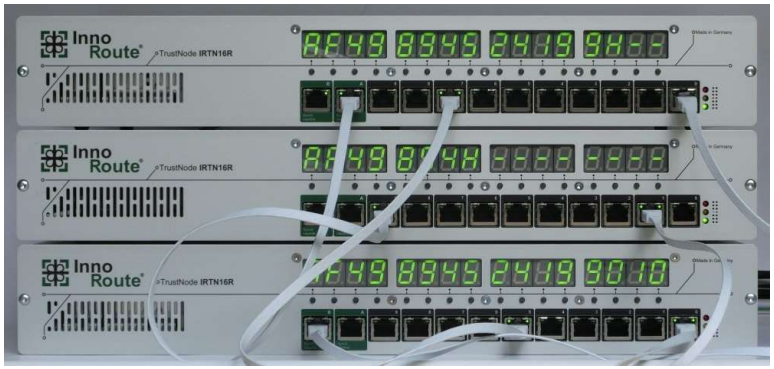


SELFNET SECURITY SOLUTION

- Cooperation with CHARISMA
- **Redirection to HoneyNet + vDPI** instead of blocking
- Gain new **insights on traffic patterns, actions, and capabilities of attackers** for improved detection & defense

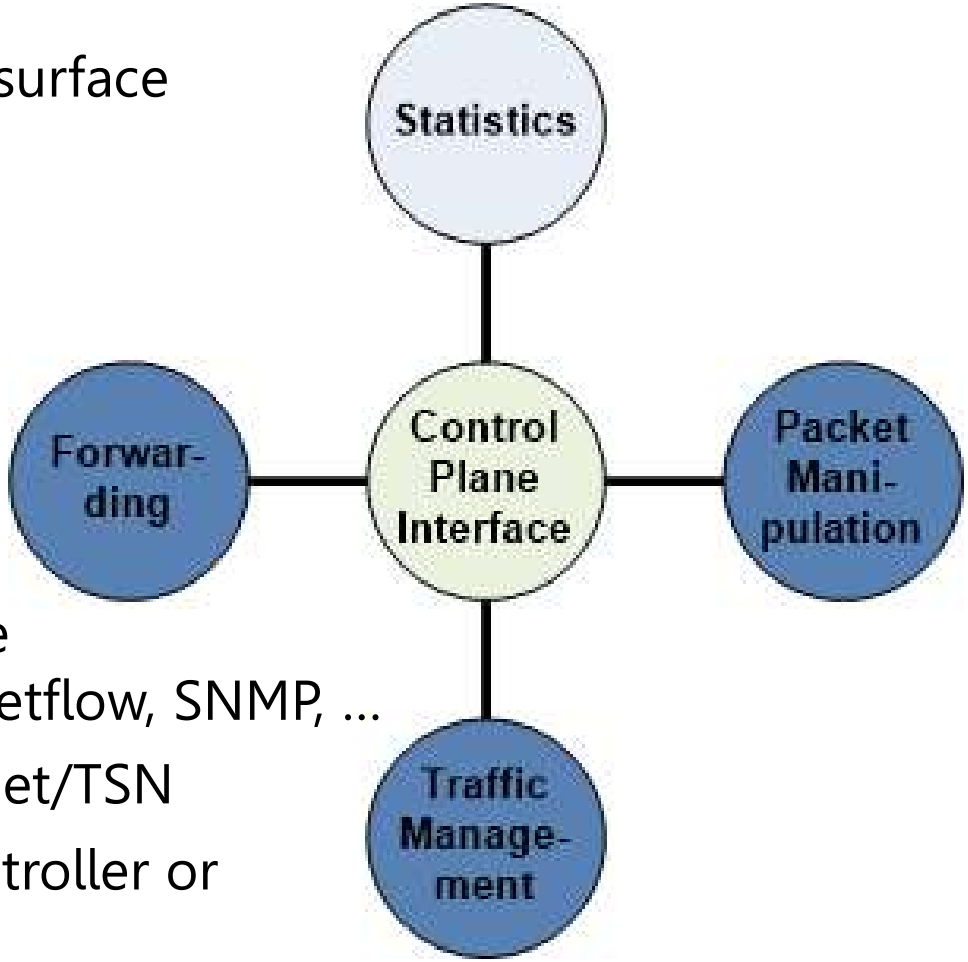






ONE PIECE OF THE PUZZLE: HARDWARE TAPS

- Complexity = bigger & heterogeneous attack surface
  → **simplicity** is key
- **Taps**:
  - distributed over the network
  - exact timestamping → **synchronized taps**
  - **real-time** provisioning to controller
    → for correlation and countermeasures
  - **flow information**, e.g., for rule compliance
    → standard formats for easy integration: Netflow, SNMP, …
  - **Example**: customized TrustNode for Ethernet/TSN
- Standard or custom taps connected to the controller or to **independent monitoring facilities**
  → to enable recognizing the big picture + to understand incidents



- Next:

Harald Weikert on IsarNet's monitoring tool IsarFlow

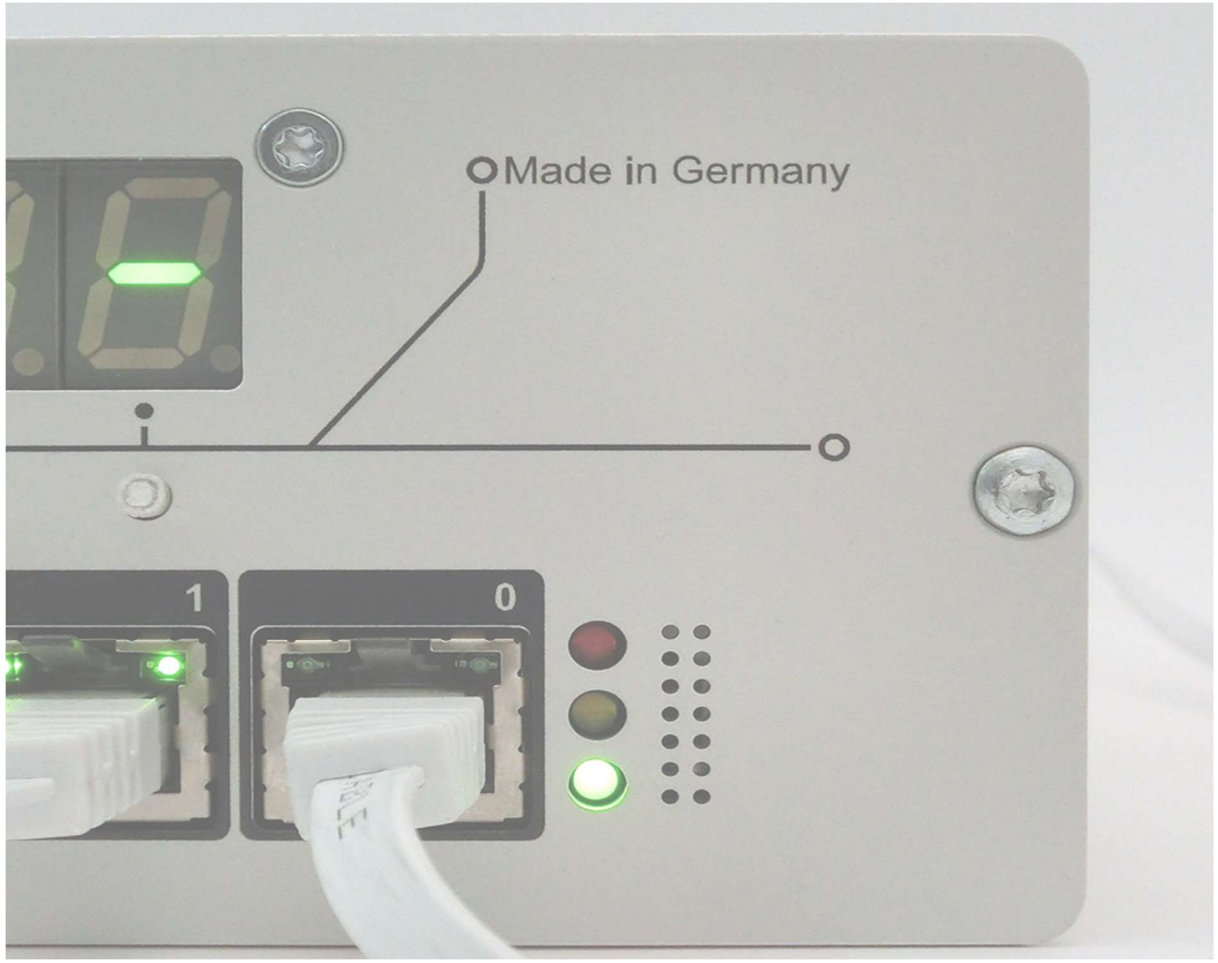
which can be connected to a customized TrustNode-based tap via NetFlow or SNMP

Contact Us

Christian Liss, Head of R&D

InnoRoute GmbH
Marsstrasse 14a
80335 Munich
Germany
+49 89 4524199 - 02
liss@innoroute.de
Visit us: www.Innoroute.de

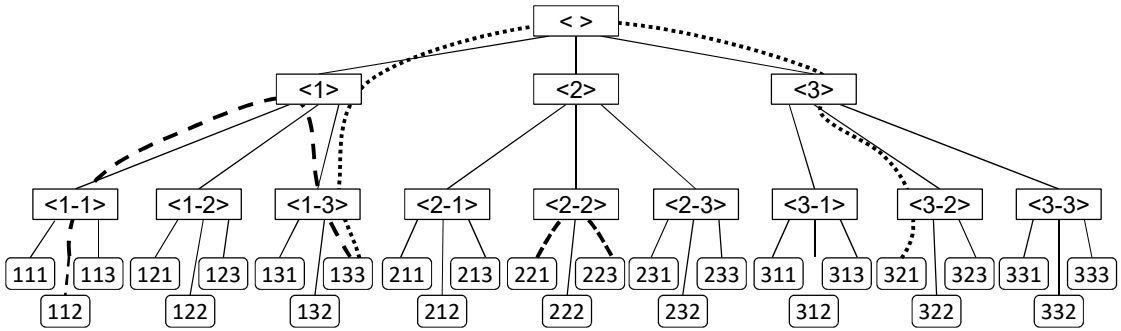
CEO Andreas Foglar
Registrations: Amtsgericht München
VAT ID: DE 271566134
WEEE: DE 84823388



FALLBACK TO DEFINED PATHS

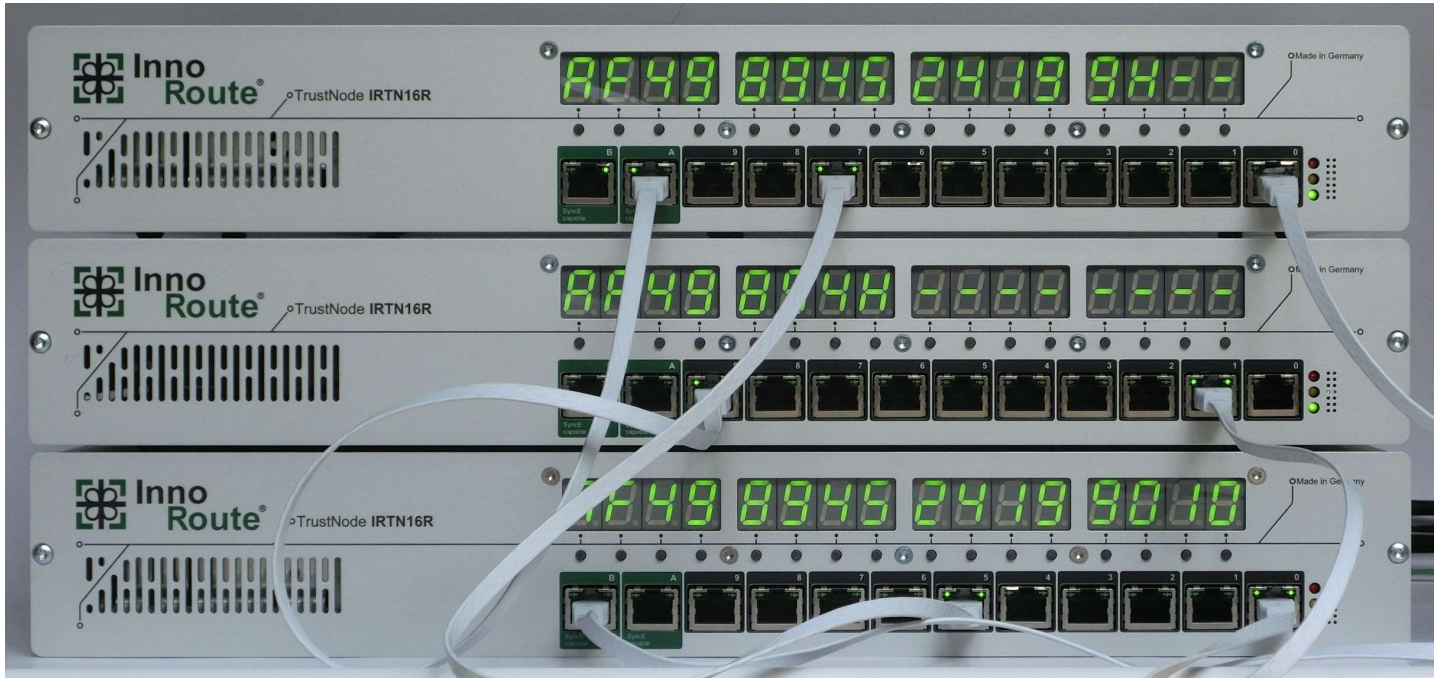
- 6Tree concept, implemented and evaluated in the 5G-PPP CHARISMA project
- Internet Draft: https://tools.ietf.org/html/draft-foglar-ipv6-ull-routing-00
- Presented at ITU SG2: https://www.itu.int/md/T17-SG02-C-0097/en

- Basic concept: Subset of the IPv6 address space is used for routing packets on a hierarchical network, with node addresses assigned like phone number

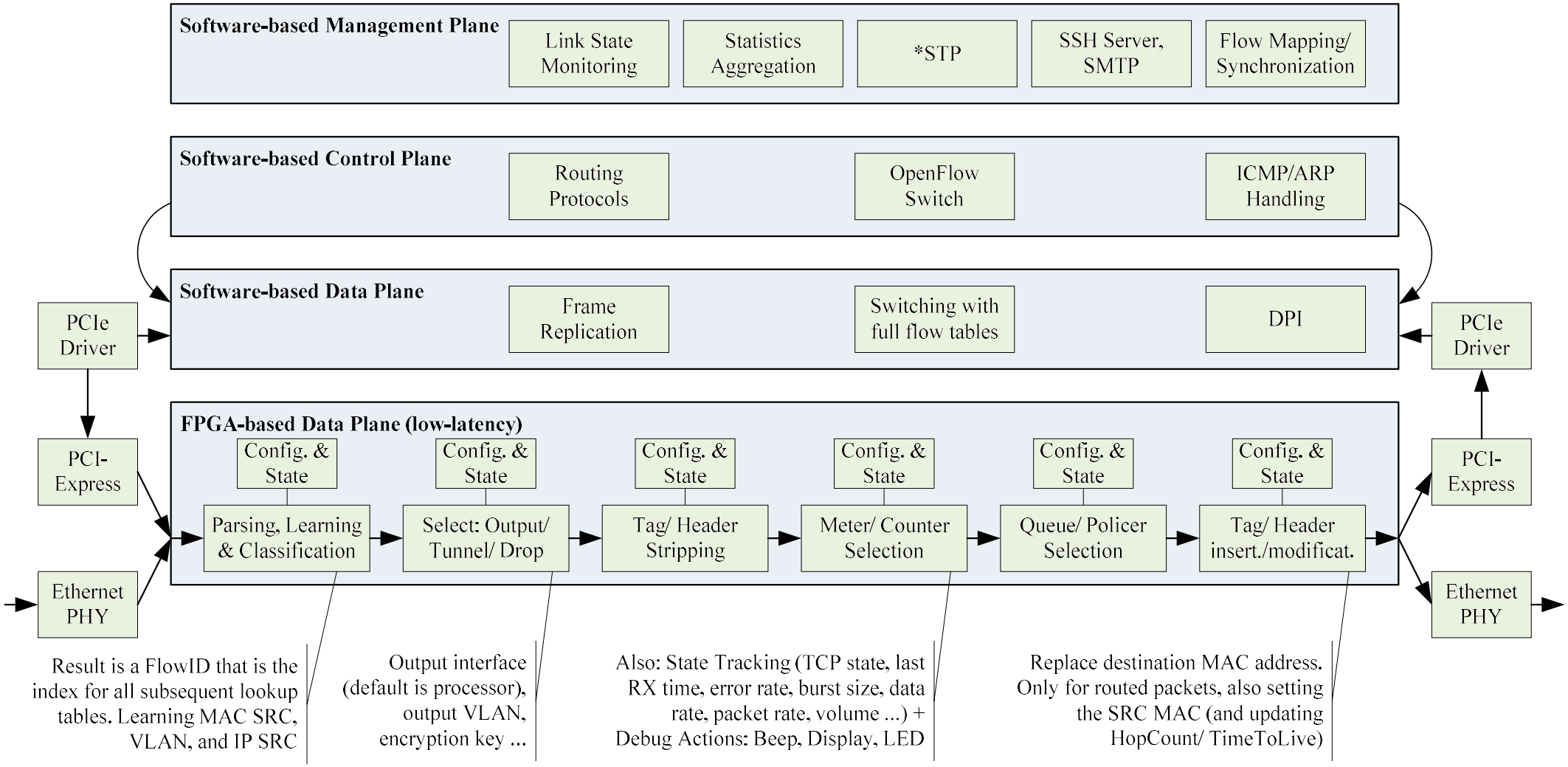


TRUSTNODE – NETWORK NODE & TAP

- TrustNode: Powerful line-speed network processing platform
- Used for customized taps that are tailored to specific applications
- Supports 10/100/1000 Ethernet and TSN, OpenFlow, SyncE, and more



DETAILLED SDN FUNCTION SPLIT



TIME-SENSITIVE NETWORKING WITH THE TRUSTNODE

1. 802.1AS(rev)
2. 802.1Qbv
3. Others
   (redundancy, preemption, …)