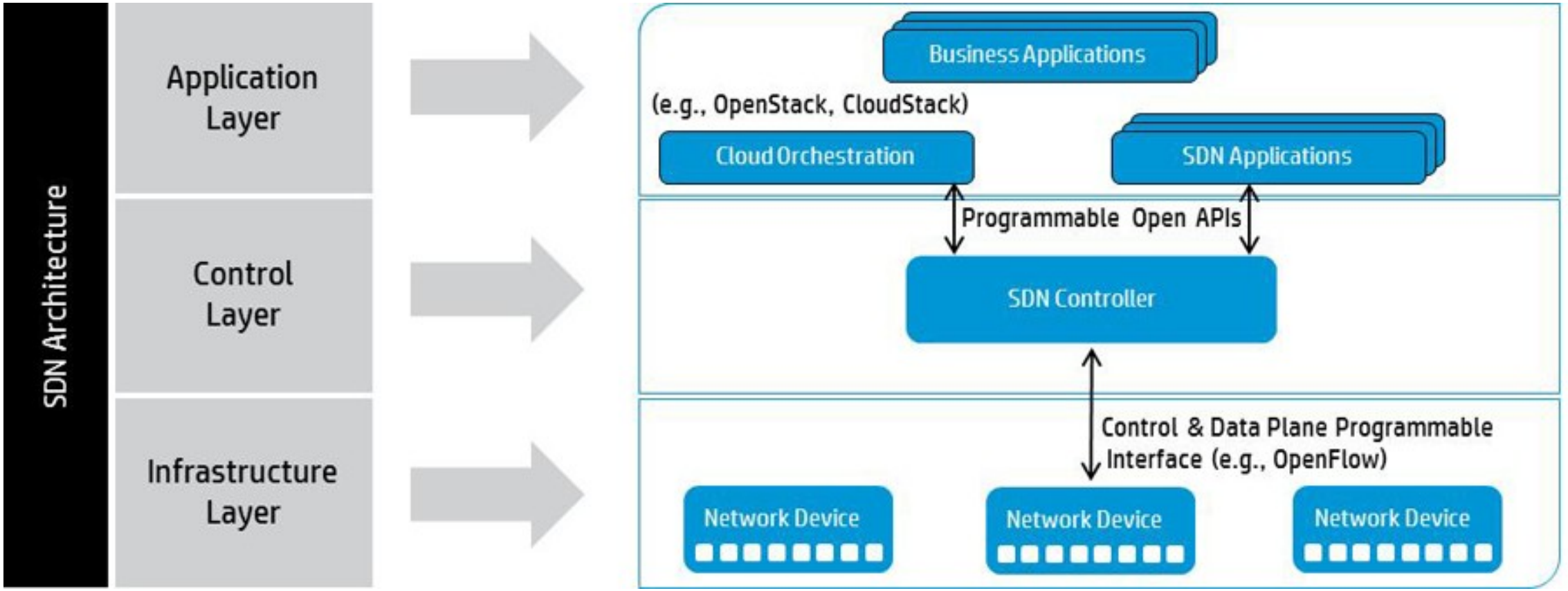
A SDN Attestation Approach

IETF 93 - SDNRG meeting, Prague

Ludovic Jacquin <ludovic.jacquin@hp.com> / 22th July, 2015

“Softwarisation” of the infrastructure

Empowering the application to change the network topology



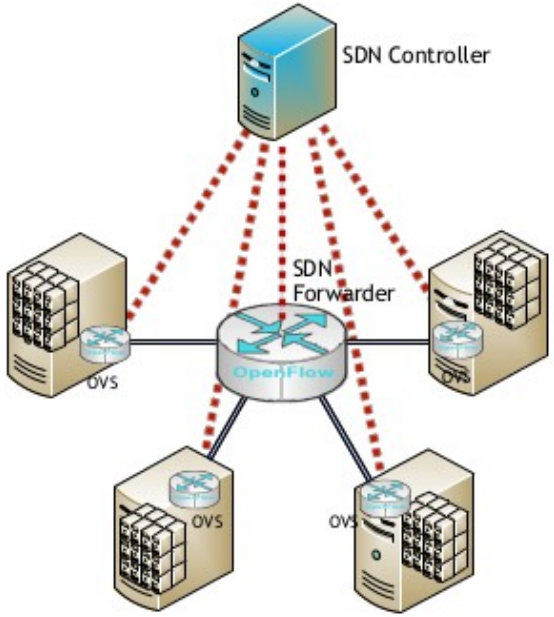
Goals and Assumptions

Towards a trustworthy infrastructure

Interception and alteration of SDN control plane packets.
Rogue SDN controller that attempts to alter configurations of network elements.
Flashing of network element firmware with customized software (malicious software, persistent bootkits).
Downgrade of network element firmware to an old version (or simply out-of-date version).

Attacker model

- An attacker can attack the Network Element
- An attacker can attack the control plane
- The SDN controller is considered secured



Automated and trustworthy monitoring for SDN

Introducing a SDN verifier

Goal: Assess that SDN configuration on devices match the controller expectations

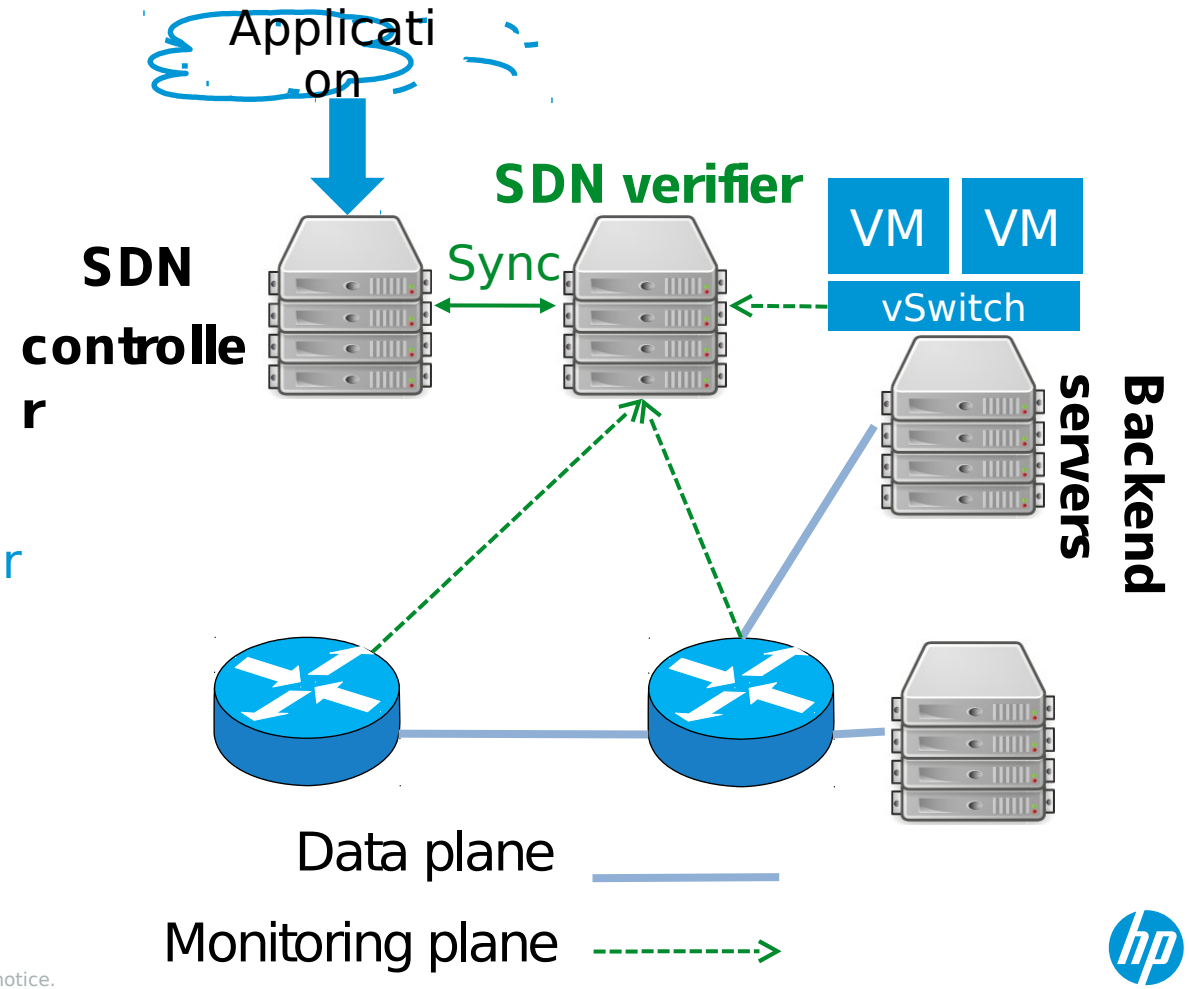
Out-of-band trusted challenge/response of each NE

Retrieve the NE expected configuration from the controller

Assess correctness of the enforced rules by any NE

Meant for continual attestation

Challenge: build a trusted reporting mechanism for every network element - physical or virtual.



Core Root of Trust for Reporting (CRTR)

Monitoring the SDN rules in a network element

Introspection of the SDN context:
Monitoring what is really enforced, not just the protocol

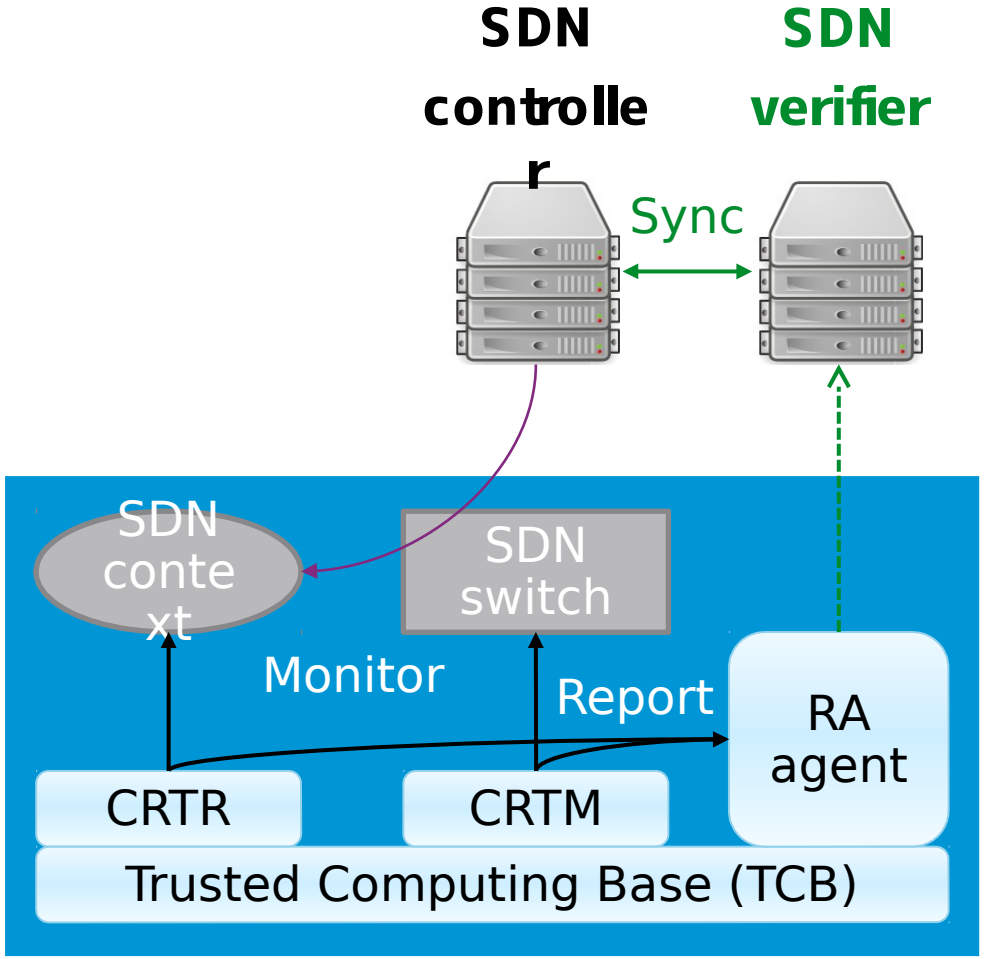
CRTR alone is not enough

The SDN “switch” still needs to be attested

- Core Root of Trust for Measurement (CRTM) required too

Remote Attestation (RA) must be possible by the SDN verifier

- Need an agent/proxy to communicate



Remote Attestation requirements

Quick primer on some Trusted Computing mechanism

Hardware-based identity

Root of Trust for the identities of the device

Secure storage

Can not be erased with by the software (unless reboot of the device)
Can be signed by one of the identities without software intervention

Measured boot

Each bootstage measures the next stage software it launches
Securely stores the measurement
Recursively, a device needs a Core Root of Trust for Measurement (CRTM):
Implicitly trusted by the user (e.g. verified/audited firmware residing in ROM)

Verifier Remote Attestation of a device:

Request a signed copy of the securely stored measurements
Can assess: device identity and firmware/software stack state (except CRTM)

TCG created a networking equipment subgroup (part of embedded systems WG).

SDN attestation report

What does the switch need to report, and how?

Based on the notion of flow:

- Filter based on L1/L2/L3/L4 headers
- Associated with a set of prioritised actions

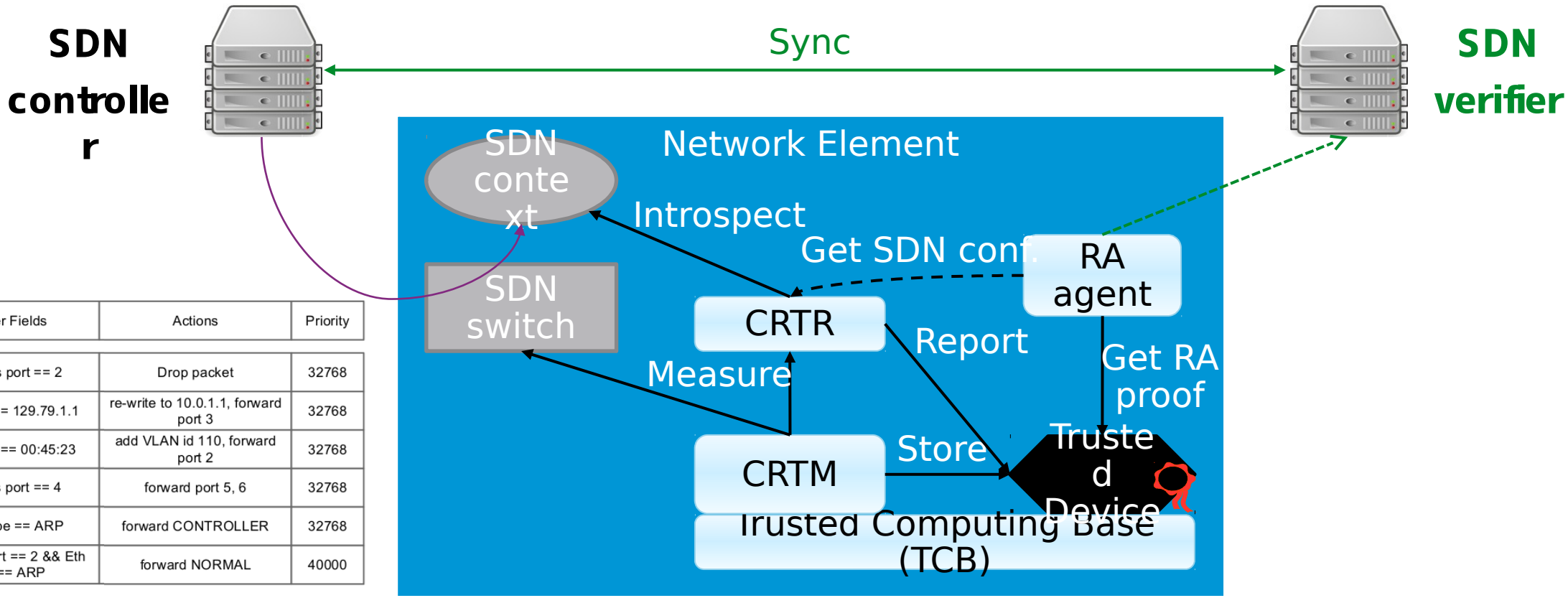
Header Fields	Counters	Actions	Priority
If ingress port == 2		Drop packet	32768
if IP_addr == 129.79.1.1		re-write to 10.0.1.1, forward port 3	32768
if Eth Addr == 00:45:23		add VLAN id 110, forward port 2	32768
if ingress port == 4		forward port 5, 6	32768
if Eth Type == ARP		forward CONTROLLER	32768
If ingress port == 2 && Eth Type == ARP		forward NORMAL	40000

7/21/15

Challenge: SDN rule changes more often than a switch configuration.

Traditional (PCR-based) TCG mechanism not fitted for that.

Remote Attestation-enabled Network Element



Header Fields	Actions	Priority
If ingress port == 2	Drop packet	32768
if IP_addr == 129.79.1.1	re-write to 10.0.1.1, forward port 3	32768
if Eth Addr == 00:45:23	add VLAN id 110, forward port 2	32768
if ingress port == 4	forward port 5, 6	32768
if Eth Type == ARP	forward CONTROLLER	32768
If ingress port == 2 && Eth Type == ARP	forward NORMAL	40000

Early prototype

Hardware Ethernet switch prototype

SDN Verifier – RA agent channel

Relies on SNMP for the moment
One SET-able OID for a nonce
One GET-able OID to retrieve the attestation proof
The SDN verifier is in charge to implement a time-out

Trusted Platform Module (TPM) as Trusted Device

Industry standard
Hardware identity
Secure storage for measurements
Slow device though
Measurement storage: ~100ms
Creation of the attestation proof: ~600ms

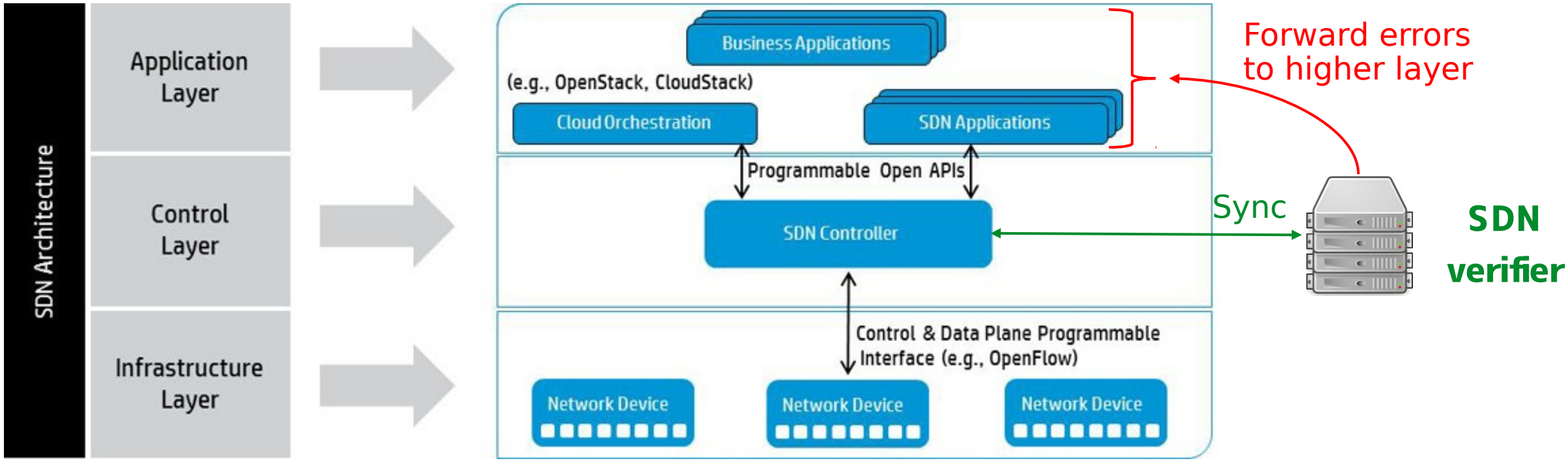
RTT (SDN verifier p.o.v.) to retrieve the attestation proof: ~1s

Next step: closing the loop

Acting on a misbehaving network elements

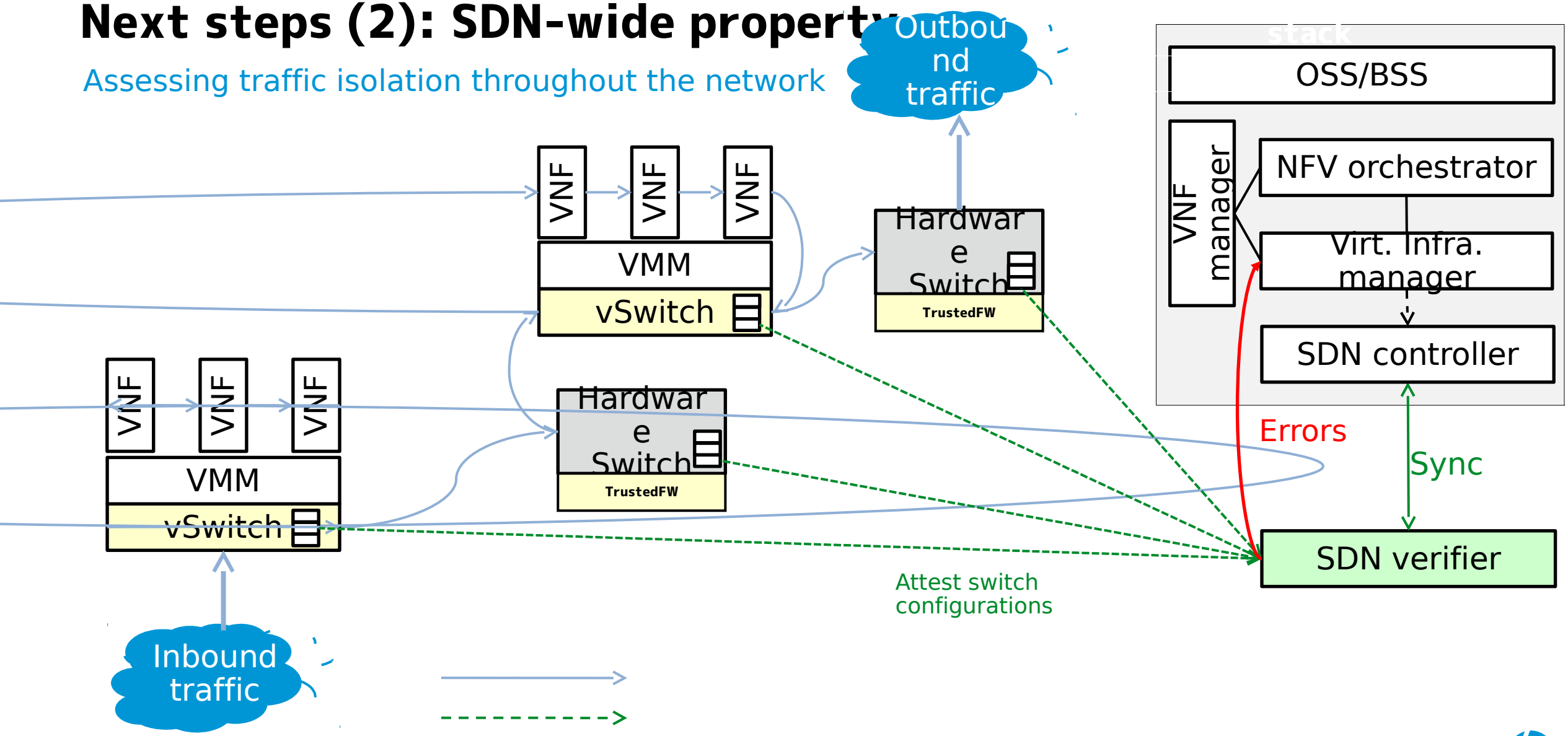
Automated response

Pass the information to the Application Layer
App Layer has the visibility to handle the error, e.g. quarantining a faulty switch



Next steps (2): SDN-wide property

Assessing traffic isolation throughout the network



Thank you