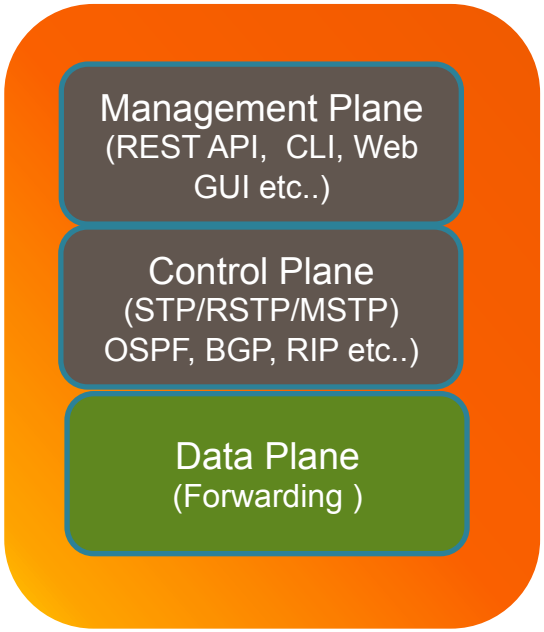
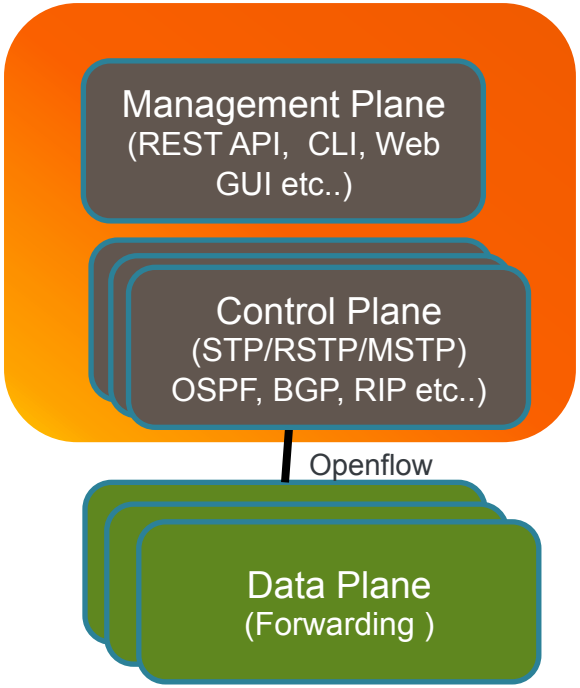
- What is SDN (Software Defined Networking) and Openflow?
  - Control and Data Plane Separation
  - Traffic Control
- SDN/OF – Part of Kernel / SoC to provide security, steering & monitoring

Software Defined Networking - Control/Data Plane Separation



Traditional Network Devices :

- A self contained box with all three planes combined into one.
- Operators have control over configuration of device,
- Expensive
  - Cost
  - Interoperability
  - Vendor lock-in



SDN/OF based Devices

- Data Plane separated out from control plane.
- Popular separation protocol : Openflow.
- Programmable data plane ***(One hardware - Personality can be changed by control plane)*** using OF based tables, flows, instructions and actions.

Benefits :

No purpose built data plane hardware : One data forwarding hardware, personality is added by associated control plane. -→ Cost

No vendor lock-in : Operators (themselves or with the help of SDOs) can develop their own control plane software or enhance CP software.

One (or few) Control Plane instance(s)→ One (or few) control plane vendor implementations in the network -→ **Lesser issues in control interoperability**.

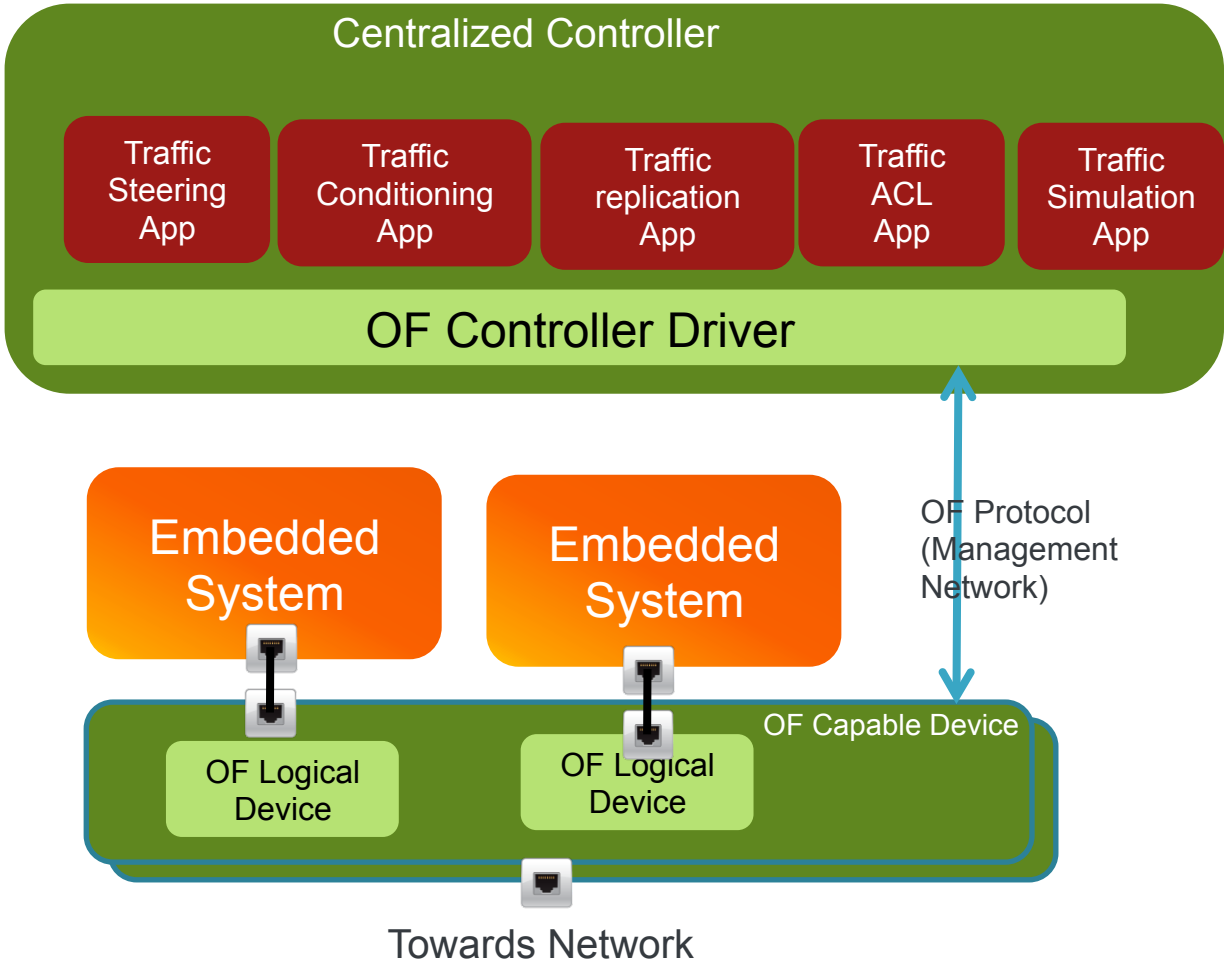
Simple and lesser **software upgrades**

Lesser vulnerabilities & Vulnerability patching is simpler with centralized control plane (90% of software is typically CP software)

Software Defined Networking – Traffic Control

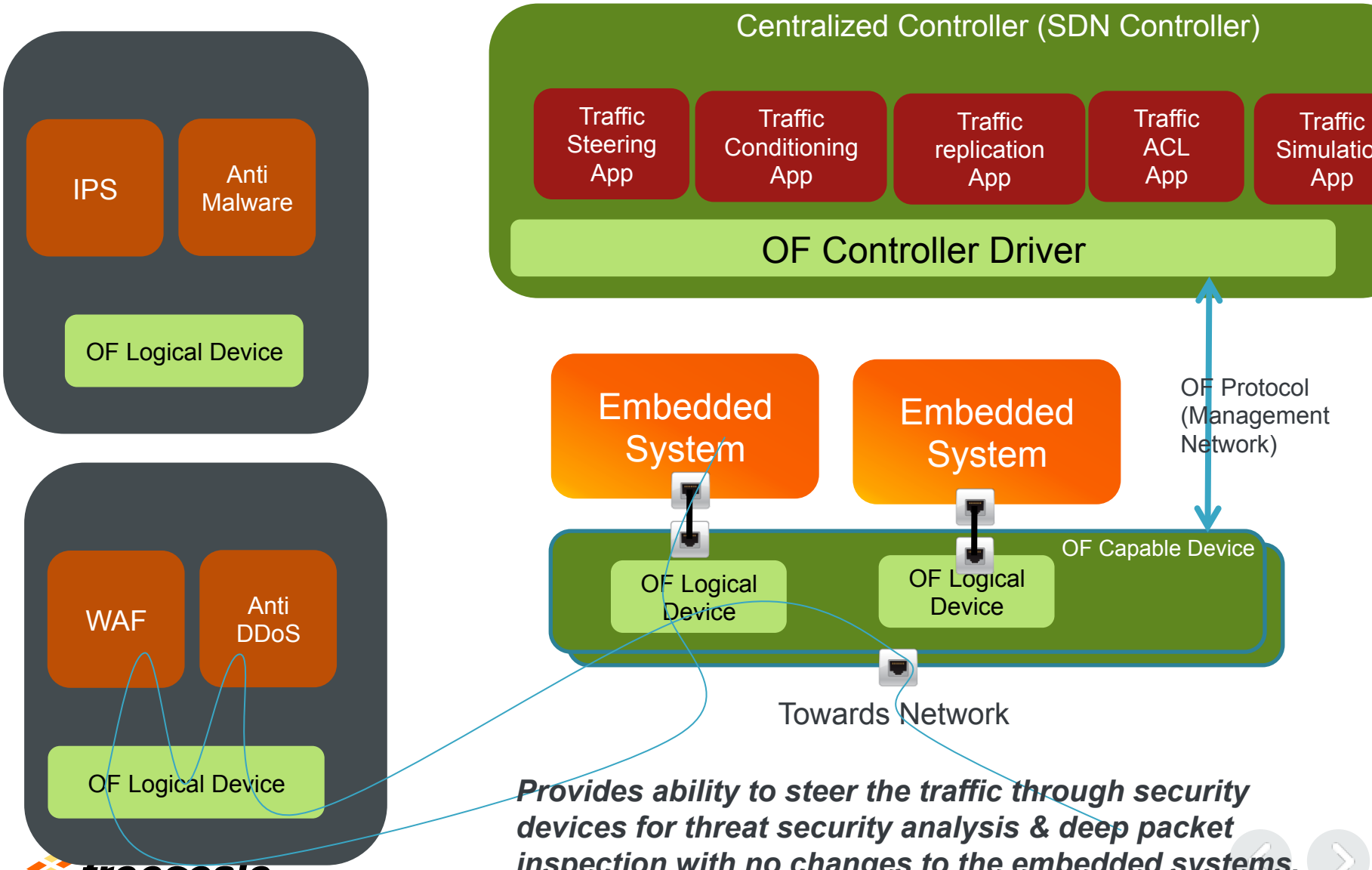
•Front End embedded systems with Openflow devices. (No changed to embedded devices)
•All traffic going to/from embedded systems go through OF devices.
•OF devices is programmed from OF controller
•Multiple applications

- **Traffic Steering** (To Steer traffic across multiple devices for security and optimization treatment) – Next slide for details
- **Traffic conditioning** – To rate limit the traffic towards going to embedded system.
- Traffic replication – For offline analysis.
- **Traffic ACL** – to stop unwanted traffic (based on time of the day, source, services being used and combination of above)
- **Traffic Simulation** : To simulate traffic towards embedded systems to
  - Check the health of embedded systems
  - Check the latency and performance of embedded systems
  - Benchmark embedded systems



Control with no changed to the Embedded systems - Secure the traffic and provide more visibility on traffic patterns

Software Defined Networking – Traffic Steering for deep security analysis



Provides ability to steer the traffic through security devices for threat security analysis & deep packet inspection with no changes to the embedded systems.

Embedded SDN & SDN Friendly SoCs (Sytem On Chip)

Avoid special SDN devices by embedding Openflow controlled logical devices within the embedded systems.

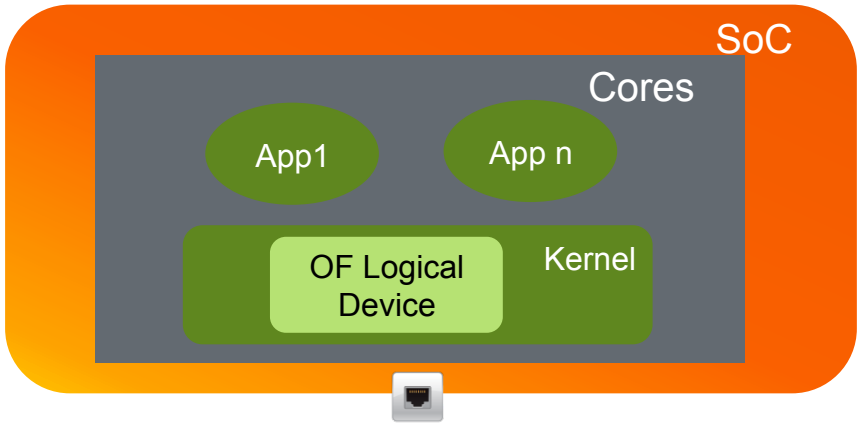
•***Embedded OF device (Software module)*** *within the Kernel – Kernel protecting the embedded applications on the SoC*

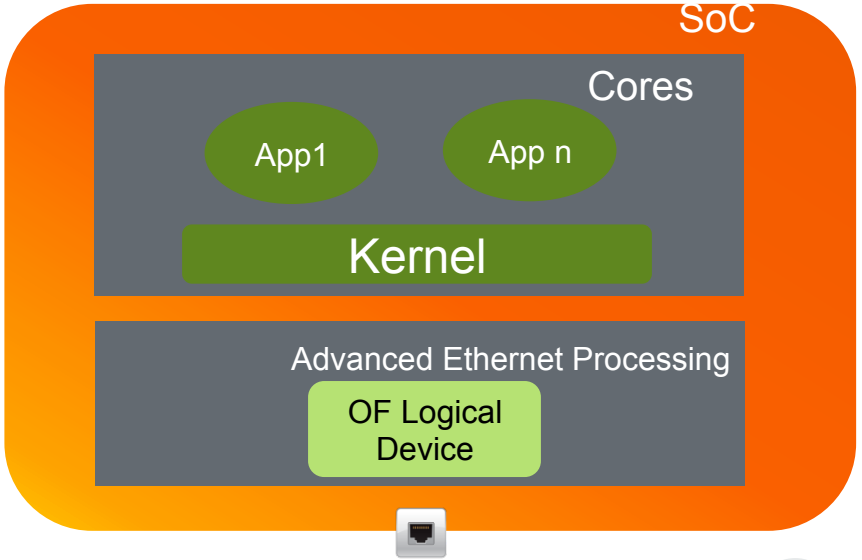
Embedded OF device in SoCs:

SoCs are being released with cores and specialized processing layer – Cores for running kernel & apps AND Advanced packet processing for OF logical devices.

No load on cores, hence deterministic performance.

Example: Freescale SoCs based on Layerscape architecture





Summary

- Embedded devices are increasingly connected to the networks (Internal and External)
  - Security is becoming critical
- Traffic Control (ACL, Conditioning, Steering etc..) becomes important to protect devices & provide visualization on the traffic going to/from the device.
- SDN/OF plays important role in achieving this.
- Embedded SDN/OF, in our view, becomes table stakes in few years.
  - Provided centralized Control
  - Provides ability to create newer applications on top of controller.
- SoC vendors such as Freescale are enabling this trend.

www.Freescale.com