Mobile network evolution towards NFV

6WIND

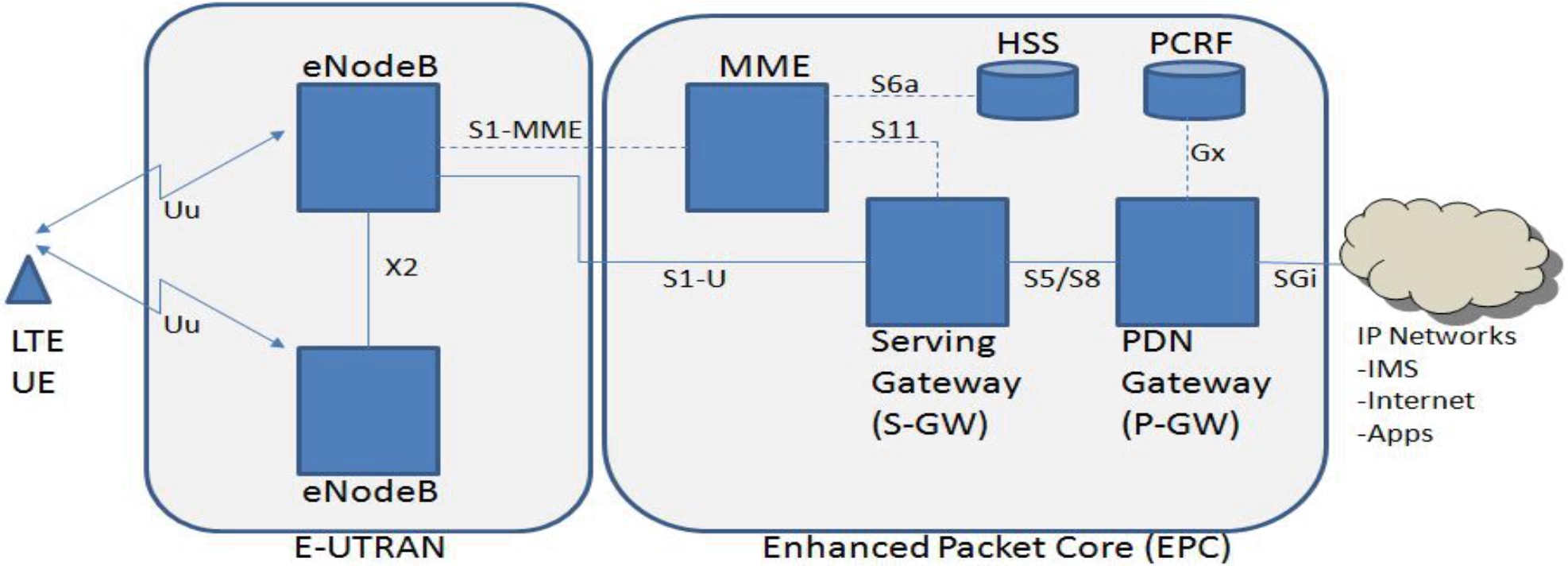
SPEED MATTERS

Nicolas Harnois

Topics

- **4G mobile network high level overview**
- Network Function Virtualization: the trend for 5G networks
- NFV use-case: virtualization of the security gateway node
- Demo: Highly Available virtualized SecGWs in a simulated mobile infrastructure

Typical 4G network infrastructure

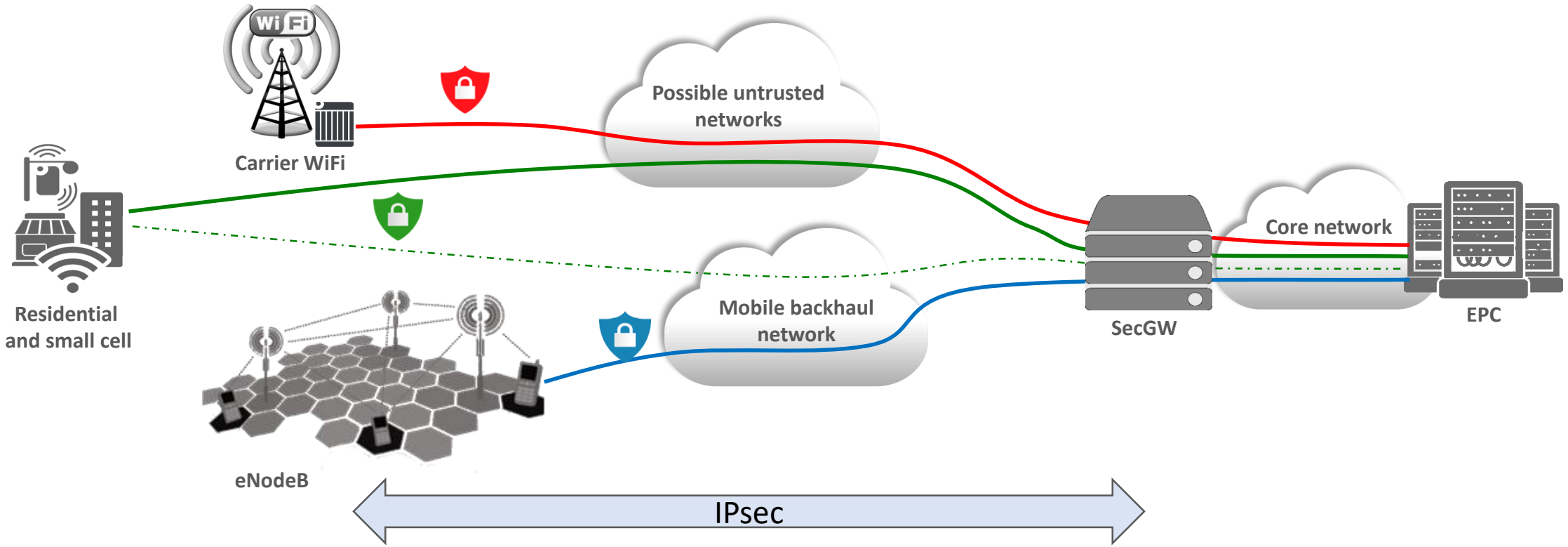


Backhaul network

4G network main components

- **UE: User equipment**: mobile phone, tablet or any other equipment accessing the 4G network
- **eNodeB: evolved Node B (LTE base station)**
- **MME: Mobility Management Entity**: Authentication and authorization of users on the network
- **HSS: Home Subscriber Server:** database of subscriber information to determine permitted services
- **S-GW: Serving Gateway:** functions as IP router with GTP support and charging functionality
- **P-GW: PDN Gateway**: acts as IP router responsible for dictating QoS and BW parameters for subscriber's session

Security issue in the 4G mobile access networks



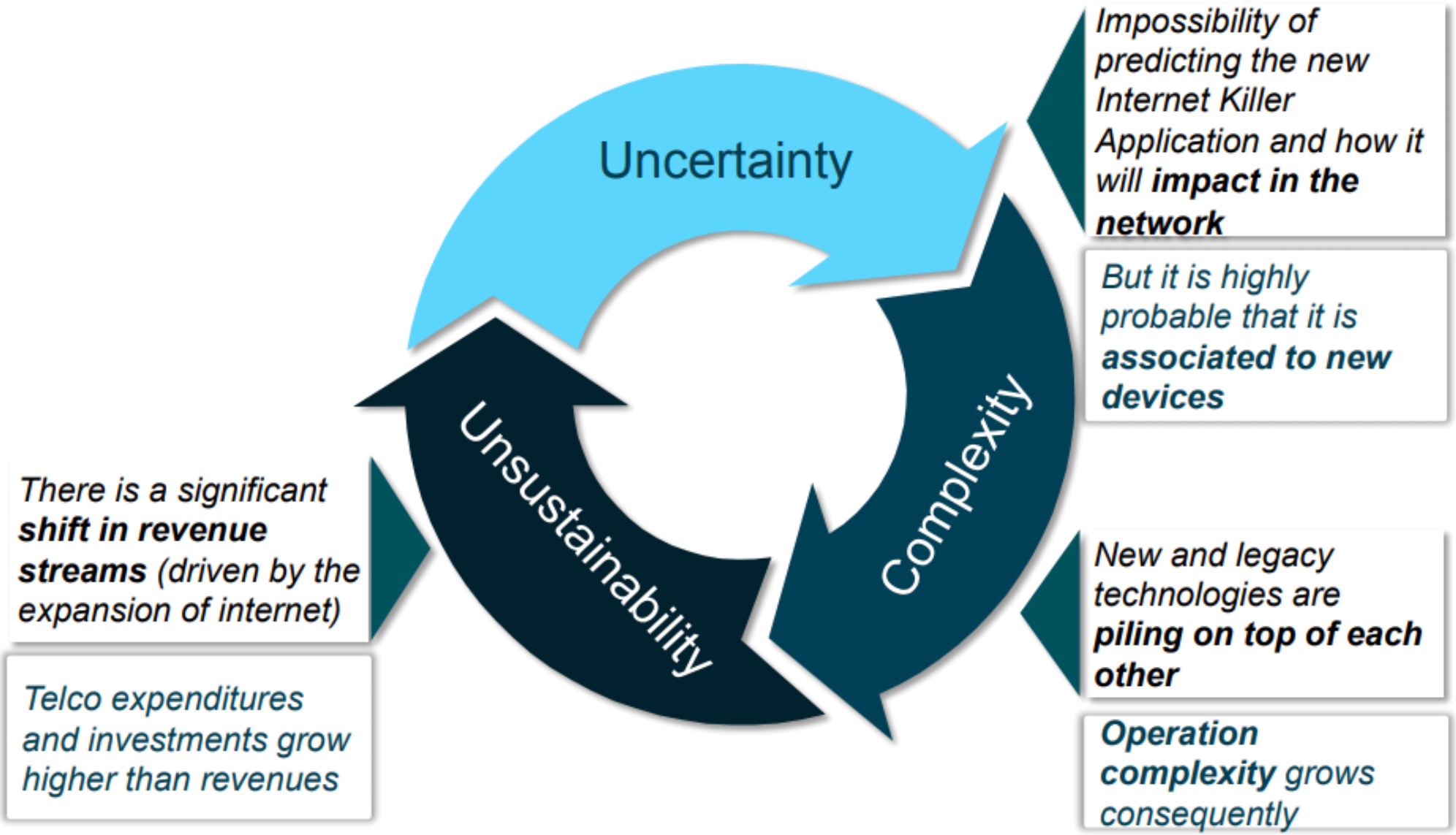
- LTE backhaul transition from ATM to full IP network: same threats than fixed such as eavesdropping and malicious eNodeB
- Connectivity everywhere: growing number of cells - small cells, HeNB, Wifi - possibly connected to untrusted network

➢ **Need to protect operator's infrastructure and customer's data confidentiality: security gateway role**

Topics

- 4G mobile network high level overview
- **Network Function Virtualization: the trend for 5G networks**
- NFV use-case: virtualization of the security gateway node
- Demo: Highly Available virtualized SecGWs in a simulated mobile infrastructure

Challenges for mobile service providers



Problematic of current Telco Networks

Long innovation cycles (2-6 years)

- Long **standardization cycles**
- **Scale is needed** to introduce **innovations**

Hardware and Software vertically integrated

- **Capacity** is tied to a **function**
- **Vendors lock in** (it is difficult to switch from one vendor to another when deployments are made)

Complex Network Management

- **Small changes in a network element requires an adaptation of the EMS** (Element Management System)
- **Complex stitching** of network functions across segments and technologies, since **network nodes are tightly coupled to the network segment and technology**

Difficult IoT

- Interoperability tests required per protocol and node

NFV: from Hardware to Software Based Packet Processing

- **Hardware based**
  - Vendor lock-in
  - Slow adopters: long development cycle and roadmap alignment with hardware capabilities
  - Not virtualization ready

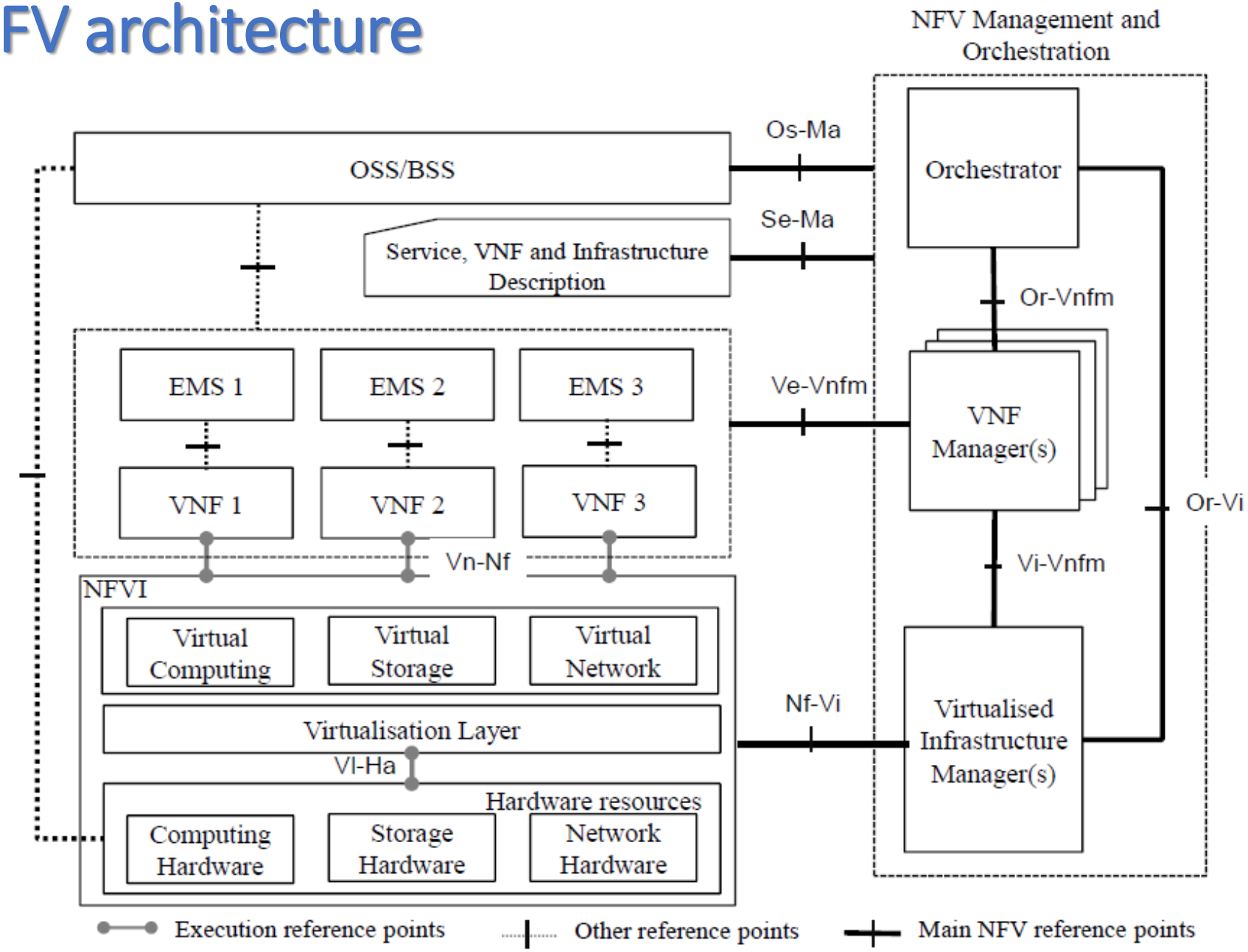
- **Software based**
  - Generic hardware, i.e. x86 COTS
  - DevOps approach for agility and rapid go-to-market
  - Virtualization ready

NFV concepts

- **Network Function (NF):** Functional building block with a well-defined interfaces and well defined functional behavior
- **Virtualized Network Function (VNF):** Software implementation of NF that can be deployed in a virtualized infrastructure
- **Virtualized Network Function Component (VNFC):** VNF can be split into multiple software components called VNFC
- **VNF Manager (VNFM):** VNF lifecycle management e.g., instantiation, update, scaling, query, monitoring, fault diagnosis, healing, termination
- **VNF descriptor (VNFD):** needed to onboard the VNF in a Management and Orchestration (MANO) layer

- **NFV Infrastructure (NFVI):** Hardware and software required to deploy, manage and execute VNFs
- **Virtualized Infrastructure Manager (VIM):** Management of computing, storage, network, software resources

ETSI NFV architecture

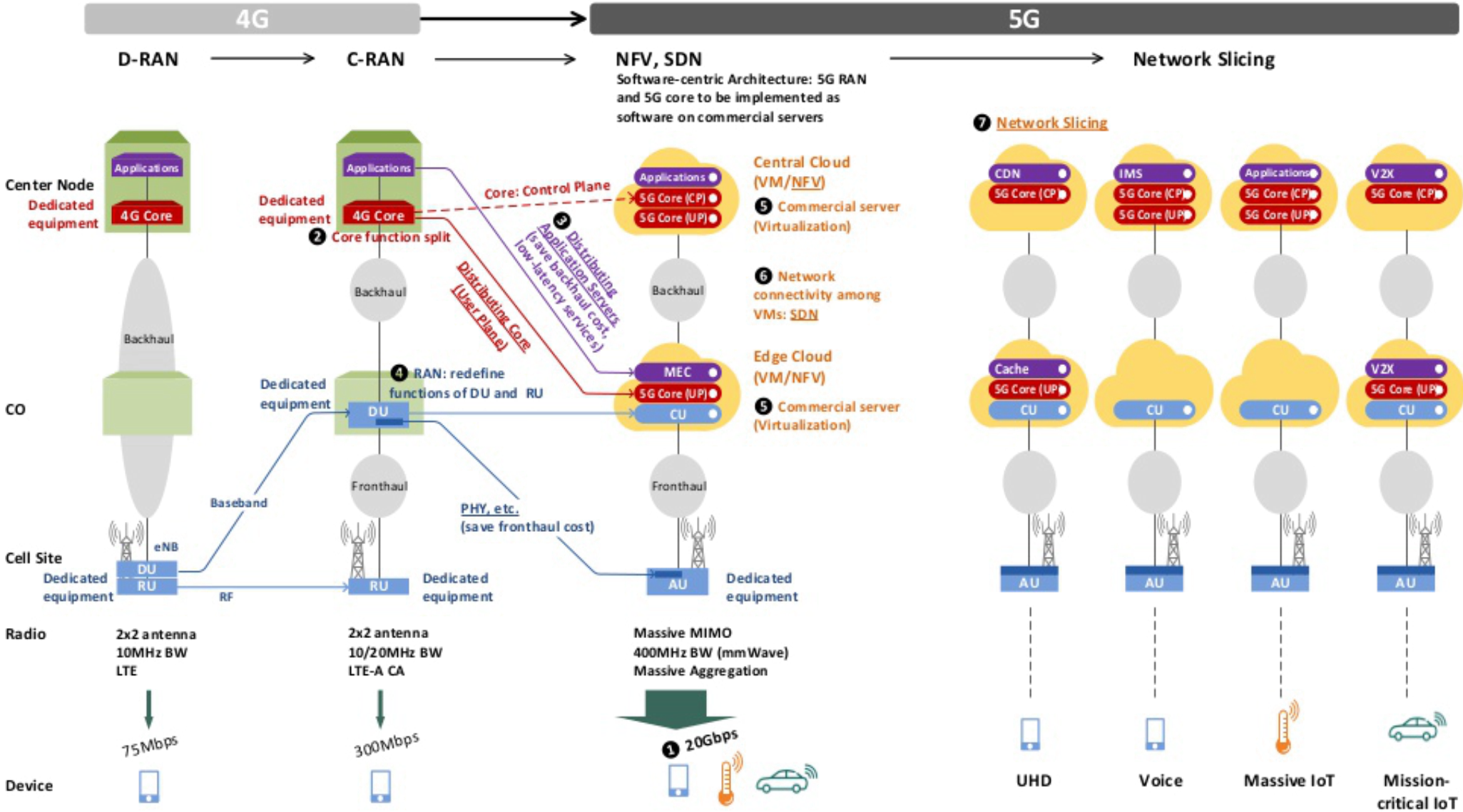


NFV promises and challenges

- Promises
  - **Virtualization** : use network resource without worrying about where it is physically located, how much it is, how it is organized, etc. Ability to provides geographic redundancy with less investment in dedicated hardware equipment
  - **Programmable**: Coupled with SDN, should be able to provide End to End orchestration of thousands of devices
  - **Dynamic Scaling**: Should be able to adapt processing power to the current performance need
  - **Energy**: Optimize network device utilization
  - **Fosters competition and innovation**: each network function can be provided independently

- Challenges
  - **Standardization**: all interfaces in the NFV architecture for good interoperability between vendors
  - **Performance**: x86 architecture challenging for user plane performance (no dedicated ASIC)
  - **Mindset**: mix network and IT expertise for design, implementation, and operational staff
  - **Support**: NFVI vendor being decoupled from VNF vendor, when issue occurs, who is supporting the solution

Mobile network evolution to 5G: virtualization and slicing

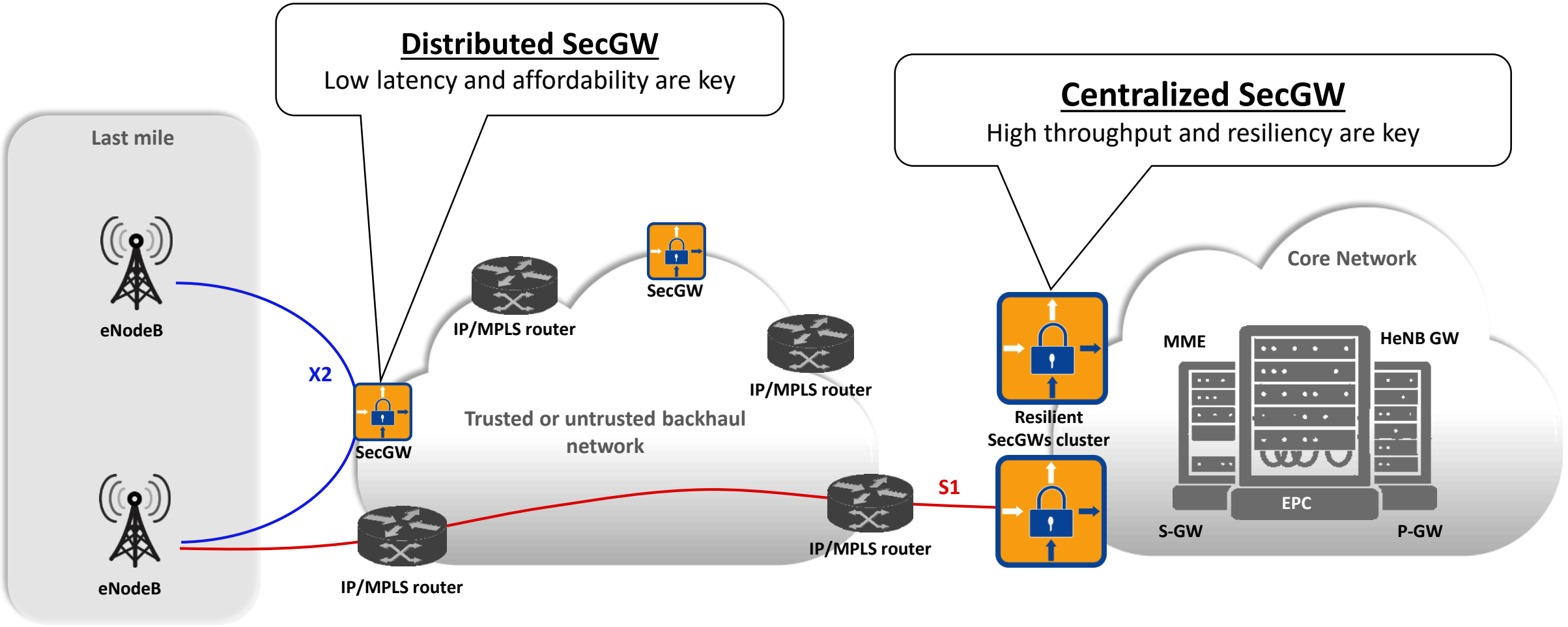


DU: Digital Unit (BBU)
RU: Radio Unit (RRH)
CU: Central/Cloud Unit
AU: Access Unit
UP: User Plane
CP: Control Plane
MEC: Mobile Edge Computing
NFV: Network Function Virtualization
SDN: Software Defined Networking
V2X: Vehicle-to-X
IoT: Internet of Things
IMS: IP Multimedia Subsystem

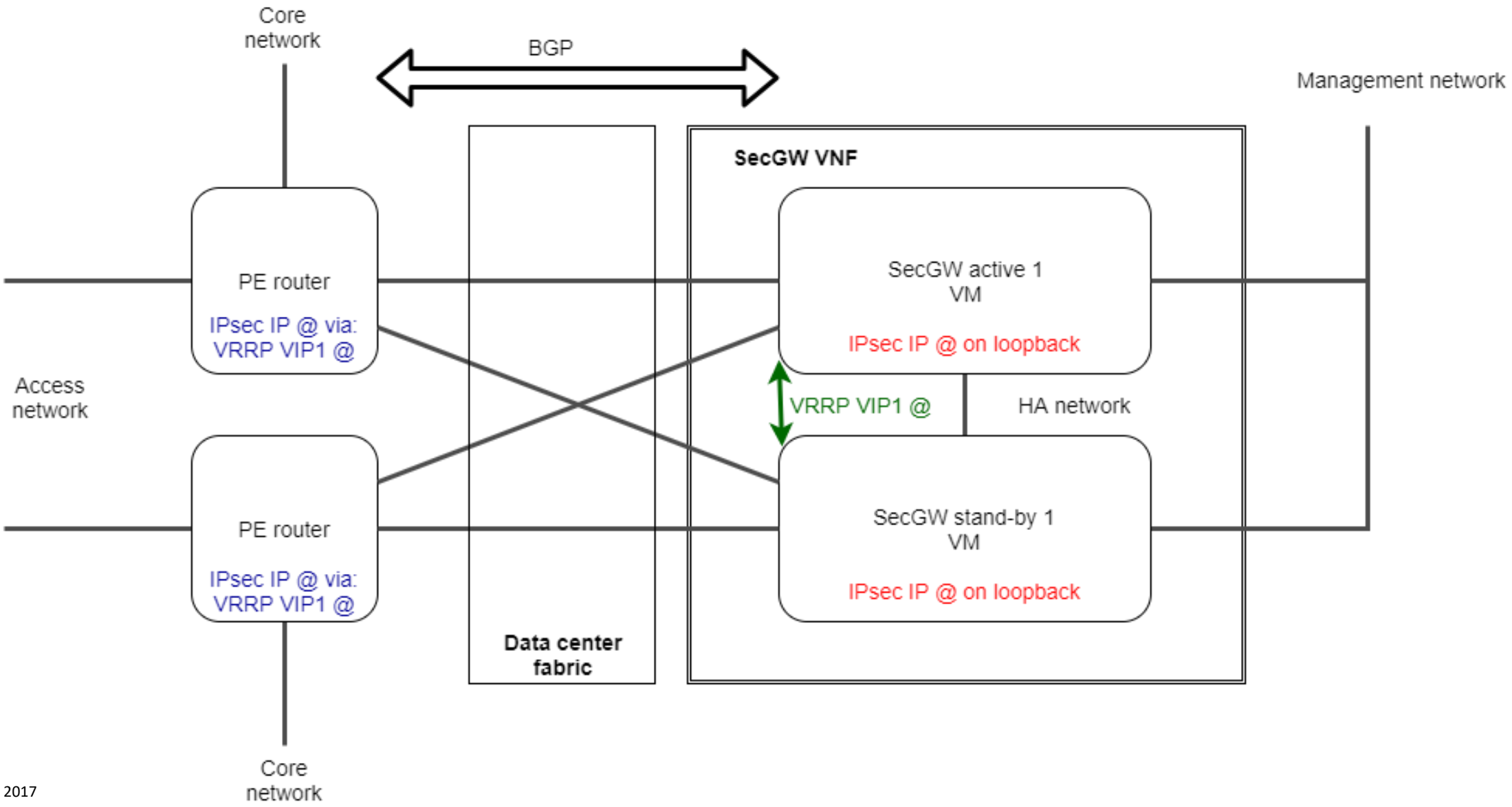
Topics

- 4G mobile network high level overview
- Network Function Virtualization: the trend for 5G networks
- **NFV use-case: virtualization of the security gateway node**
- Demo: Highly Available virtualized SecGWs in a simulated mobile infrastructure

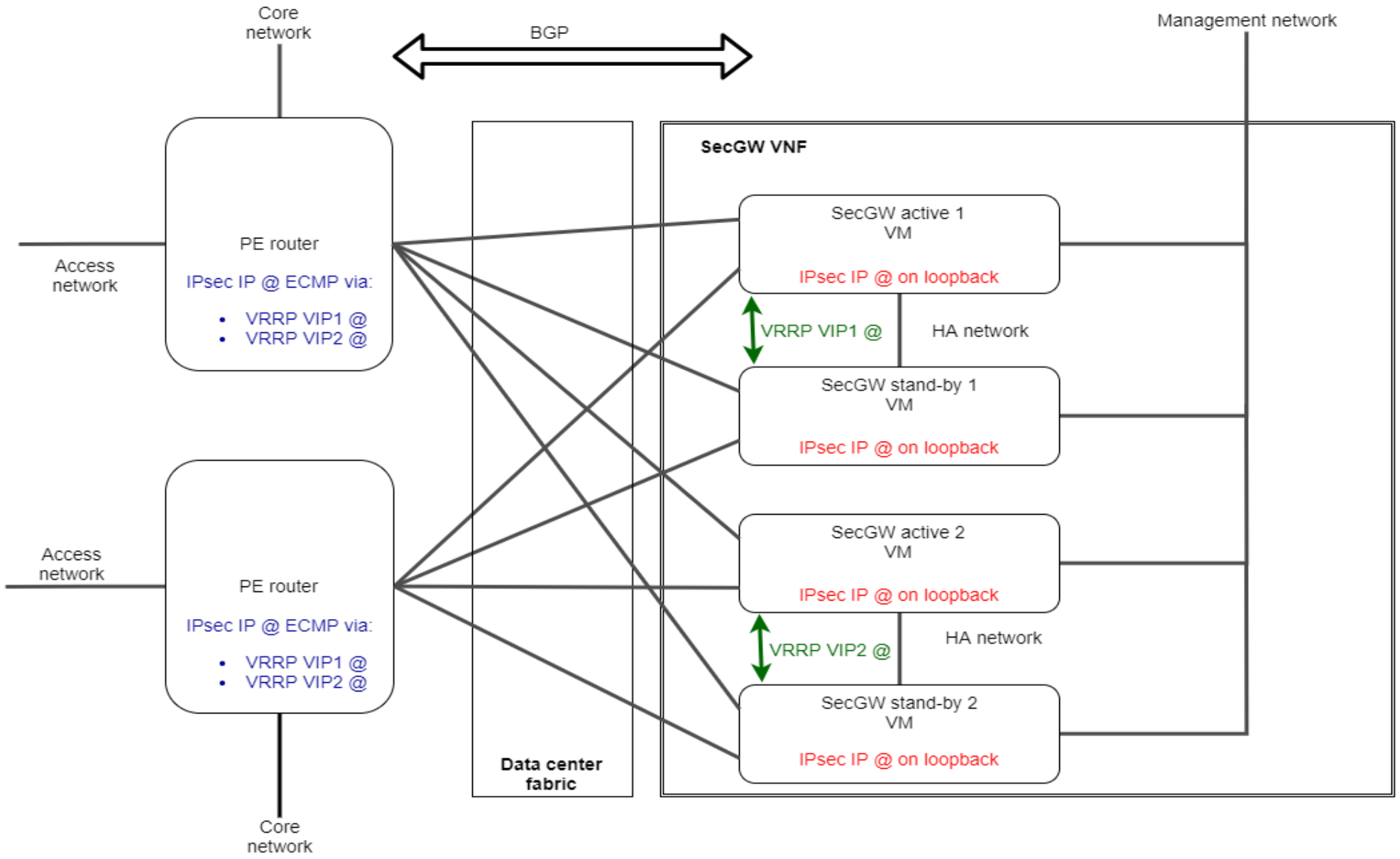
SecGW virtualization deployment options



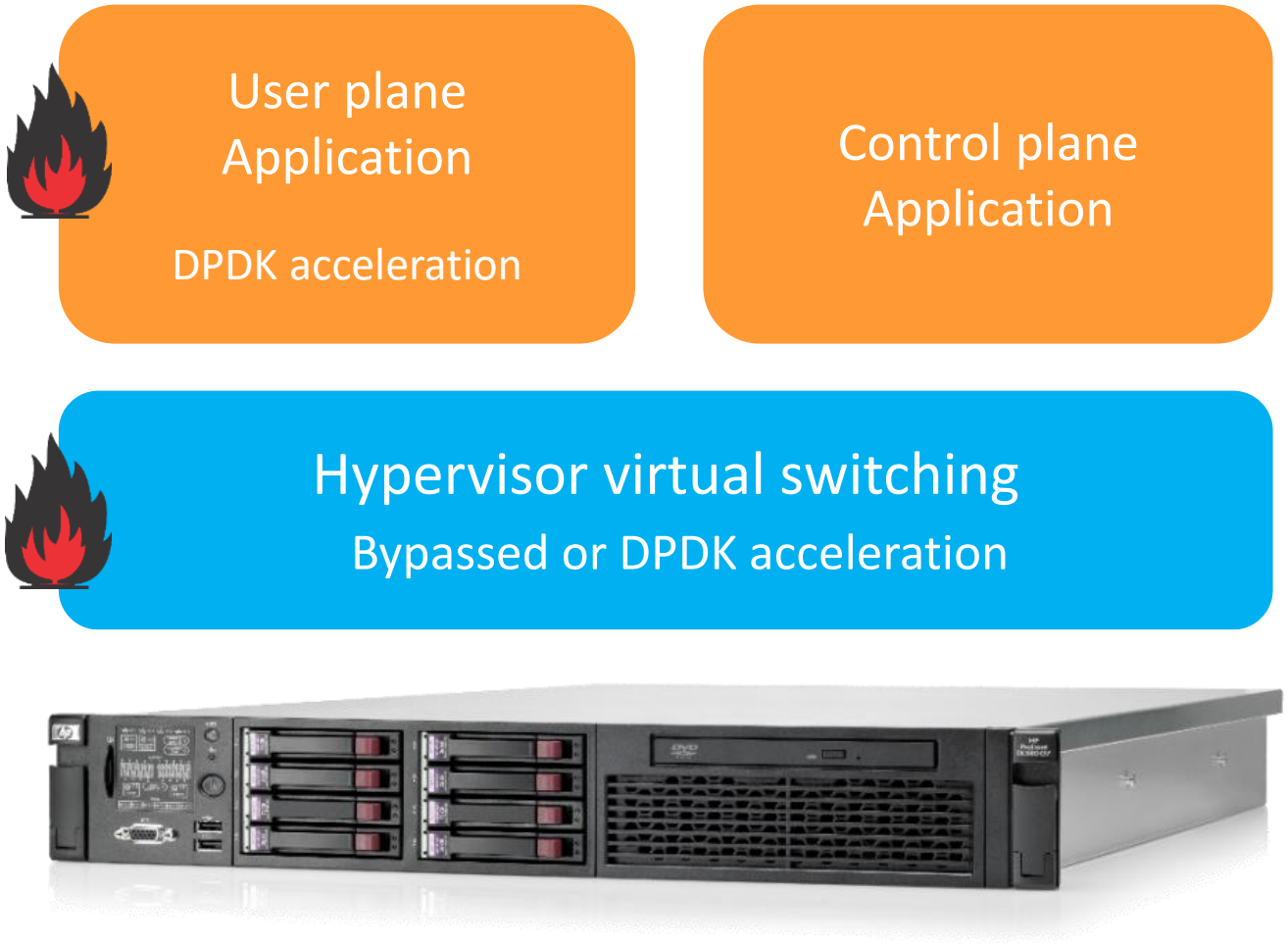
SecGW virtualization architecture: initial deployment



SecGW virtualization architecture: scale out



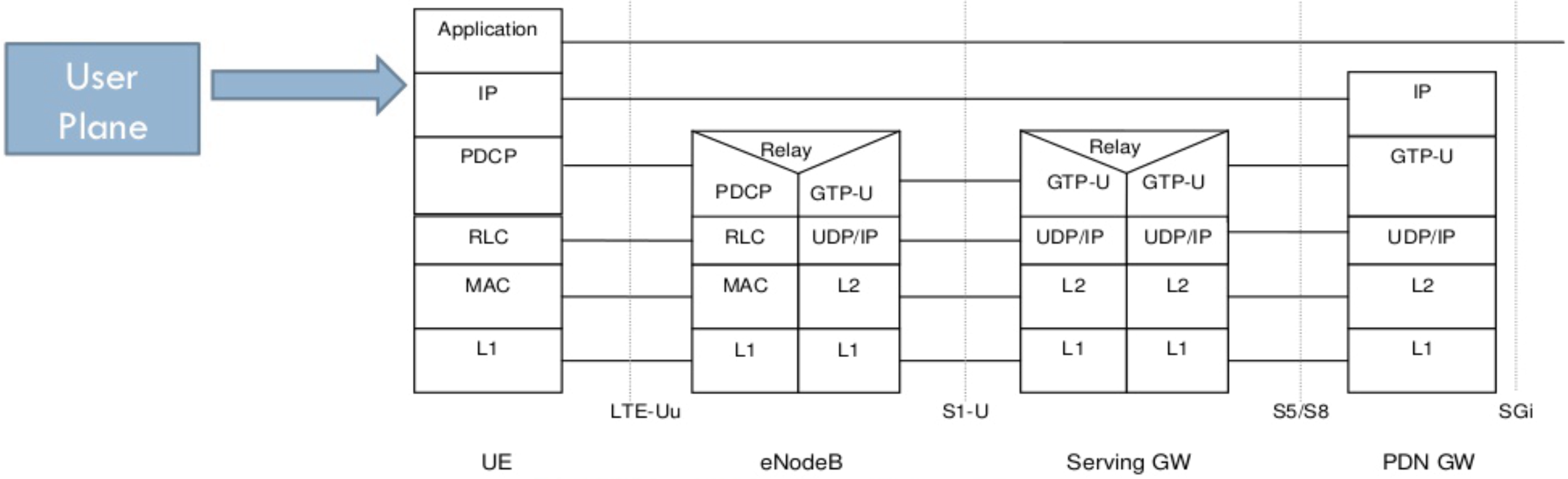
User plane performance challenge on COTS



Topics

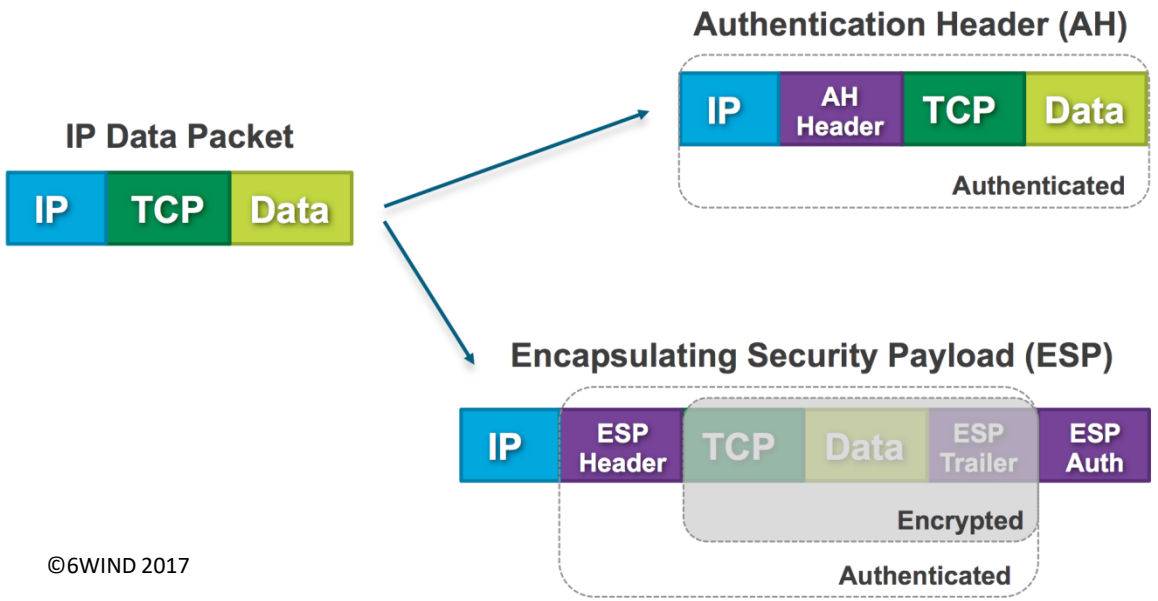
- 4G mobile network high level overview
- Network Function Virtualization: the trend for 5G networks
- NFV use-case: virtualization of the security gateway node
- **Demo: Highly Available virtualized SecGWs in a simulated mobile infrastructure**

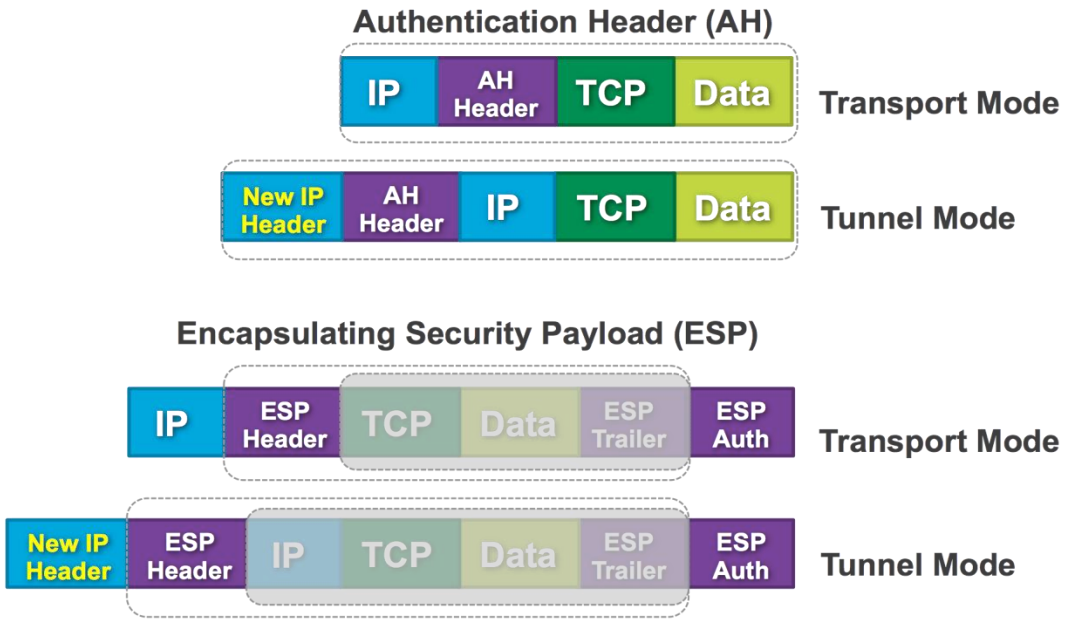
4G network user plane stack from UE to P-GW



Few words about IPsec

- **IPsec is a standard based security architecture for IP hence IPsec**
- **Two different protocols:**
  - Authentication only: protect and verify integrity of data - make sure data is not changed during transport. Using AH (Authentication Header) and IP protocol 51.
  - Authentication and encryption: make sure nobody can eavesdrop on the data in transport. Using ESP (Encapsulating Security Payload) and IP protocol of 50.
- **Two different modes**:
  - Transport: preserving original IP header. Typically used in combination with GRE or other encapsulating protocols.
  - Tunnel: encapsulating entire IP datagram within a new header, essentially tunneling the packet.

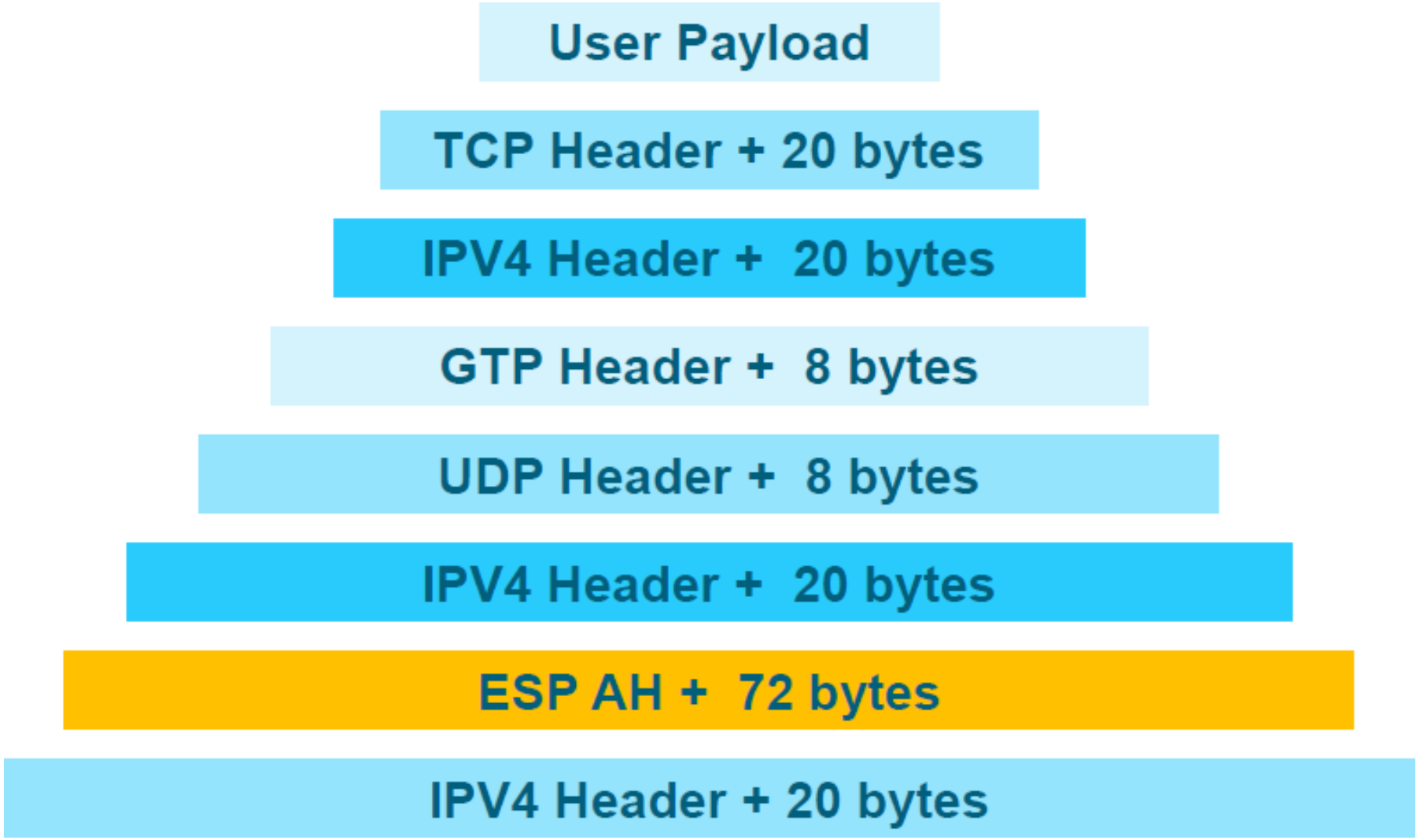




Few words about IPsec (cont'd)

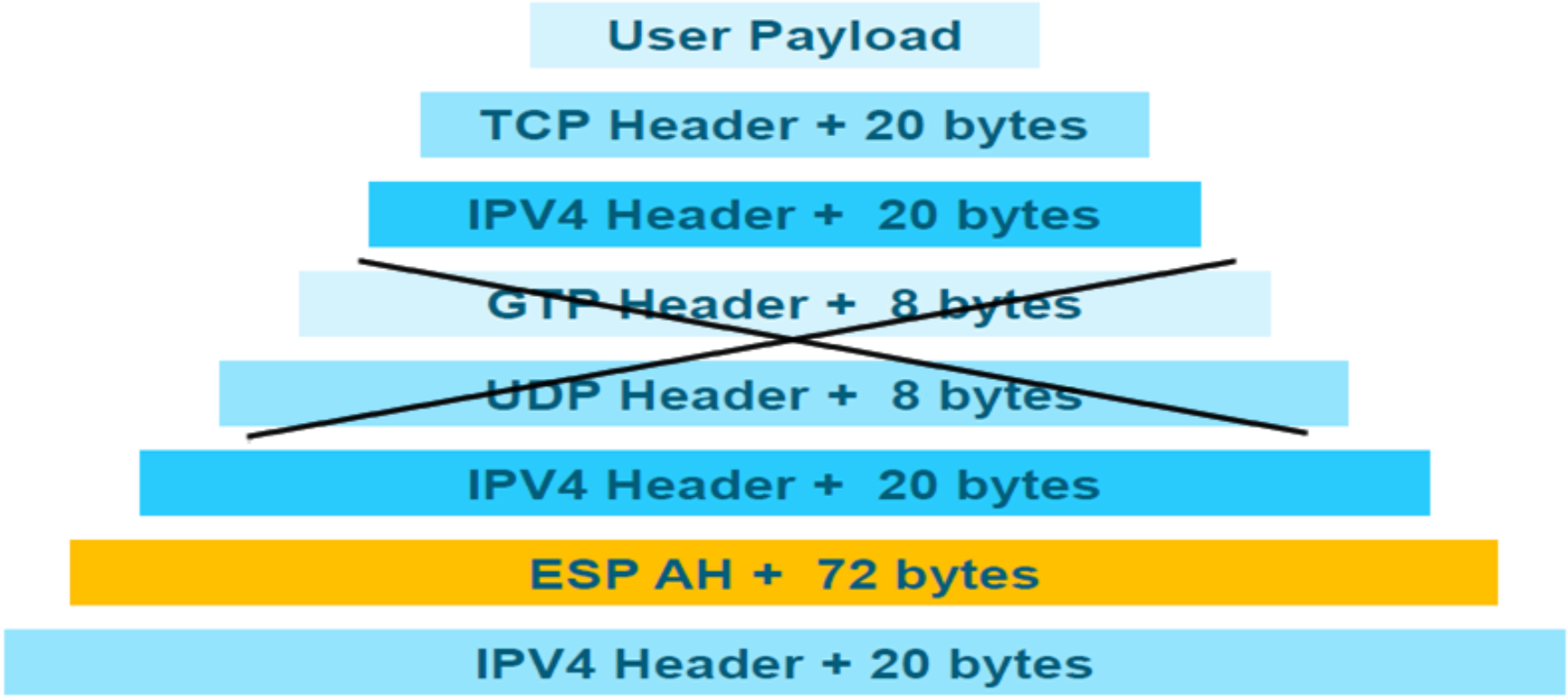
- **Security Policies (SP):** some kind of ACLs to define which traffic must be cipher
- **Security Association (SA)**: defines how to cipher the traffic matching a security policy (mode, protocol, algorithm, tunnel endpoint IP addresses, etc.)
- **Static versus dynamic IPsec**
  - **Static**: SP & IPsec SA are configured manually (e.g. ip xfrm <state|policy> <add|del> commands)
  - **Dynamic**: use a specific control plane protocol: **IKE** (Internet Key Exchange), e.g. strongSwan, to negociate keys (SA) between two peers. Allows usage of certificate, integration with a Public Key Infrastructure (PKI), automatic rekeying, etc. There are two phases in IKEv2 protocol:
    - IKE phase 1 (aka IKE SA phase): IKE gateways authenticate each other and negotiate cryptographic material (IKE SAs), to secure one or more IKE phase 2 exchanges
    - IKE phase 2 (aka Child SA phase): IKE gateways negotiate the IPsec SAs themselves. One or more successive phase 2 exchanges are authenticated and encrypted thanks to cryptographic material negotiated during IKE phase 1.

4G network user plane stack with IPsec (ESP tunnel mode)

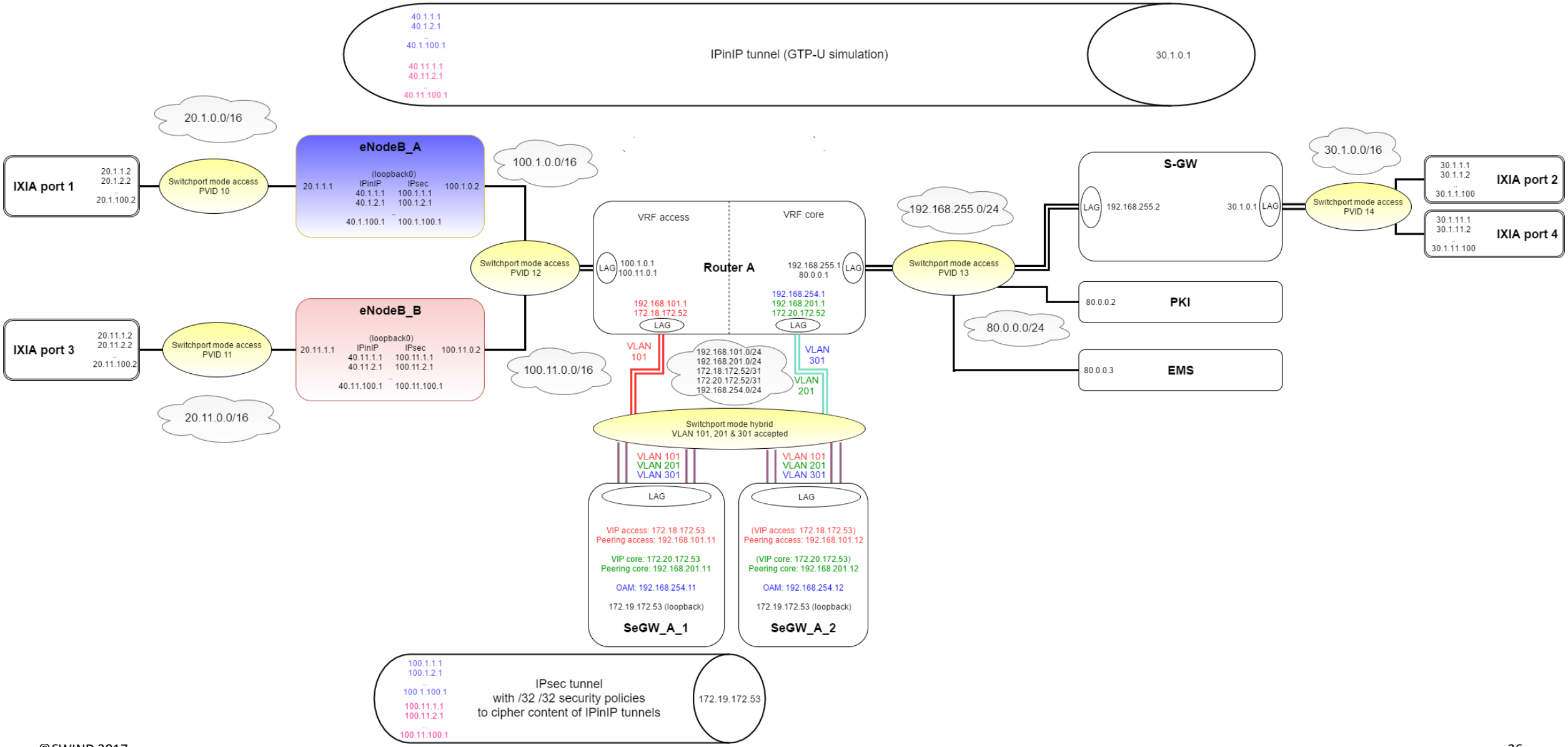


Demo scenario

- Representative use-case of encapsulation and IPsec policies of a realistic scenario from the security gateway point of view, for S1-U traffic encryption
- To simulate GTP tunnels between eNodeB and S-GW, simple IPv4 in IPv4 tunnels are used instead of GTP-U



Demo network scheme



Demo – Physical description of the setup

- **Five physical servers are used:**
  - Combination of mono and dual sockets x86 servers: 12 cores/24 threads per CPU
  - 10Gbps connectivity
  - 64GB RAM
- **All the Network Functions are running as VMs, using 10Gbps interfaces in PCI passthrough mode**
- **IXIA IxNetwork is used to generate the traffic**
  - 2x10Gbps port are connected to the eNodeB VMs
  - 2x10Gbps port are connected to the Serving Gateway
- **6WIND's Network Testing Framework (NTF) is used to instantiate the network scenario on the machines**
  - Coupled with Jenkins, provides function and performance test automation

Demo – Flow description (from UE to Internet)

- **IXIA simulates UE and generates traffic from 20.x.y.2 to 30.1.x.y**
- **eNodeBs encapsulate IXIA traffic in IPinIP tunnels (with S-GW as endpoint) to simulate GTP tunnels encapsulating UE traffic (S1-U traffic)**
  - eNodeBs route each 30.1.x.y address through an individual IPinIP tunnel, to simulate multiple eNodeBs (100 per VM)
  - eNodeBs define security policies to secure its communication with S-GW
  - eNodeBs will then negociate keys with the security gateway (IKEv2)
  - After successful key exchange, IPinIP packets are encapsulated in IPsec tunnels
- **The router routes the traffic to the Security gateway in the access VRF**
  - This router only see IPsec traffic between eNodeBs and the security gateway
- **VRRP master Security Gateway receive the encrypted traffic**
  - IPsec tunnel is terminated on the active security gateway, packets are deciphered and routed to S-GW
  - The route to 30.1.0.0/16 network has been previously learned using BGP (pushed by S-GW)
  - After IKE negociation with eNodeB, IKE daemon adds a route for reverse traffic for each IPsec tunnel, and propagate the route using BGP to S-GW.

    Known as Reverse Route Injection (RRI) (e.g. 40.1.1.1 via 172.20.172.52)
- **The router routes the traffic to the Serving gateway in the core VRF**
- **S-GW terminates IPinIP tunnel, retrieve the original IXIA packet (20.x.y.2 to 30.1.x.y) and route original UE traffic to its connected IXIA port (Internet)**

Demo – Flow description (from Internet to UE)

- **Ixia generate traffic from 30.1.x.y to 20.x.y.2**
- **S-GW encapsulate IXIA traffic in IPinIP tunnels (with eNodeB as endpoint) to simulate GTP tunnels encapsulation of S1-U traffic**
  - Destination IP after IPinIP encapsulation is then 40.x.y.1
  - Route to reach this eNodeB is learned by BGP, after Security Gateway added the route using RRI, and propagated the route to the S-GW.
- **The router routes the traffic to the VRRP master security gateway (in the core VRF)**
- **VRRP master Security Gateway receive the clear traffic from S-GW**
  - As it matches the defined security policies, traffic is encapsulated in IPsec tunnel and ciphered
  - It is then routed to the eNodeB through the Mobile Backhaul router
- **The router routes the traffic to the eNodeB**
  - This router only see IPsec traffic between eNodeBs and the security gateway
- **eNodeB receives encrypted traffic**
  - IPsec tunnel is terminated on the eNodeB, packets are deciphered
  - IPinIP tunnel is then terminated, retrieve the original IXIA packet (30.1.x.y to 20.x.y.2) and route traffic to its connected IXIA port

Demo – HA: VRRP and IKE/IPsec stateful failover

- **When a Security gateway fails, the VRRP protocol ensures that the VIP will change from master to backup**

- **IKE/IPsec HA is used at the security gateway level to ensure continuity of the traffic during the failover**
  - IKE and IPsec Security Associations (SA) synchronized between the VRRP master and slave
  - IPsec sequence numbers synchronized for each SA

- **All the routes are exchanged with the next hop selected as the VRRP VIP**
  - VRRP on both access and core sides, with group synchronization
  - No need to learn back routing information using BGP, would be too long
  - Failover time is the time to learn new MAC address on a different switch port (gratuitous ARP sent by the new VRRP master)

Sources

Telefonica: challenges of service providers and problemtatics of Telco networks

http://www.it.uc3m.es/fvalera/t2/5.pdf

Netmania: Network evolution (5G and NFV)

https://www.slideshare.net/Netmanias/netmanias20170424sdnnfvstrategies-and-progresses-in-network-operators?ref=https://www.netmanias.com/en/post/reports/11966/sdn-nfv-vcpe/sdn-nfv-strategies-and-progresses-in-network-operators

https://www.slideshare.net/Netmanias/netmanias201512315-g-network-architectureen

Cisco: IPsec introduction:

https://supportforums.cisco.com/t5/security-documents/crypto-map-based-ipsec-vpn-fundamentals-negotiation-and/ta-p/3153502