# A Comprehensive Survey on 5G Adaptive Network Slicing: Key Technological Principles, Deployment and Operation Challenges

**Evangelos G. Siatiras**

# State of the Art Concepts in 5G Architecture

- Service Based Architecture
  - An abstract concept of an application function
  - Inherits Publisher and Consumer Model
- Orthogonality of the Functions
  - Management roles are uniquely assigned to functions
  - Every function serves for a specific purpose
  - Clear separation between Control and User Plane Signaling
- SDN Principles Adoption
  - SMF has the role of an SDN Controller for the UPFs
  - PDU Flows can be dynamically been setup and programmed

# Considerations in SBA

- HTTP2 is totally inherited in CN
  - One Signaling Stack in every interface
  - One common interface will support any type of request between all network functions
  - The induce of signaling protocols is performed right once rather than having five or six different protocols

# A State-of-the-Art Concept behind Network Repository Function (NRF)

- Offers Enhanced capabilities for gateway selection comparing to DNS in 4G
  - Replacing DNS with a much broader operator central repository concept
  - Layer 2 and Layer 3 information and application layer information are being stored
  - Every Function can pull all the required information for a 3GPP Procedure Initiation
  - Operators especially in roaming scenarios can request such data faster
  - Reduces the potential for human error

# Exposure Capabilities of 5G Architecture

- CN can be securely exposed to 3rd parties
  - Security Level and Hierarchies are defined
- 3rd parties can request to change data (Policies, Charging) within CN
- Gives an initiative to Big Data
  - Offers dynamic subscription or pulling for data
- Offers troubleshooting functionality in roaming scenarios
  - The Serving Operator can request through an interface for subscriber data
    - SLA Agreements should be considered for the required permission to be granted

# Stand-Alone (SA) and Non-Standalone (NSA) Architecture Comparison

- Standalone Option: the New Radio (NR) is directly connected to the 5G core
- Non-Standalone Options: The LTE is connected to the Core network and the NR connected to the LTE and vice versa

| |  NR (5G) |  LTE/eLTE (4G) NR (5G) |  NR (5G) eLTE (4G) |
|---|---|---|---|
| **Feature** | **Standalone (SA)** | **Non-standalone (NSA)** | |
| **Master carrier** | NR | LTE and eLTE | NR |
| **Secondary carrier** | - | NR | eLTE |
| **Core choice** | 5G core (5GC) | 4G EPC or 5G core (5GC) | 5G core (5GC) |
| **Operator perspective** | Simple, high performance overlay | Leveraging existing 4G deployments | |
| **Vendor perspective** | Independent RAN product | Requires tight interworking with LTE | |
| **End user experience** | Peak bitrate set by NR<br>Dedicated Low Latency transport | Peak bitrate is sum of LTE and NR<br>Latency impacted if routed via LTE master | |


| **Feature** | **EPC** (4G core) | **5GC** (5G core) |
|---|---|---|
| RAN interface | S1 with per UE assigned MME & assigned SGW | NG2 to per UE assigned AMF & multiple NG3 to UPF |
| Authentication | Access dependent procedures | Unified procedures: fixed, 3GPP & non-3GPP access |
| Network slicing | Single slice per UE | Multiple slice per UE |
| QoS model | QCI based bearers | Flow based QoS |
| Short packet | Connection oriented only | Connection and (later) connectionless mechanisms |
| Cloud native | Possible but node based | Explicit linkage to cloud based mechanisms |

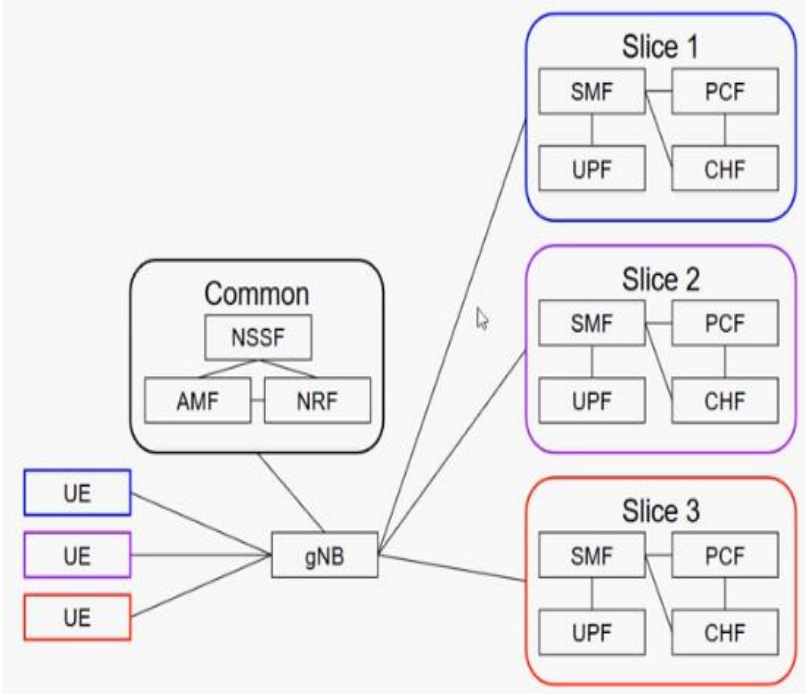
# Network Architecture Comparison

# Network Slicing Research Based on Different Requirements

- There is no common definition of Network Slice and it's provided services
- Diverse SDOs are dedicated to research Network Slicing
- There variations between each organization based on opposing views on network slicing
- Goal: Standarization of network slicing in an independent way focusing to their own perspective of network slicing
- There are four Main SDOs: IETF, 3GPP, ETSI and GSMA
- 3GPP is focusing on Standardizing the architecture concerning the Management and Orchestration Planes
- IETF has been inspired by 3GPP and focus on standardizing a technology-independent information model
- ETSI advises how to map network slicing use cases identified in other SDOs to the ETSI NFV architecture framework
- GSMA gives an overview on network slicing and how it serves and promotes 5G roadmap but from a business perspective

# 3GPP Perspective: High-Level Network Slicing Principles and Mechanisms Overview

- Network Slicing can be considered as a session management profile or a service profile where a single network is logically divided into slices of networks to provide a different type of service to specific subscribers.
- Several Mechanisms offered through this profile (Policy Control, Charging)
- Every NF instance is 3GPP defined
- Every NF instance is considered as a communication service, combined with several core networks and with several access networks



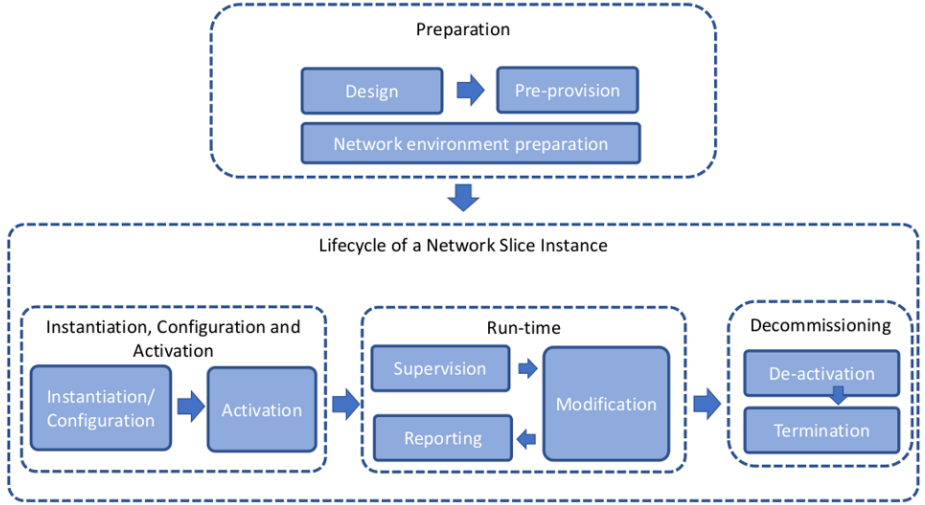
# 3GPP Perspective: Security Aspects in Network Slicing

- A virtualized E2E Packet Core comes inherently with Network Slicing
- The 5G network is being isolated and thus every NSI running in an independent way for the others
- An attack in a particular slice to intrude into the virtualized Packet Core of that Slice, does not affect the other existing slice instances as they are isolated.
- However, is an operator's decision of the architecture and the orchestration tools will be used for the Packet Core
- Goal: The data traffic and critical session or even access management traffic should be isolated from the common dedicated devices per slice.
  - The Corresponding Functions should be isolated in in different containers or different virtual machines.

# ETSI Perspective: Network Slicing Lifecycle Management and Monitoring Phases

A network slice is a dynamic entity therefore its lifecycle must be managed in the following phases

1. Preparation Phase
   - Design and preparation of a slice template
2. Commissioning Phase
   - Instantiation request to create, configure and activate the slice
3. Operation Phase
   - Activation, supervision, performance reporting
4. Decommissioning Phase
   - Removing the network slice instance specific configuration from the shared constituents



# Management and Orchestration Plane Derived Models

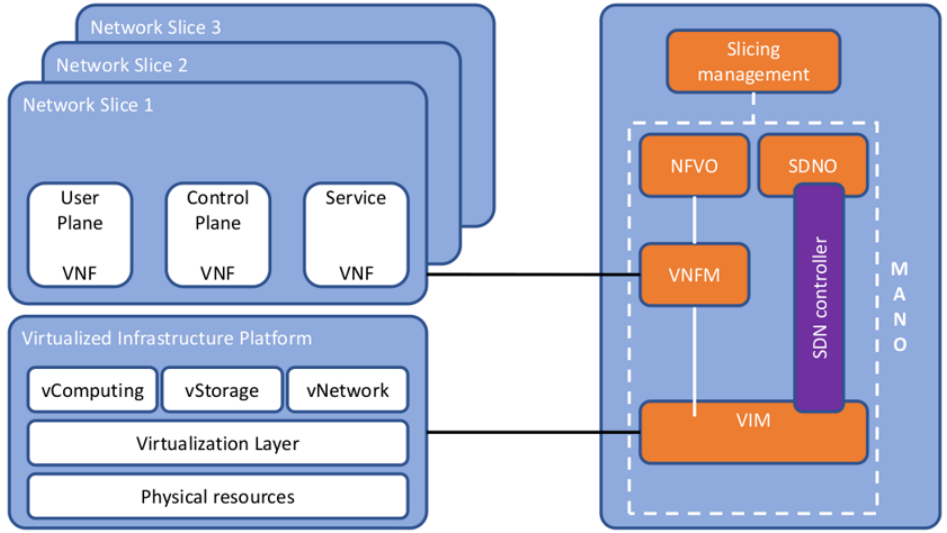
Single Owner Single Controller Model

Single Owner and Multiple Tenants Model

Multiple Owners or Multiple Tenants Model.

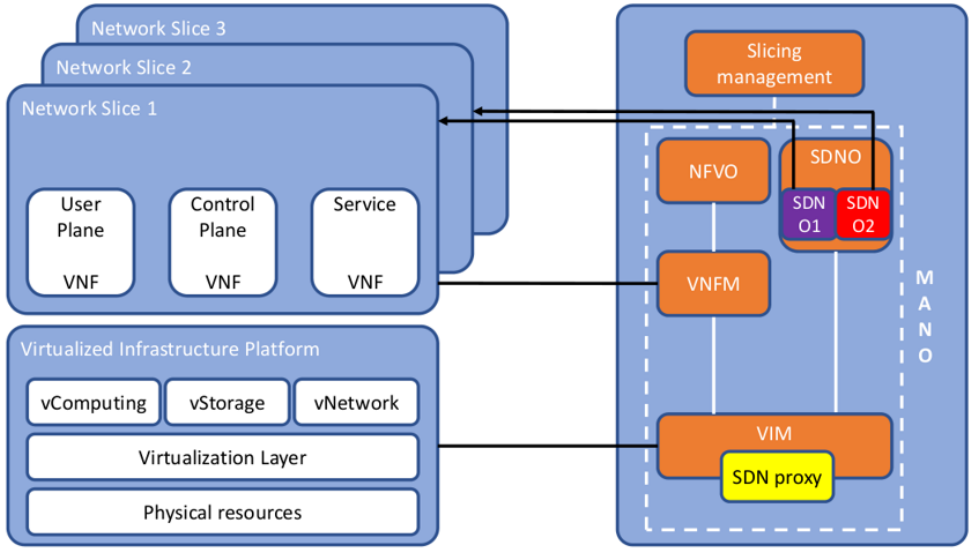
# Single Owner Single Controller Model

- The management and orchestration functionalities are subsequently implemented on top of the SDN controller by exploiting the northbound interface
- The SDN controller operates as an SDN Orchestrator
- One SDN controller will completely orchestrate all the different slices
- Ideal for small network operators especially in a case of a single infrastructure owner
- Bottleneck in terms of performance and reliability as the presence of the single controller limits the programmability of the networking infrastructure especially in case multiple tenants desire deploying network services



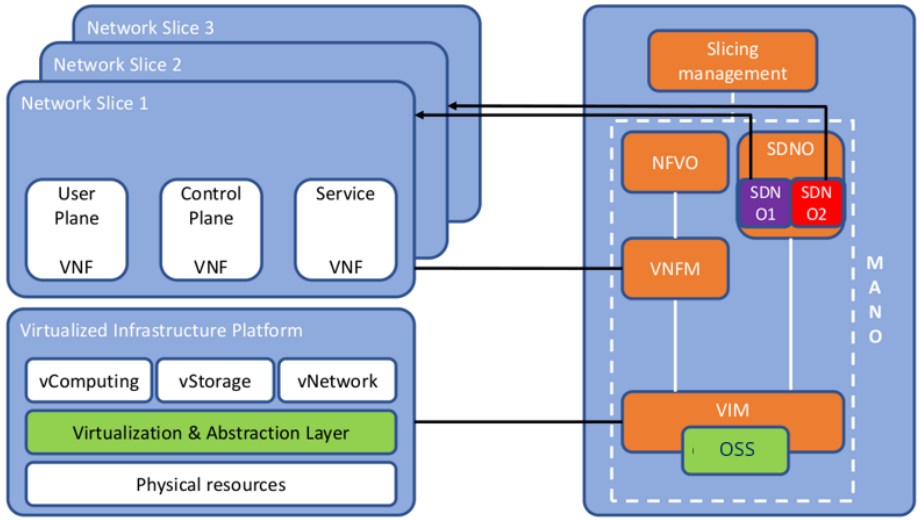
# Single Owner, Multiple Tenants Model

- Introducing an SDN Proxy typically controlled by the owner of the physical network infrastructure
- The SDN Proxy provides the network forwarding path based on the specs defined in each NS by maintaining the required isolations
- Enabling multiple virtual tenants to deploy their own controllers or SDN Orchestrators on the shared infrastructure



# Multiple Owners or Multiple Tenants Model

- Allow multiple tenants to specify their desired way for their resources to be connected
- The implementation choice is independent from the service or infrastructure providers
- One or more Controllers are used to handle the portion of requirements per tenant in an isolated way
- An “Abstraction Layer” is introduced allowing to create isolated virtual networks with the topology specified by the tenants
  - Any SDN Controller can be deployed
- User are able configure their virtual network on demand
- Infrastructure owners retain control of its own virtual SDN network for recovery purposes (Physical Failure).



# The GSMA Perspective of Network Slicing

"The whole 5G will require one network with low delay, high throughput and high resilience"

- Diverse Services require diverse performance requirements able to be provided through a unified network concurrently.
- Today's networks are not able to fulfill this kind of demand as offering the best effort service
  - Traditional networks resulting in any guarantees in delivery of data and are not capable of providing E2E QOS Services
- 4G Architecture is only appropriate only for today's Specifications
  - Is a balanced network among divergent solutions, thus not capable of support all the requirements simultaneously
  - These requirements are continuously changing with an unpredicted way
  - Network Slicing will lead to several physical networks with individually determined quality of service parameter sets
- Two Mechanisms must be defined for future Networks
  - Enable rapid deployment of the related network configuration
  - Multiple QOS parameter sets on one shared physical network infrastructure should be able to be provided

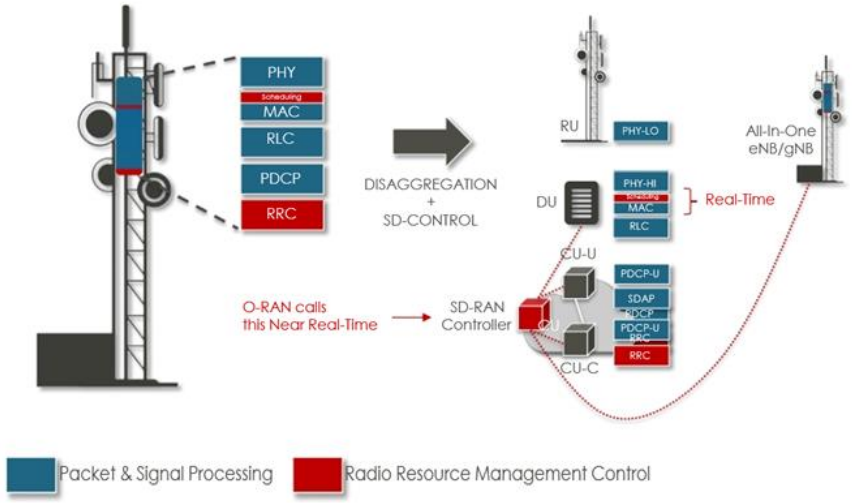
# 8. FUTURE CHALLENGES AND RESEARCH DIRECTIONS

# Different Understanding and Emphasis of Each Organizations

**Table 1: Summary on the Similarities and the Differences Between SDOs' Visions**

| SDOs Modelling Aspects | Provision Models | | | NS Service Request | Network Domain | | | | Main Contribution |
|---|---|---|---|---|---|---|---|---|---|
| | SaaS-like | PaaS-like | IaaS-like | Service/Slice profile | RAN | Core | Transport | General | |
| ETSI | | ✓ | | | | | | ✓ | Generalized NS architecture and its associated workflows |
| 3GPP | ✓ | | | ✓ | ✓ | ✓ | | | Information/data model for NS provisioning and management on RAN and Core network |
| GSMA | ✓ | | | ✓ | ✓ | ✓ | ✓ | | GST/NEST |
| IETF | | ✓ | | | | | ✓ | | Technology-Independent information model for NS management via a network-agnostic interface |

# ORAN Protocol Stack Disaggregation for Network Slicing




- An SDN Controller can be applied separating CU into CU-U and CU-C orchestrated by an SD-RAN Controller
- The Near-RT RIC is logically centralized and it's at the edge
- Slicing of the RAN comprises the disaggregation of the scheduling operation and the virtualization of the available physical resources in such a way that the scheduler maps the physical to the virtual resources.
  - Dedicated Schedulers with private resources serving UEs based on type of service.
- Overall, can be considered as many virtual base stations dedicated to different slices in a composite physical hardware.

# Extending Network Slicing at the Edge

- Edge is where public Cloud meets the network Cloud
- UE should be able to reach an OTT Application with the minimum latency
- OTT disaggregation into microservices leading to hosting closer to the UE
- The optimal solution is to host a microservice in the Mobile Network cloud
  - Special agreements on co-hosting between Operators and Public clouds may not feasible
- By adopting NS multiple UPFs can be placed accordingly, based on the type of service
- The OTT application is becoming a tenant to the Telecom Operator's cloud and as a tenant asks for a particular service type through a particular network slice

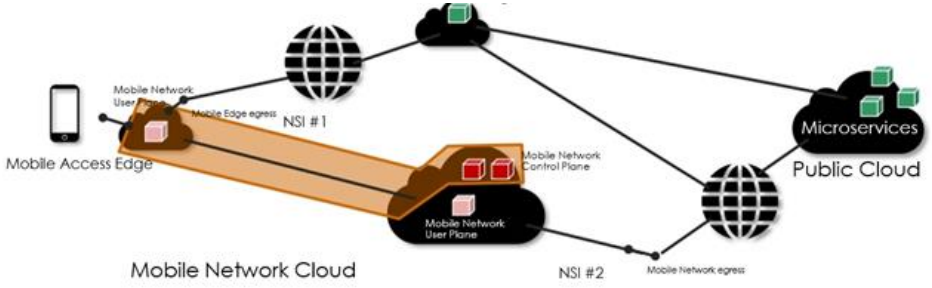



**Figure 55: UPF at the edge**

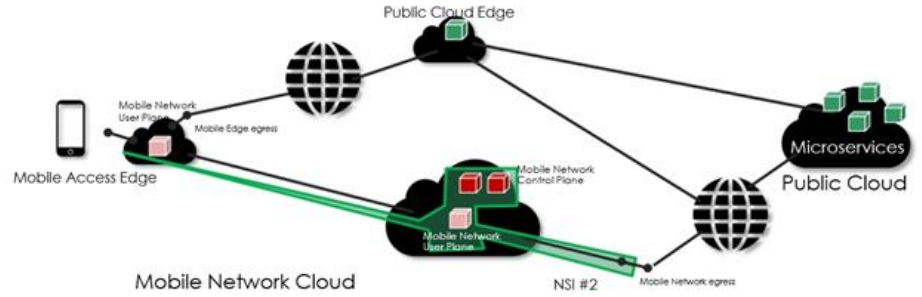
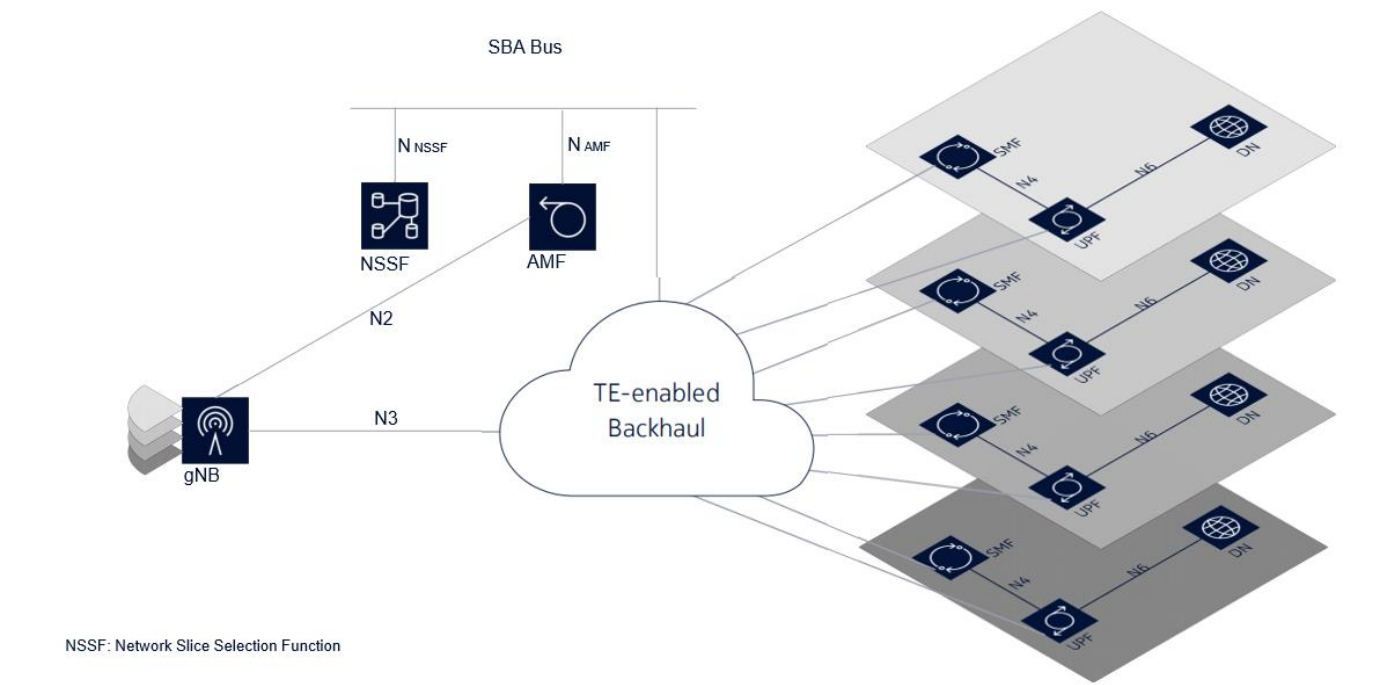



**Figure 56: UPF in the Central Mobile Network Cloud**

# The IP Perspective of Network Slicing for “Network as a Service”




- Slicing a network into virtual containers or virtual elements is not new for IP networks
- A slice is being instantiated all the way from the UE to the Packet Core
- Transport layer is not standardized for NS
- The IP Network will have to deal with a TE problem to achieve isolation between traffic flows
- Mechanisms can be applied like segment routing or MPLS TE in a more centralized manner
- The Key for NaaS is the Cross-Domain orchestration at the RAN and Core Elements in a 5G network

# Need for Slice Isolation

- The are two aspects for the need to enhance the network slice isolation
  - **Slice Security**:
    - In case of a cyberattack or a fault occurrence, only the target slice will be affected
  - **Slice Privacy**:
    - The private information related to each slice its state and its traffic are not shared among the slices

# Operation and Service Assurance Perspective for Success of Network Slicing

- The demanding needs of the architecture of 5G for the additional emerging Services overstretches the network
- The potential to deploy several network slices to serve diverse facilities is an emerging requirement for service providers deploying 5G networks
  - A mechanism and method of registering a UE with a network service or a network slice or more than one has been inherited to address the shortcomings of 4G
- This whole set of knew services requires different mechanisms in terms of management and operation procedures and different treatment from the Customer perspective
  - Life Cycle of creating these services has to be reduced
  - An SDN Controller should optimize and manage the network behavior for every service
  - Virtualization enables pieces of software that can be chained together to provide the service
  - RAN architecture has to be simplified
    - Cloud Based RAN requires one type of skill where every customer needs only one type of skill to maintain it
  - Mobile Edge Computing is going to enable a lot of services that require massive processing

# Network Slicing Architecture Considerations

- NS can be considered as the function associated with a network that supports a specific service and is optimized to this specific service based on the SLA with the customer.
  - Certain policies are associated with this network
  - The horizontal aspect of the slice is being continuously broadened
  - The network is not being optimized just for the service but also operationally for that service with the inherited mechanisms for SDN and NFV

# Infrastructure Testing Considerations

A network slice is created virtually in the cloud and the components can be from different vendors and the requirements can be different, and the scalability also can be different

Quality Assurance department needs to test the infrastructure in the cloud in the exact behavior and the exact situation that it would be used

# Complexity Demands Scaling in the Network Maintenance

The scaling of the complexity as the number of devices increases leads to the increase of the maintenance procedures along with the number of slices

- Edge data centers need to be increased
- A demanding need of an orchestration in the network is being emerged
- Upon Slice Instantiation the whole network and its users must be adopt base on the type of service
- Spun Up VMs must be configured with embedded configuration, should be integrated to FCAP, should be logging and should be protected in a dynamic and agnostic way.

# Network Maintenance Aspects

The existence of many slices instantiated in End-to-End isolated environments has to be done carefully as it may harden the network infrastructure

- An emerging need came out for continuous validation of the configuration files in transport layer devises and in Packet Core
- Access between Operator's networks has to be managed in order to be able to be revoked on demand
- FCAPS in production must be broaden ensuring the overall Quality of Experience
- Logging must be existing in a centralized manner for E2E troubleshooting purposes
- Vulnerability Management Solution should be thoroughly maintained and adopt to new threats

# CONCLUSIONS

- Diverse definitions of network slicing leading to a introduce alignment gaps to a concrete definitions of the mechanism and principles should be adopted.
- Management and Orchestration Plane strategies should be defined in a common approach
- Real-World 5G systems will require additional components to deploy and manage the slices leading to more complex procedures and mechanisms to be inherited

➢ GOAL:

- The success of adaptive network slicing in a continuously broadened deployment will further be enhanced by evaluating the perceived quality of its performance through optimally multi-vendor 5G systems by continuously evolving the testing frameworks, FCAPS and Logging Solutions and overstretching these networks with traffic flows based on many different QCI parameter sets.

# Thank you