



ETSI SUMMIT ON 5G NETWORK INFRASTRUCTURE

Overview: What Needs to be done in the Core Infrastructure Today to Support Tomorrow's 5G Services.

Presented by Sue Rudd, *Director Service Provider Analysis*, Strategy Analytics

April 6th. 2017

© All rights reserved

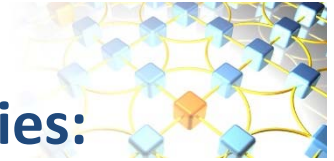
ETSI Summit
5G Network Infrastructure

STRATEGYANALYTICS



Overview: *Setting the Stage for ETSI 5G Infrastructure Summit*

- **5G Moving from Hype to Reality**
 - Diverse Operator Priorities
- **A. Challenges for the development of 5G infrastructure:**
 - Moving Ahead with ‘De Facto’ Standards.
- **B. Beyond Today’s Network Service Management:**
 - Implications of NFV, SDN & Service Orchestration
- **C. 5G Network Protocol Transformation:**
 - Protocols Changes needed
- **D. Designing a Secure and Flexible 5G Core:**
 - Secure
 - ‘Future Proof’
- **Potential 5G ‘Showstoppers’ ...Solutions Need Stds.**



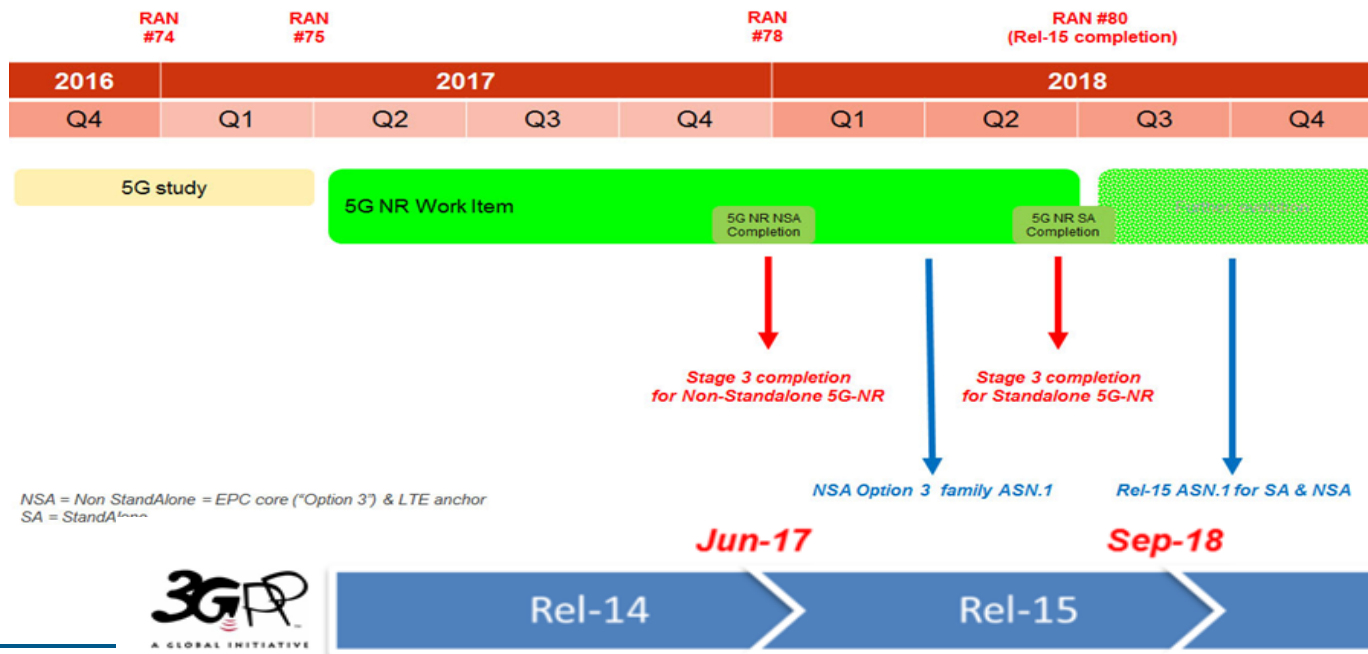
5G Moving from Hype to Reality – Diverse Operator Priorities:

Timeline for 5G New Radio (NR) Accelerated by Asia and US

- 3GPP approved Asian & US Operators' [proposal for accelerating 5G NR progress](#)(Below)

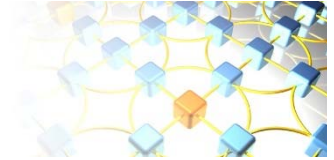
Despite Objections at MWC:

- *Enrique Blanco Telefónica's Global CTO* [noted](#) that “There is a lot of noise about the (5G) radio but we need to make noise about the whole architecture -- for me, much more relevant is the issue of network slicing.”
- Yves Bellego, [Orange](#) Director of Technical Strategy, said that focusing attention on the New Radio (NR) specifications alone would be a risky move
- Deutsche Telekom's *CTO Bruno Jacobfeuerborn* also [commented](#) that "We have to collaborate as an industry to drive the (5G) cost down" in particular to reduce the cost of the dense 5G small cells."



Source: [3GPP](#)





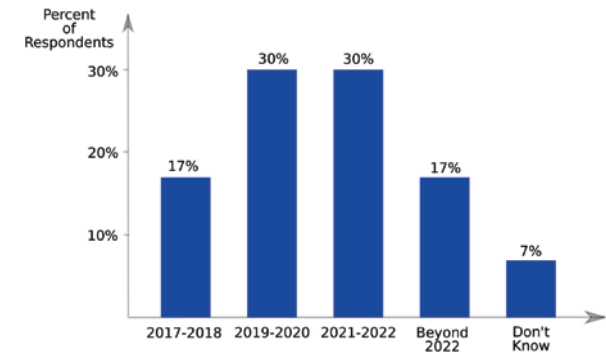
5G Moving from Hype to Reality - Operator Priorities:

TIA [Operator Survey](#) January 2017

TIA Survey Reveals Deployment Hurdles for Operators Before Commercial 5G in 2020

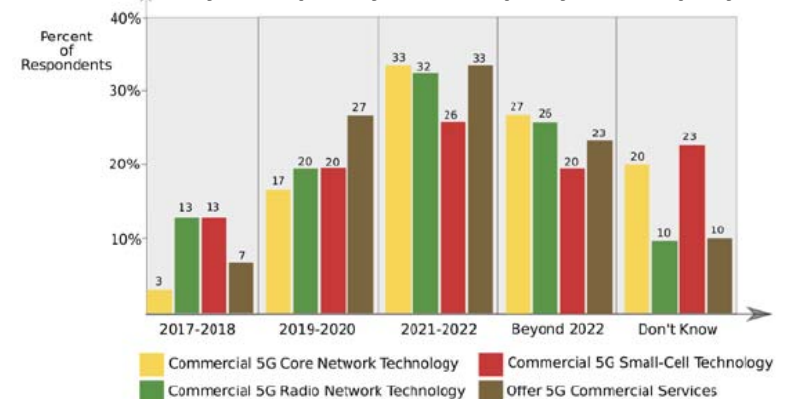
- 26% of operators planning 5G Trials over the next 2 years. - *China, Japan, Australia and US*
- Almost half of Operator respondents expect to spend CAPEX for 5G by the end of 2020. (See Chart on Right)
- Over 66% in favor of Trialing Radio rather than Core Network technology. For the operators trialing Core Network - focus is on deploying NFV/SDN precursors of 5G.
- Fiber Ranked as most important Backhaul and Transport technology for 5G, followed by *mmwave*.
- 90% concerned about Security for 5G:
 - *Autonomous Vehicles;*
 - *Ultra-Reliable and Low Latency Services*
 - *Massive Machine Type Communications.*
- Network Slicing is important for:
 - *Revenue Opportunities.(83.4%)*
 - *Enhanced Service Quality (73.4%)*
 - *Network Efficiencies (70%)*

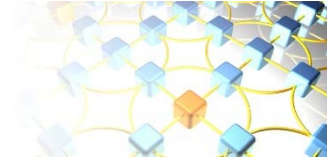
When do you expect to make 5G investments as part of your CAPEX budget?



TIA [Operator Survey](#) January 2017

When do you expect your company will deploy?

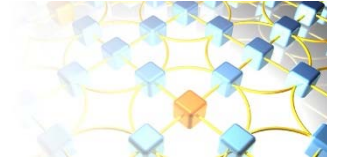




A. Challenges for the development of 5G infrastructure - Moving Ahead with 'De Facto' Standards

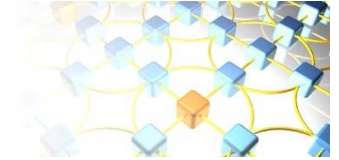
- 5G ready E2E platforms unveiled at MWC - Cloud RAN, C-RAN and vRAN “virtually everywhere”:
 - Ericsson’s 5G [Cloud Core, vRAN and New Radio \(NR\)/LTE Interworking](#)
 - Nokia’s [commercial End-to-End 5G](#)
 - Huawei E2E 5G solution later in 2017
 - ZTE’s full range of [5G pre-commercial base stations](#) for mmWave and sub-6 GHz frequencies
- Digital Transformation & Cloud Focus:
 - Both [Ericsson](#) and Nokia focusing on 5G Transformation/Acceleration Services
 - Huawei focusing on ‘Elastic Cloud-Native’ 5G Services
- 5G ‘Network Slicing’ is here:
 - Huawei, Samsung and [DT demonstrated all cloud based 5G E2E ‘Network Slicing’](#) (RAN, Transport, Core)
 - Ericsson, Deutsche Telekom and SK Telecom successfully demonstrated World's first 5G Transcontinental multi-operator [Federated ‘Network Slicing’](#)

Source: Strategy Analytics [Networks and Service Platforms](#)



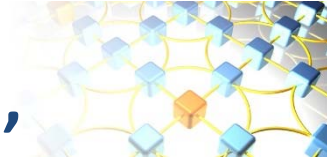
B. Beyond Today's Network Service Management:

- **Implications for:**
 - **NFV - Beyond Legacy Appliance 'Virtualization' & SLA 'Tunnels'**
 - **SDN - Enablers as Source of Revenues – 'On Demand Slices'**
 - **Service Orchestration - *Operators Leveraging Service Orchestration and OSS Systems***
 - **AT&T, Orange and Colt with API standards for SDN Service Orchestration (*see our blog [here](#)*)**
 - **AMDOCS leveraging AT&T ECOMP Systems Integration for [Orange Polska Trial](#)**
 - **[Globe Telecom](#) (Philippines) selects NEC/Netcracker OSS suite and Service Orchestration solution for Agile Virtualization**
 - **[Verizon Enterprise picks Ericsson](#) orchestration platform for enterprise managed services**
 - **[Nokia integrates Service Assurance and Service Orchestration](#) with acquisition of Comptel**



C. 5G Network Protocol Transformation:

- **Next Gen. and 5G Networks demand Protocols that:**
 - **Simplify the Exponentially Increasing Complexity of 5G from RAN to Core ‘New Protocol for every Class of App.’ – IoT, MTC. Connected Cars...etc**
 - **Address TCP issues identified in two NGP Reports:**
 - May 2016 ‘[Next Generation Protocols – Market Drivers and Key Scenarios](#)’:
 - “TCP/IP protocol suite doesn’t identify where security functions such as authentication, access control, integrity, confidentiality, or auditing should belong”
 - “Internet addressing architecture lacks naming of content, in particular the lack of application names makes the Internet more vulnerable”
 - “TCP/IP based Internet does not define ‘scope’”
 - October 2016 ‘[Next Generation Protocols; Scenarios Definitions](#)’:
 - Handshake
 - Slow start
 - TCP congestion control mechanism
 - Mismatch among buffer management
 - **Unified Network Architecture which:**
 - **Simplifies Replicable Functionality at every Layer**
 - **Isolates true layers so that Network Slice performance and QoS SLAs are guaranteed *without tunnels* that obviate many of Efficiencies of Virtualization**
 - **Optimizes Virtual Network Function (VNF) Reuse**
 - **Isolates Applications Flows from one another**
 - **Makes Inherent Security the Default**



D. Designing a Secure 5G Core – ‘Inherent Security’

- In 2016 DDoS attacks on Network Infrastructure exceeded those on Web Servers

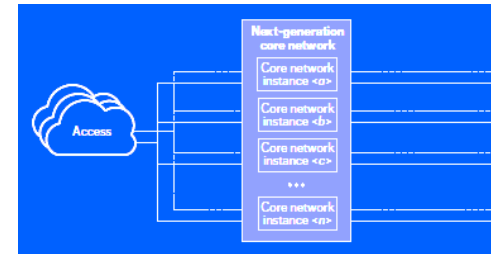
<p>5G Security Threats demand Shift away from ‘Assuming Trust’ to ‘Positive Validation’</p>	<ul style="list-style-type: none"> ▪ Massive <i>DDoS Attacks on Network Infrastructure</i> ▪ Network Slices/Service Logic Chains and Hypervisor etc. <i>Vulnerable e.g. to ‘Phantom Attacks’</i> ▪ Large Scale <i>Fraudulent User Service Access</i> 	<ul style="list-style-type: none"> ▪ Separation of ‘IDs’ or Names from Network Addresses ‘No user App. should ever see a Network Address’ ▪ Inherent Security w. Service Layer Isolation that Isolates Network from Users and Users from one another ▪ Authentication to Service Layer based on combined User/App./Device/ID.
---	---	--

- Ensure security through:
 - **Integrity** including authorization and authentication of sender and receiver
 - **Confidentiality** information is not accessible - or even visible - for unauthorized elements
 - **Isolation** delivers inherent low cost security with ‘Reusable Containers’



D. Designing Flexible 5G Core: *HPE Compute Fabric & Ericsson Cloud*

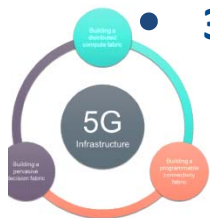
Ericsson: 'Slicing Next-Gen. Core Network



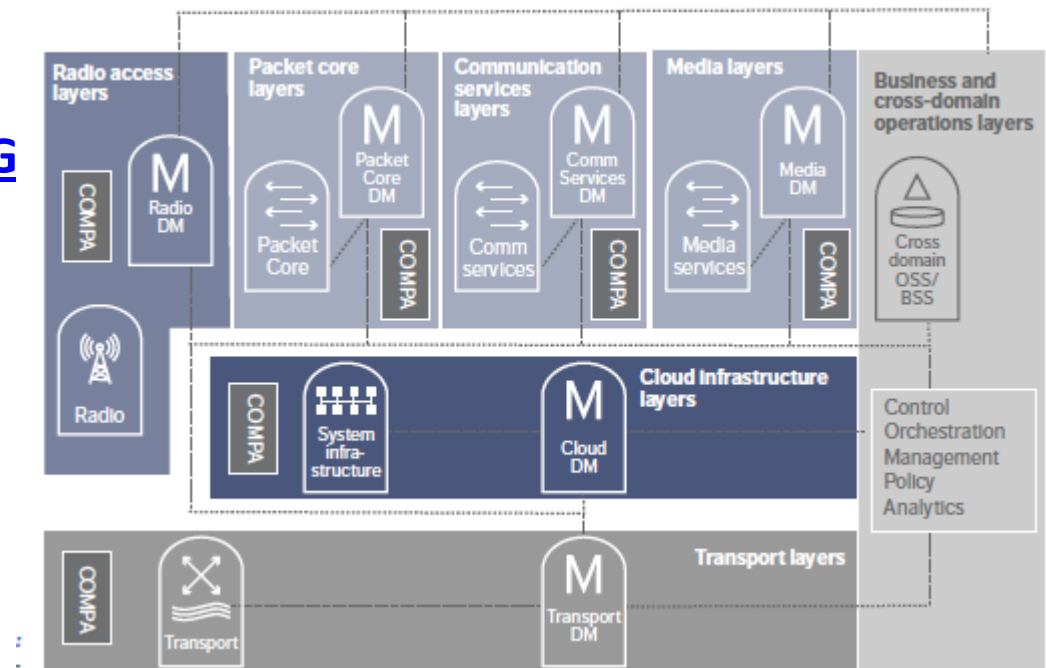
- **'Future Proof' Flexibility:**
 - Software Defined Infrastructure (SDI)
 - Virtualized Core: vEPC, vIMS, vTAS..
 - Cloud Based Infrastructure: Ericsson, Huawei, Nokia

HPE 'Laying the Foundations for 5G Infrastructure'

- **Distributed Computing Fabric**
 - 1. Distributed Compute Fabric
 - 2. Programmable Connectivity Fabric
 - 3. Pervasive Decision Fabric



Ericsson : Service Processing over Cloud Infrastructure



Source: [Ericsson Technology Review on 'A Vision of the 5G Core' 2016](#)



Potential 5G ‘Showstoppers’ Demand New Solutions/Std

Reference: [Multi-billion dollar market opportunities may be lost unless Next Generation Broadband meets Seven Key Challenges](#)

Potential ‘Showstopper’	Potential Issues	Possible 5G Solutions that Require Standards
5G Access faster than Fixed Network	<ul style="list-style-type: none"> Access no longer the Broadband Bottleneck - Fixed IP Network may be the ‘Choke Point’ 	<ul style="list-style-type: none"> Multi-Access Edge Computing (MEC) w. Processing in 5G Infrastructure Load Management at the Edge/PGW
5G Small Cells, Multi-Frequency HetNets Interact Dynamically w. Devices/ Apps.	<ul style="list-style-type: none"> Small cells require smooth fast ‘Soft Handover’ and dynamic SON based power control Smart User Applications can Request ‘Class of Service’ 	<ul style="list-style-type: none"> Multi-Homing of Devices Intelligent Channel Selection across Multi-frequency HetNet
IoT Scale lacks Security Mechanisms	<ul style="list-style-type: none"> IoT entities exhaust Address Space ‘Dumb’ IoT entities create Security problems 	<ul style="list-style-type: none"> Network Independent Personal or Unique Digital Identifiers (eSIM ‘like’)
Security Threats demand Shift away from Assuming Trust to Positive Validation	<ul style="list-style-type: none"> Massive DDoS Attacks on Network Infrastructure Network Slices/Service Logic Chains and Hypervisor etc. Vulnerable e.g. to ‘Phantom Attacks’ Large Scale Fraudulent User Service Access 	<ul style="list-style-type: none"> Separation of ‘IDs’ or Names from Network Addresses ‘No user App. should ever see a Network Address’ Inherent Security w. Service Layer Isolation that Isolates Network from Users and Users from one another Authentication to Service Layer based on combined User/App./Device/ID.
‘Nailed Up’ 5G Net-work Slices Impede NFV Resource Allocation	<ul style="list-style-type: none"> Network Slices conflict with NFV resource allocation - only guarantee QoS if ‘nailed up’ w. Tunnels and VPNs 	<ul style="list-style-type: none"> True Service Layers: End-to-End or with Variable Network Scope - Not ‘Stacked Silos’. All resources/PNFs available to all VNFs
Gigabit Traffic Bursts can Collapse TCP based networks	<ul style="list-style-type: none"> Lack of Flow Control - Bursty Video and P2P Live Streaming could Crash Network 	<ul style="list-style-type: none"> Pro-Active Congestion Avoidance/Policy Based Load Management
Data Centers do not Scale Globally w. Telco Cloud	<ul style="list-style-type: none"> Network Scales but Data Center Islands hit limit - e.g. Exceed VXLAN 1 Million address limit 	<ul style="list-style-type: none"> Global Multi-Protocol Layer 2 Interworking for Software Defined Data Centers (SDDCs)



Contact Information

Sue Rudd

Director Service Provider Analysis

Strategy Analytics

email: srudd@strategyanalytics.com