Mitigating the Operation and Maintenance Challenges of the Next Generation Mobile Networks

Table of contents

1. Executive Summary

This white paper focuses on operation and maintenance (O&M) of the next generation mobile networks (typically referred to as 5G), the challenges operators are facing, and potential ways to manage these.

The next generation mobile networks will introduce many new network architectures and functionalities, which means that the complexity of the network will increase significantly. So the main goal regarding O&M for the next generation mobile networks will be to hide this complexity from the operator. The main ways are to automate the O&M as much as possible, e.g. through automatic orchestration of virtual network functions, and to go from management of network elements to management of E2E (end-to-end) services.

The future mobile networks and corresponding O&M will also be much about reducing cost and finding new sources of revenues, especially since the traditional income from phone calls and messaging is declining rapidly, while at the same time requirements on network build-out is increasing. This can e.g. be remedied by different sharing models and offering the network as a platform for 3rd party services.

2. Current Situation

People are getting more and more dependent on mobile devices and the internet. The following network dependent trends can be seen:

- Social networks heavily used (Facebook, Instagram, Twitter, WhatsApp, etc.).
- Over-the-Top (OTT) content services (Spotify, Netflix, YouTube, etc.) replacing physical media (discs) and broadcast.
- OTT voice and messaging services (Skype, Messenger, etc.) replacing corresponding network services.
- News via the web replacing newspapers.
- Cloud computing and storage reachable everywhere replacing local applications and storage (Google™ apps, Office 365, Adobe Creative Cloud™, etc.).
- IoT (connected cars, wearables, smart homes, industrial applications, etc.) is hot but is fragmented with a lot of proprietary solutions.
- Virtual/augmented reality, possibly with haptic (force feedback) techniques, is also a much-hyped technology that is being shown everywhere.
- UHD (4K) giving even higher resolution than full HD is supported by a lot of equipment, but content is lacking.
- Payments via mobile phones replacing cash payments.

Note that most of the above works with both mobile and fixed (cable connected) user equipment.

All this results in rapidly increasing network traffic, calling for big network investments. However, from the traditional network operator's point of view, the traffic mainly consists of so called bit-piping, that is, the operators are not directly involved in the delivery of the services. At the same time revenues from traditional network services, such as voice calls and messaging, are rapidly declining. Because of the subscription models for bit-piping, the operators typically do not get paid in relation to the traffic increase, making network investments less profitable.

This makes the operators look for new revenue streams, but also for reducing the total cost of ownership (TCO).

The coming sections will, in light of the next generation mobile networks, show how O&M is affected by the new requirements and architectures, what challenges the operators will face, and how these challenges could be managed.

3. Implications on O&M from Next Generation Mobile Networks

3.1 Requirements

Next generation mobile networks (5G) will provide many new features and capabilities. 5G is not only about providing a new air interface, but to large extent also about providing a platform supporting a variety of network based use cases. The requirements on capabilities in terms of data rates, latencies, coverage and number/density of devices/users will be tough to meet, not only from the equipment vendor's point of view, but also from the operator's point of view. For instance, the requirements on geographical coverage and user/device density will require heavy investments in network build-out. But 5G will also offer new ways of reducing the energy consumption (e.g. by co-locating control functionality), reducing the cost of equipment (e.g. by using commodity hardware), and making use of the equipment more efficiently (e.g. by scaling to match needs and sharing resources among network operators).

The NGMN Alliance's 5G white paper[1)] is a main source for 5G requirements. Since NGMN mainly represents the operator's view on the next generation mobile networks, they focus not only on supporting new use cases, but also on finding new business models and new value creation opportunities.

3.2 Design Principles

Regarding O&M, the NGMN Alliance wants a 5G network to follow the following design principles:

- Expanded network capabilities and flexible function allocation should not imply increased complexity on operations and management (on the contrary, O&M should be simplified).
- Procedures should be automated as far as possible, with well-defined open interfaces to mitigate multi-vendor interworking problems as well as interoperability (roaming) issues.
- Use of dedicated monitoring tools should be avoided and network functions (software) should be embedded with monitoring capabilities.
- Big data analysis should drive network management from reactive to a predictive and proactive mode of operation.
- Carrier-grade network cloud orchestration is needed to ensure network availability and reliability.

3.3 Architectures

3.3.1 General

In order to meet the requirements and follow the design principles, various architectural solutions will be used, including:

- Network Functions Virtualization (NFV)
- Software Defined Networks (SDN)
- Cloud RAN (C-RAN)
- Mobile Edge Computing (MEC)
- Internet-of-Things (IoT) infrastructure
- Network slicing
- Network sharing

All of these will have impact on O&M of the network. The architectures and their impacts on O&M are further elaborated below. Note that most of these can be applied to current mobile network generations as well, and be part of the evolution towards 5G.

3.3.2 Network Functions Virtualization (NFV)

NFV allows network functions to be virtualized in a cloud environment, that is, they will run as applications on virtualisation containers (such as virtual machines (VMs)) on servers in data centres. The main benefits are greater flexibility allowing faster service deployments, and possibility to scale used resources according to current needs. The hope is also that the equipment cost is reduced by using Commercial-Off-The-Shelf (COTS) hardware. The NFV architecture is being defined by ETSI[2].

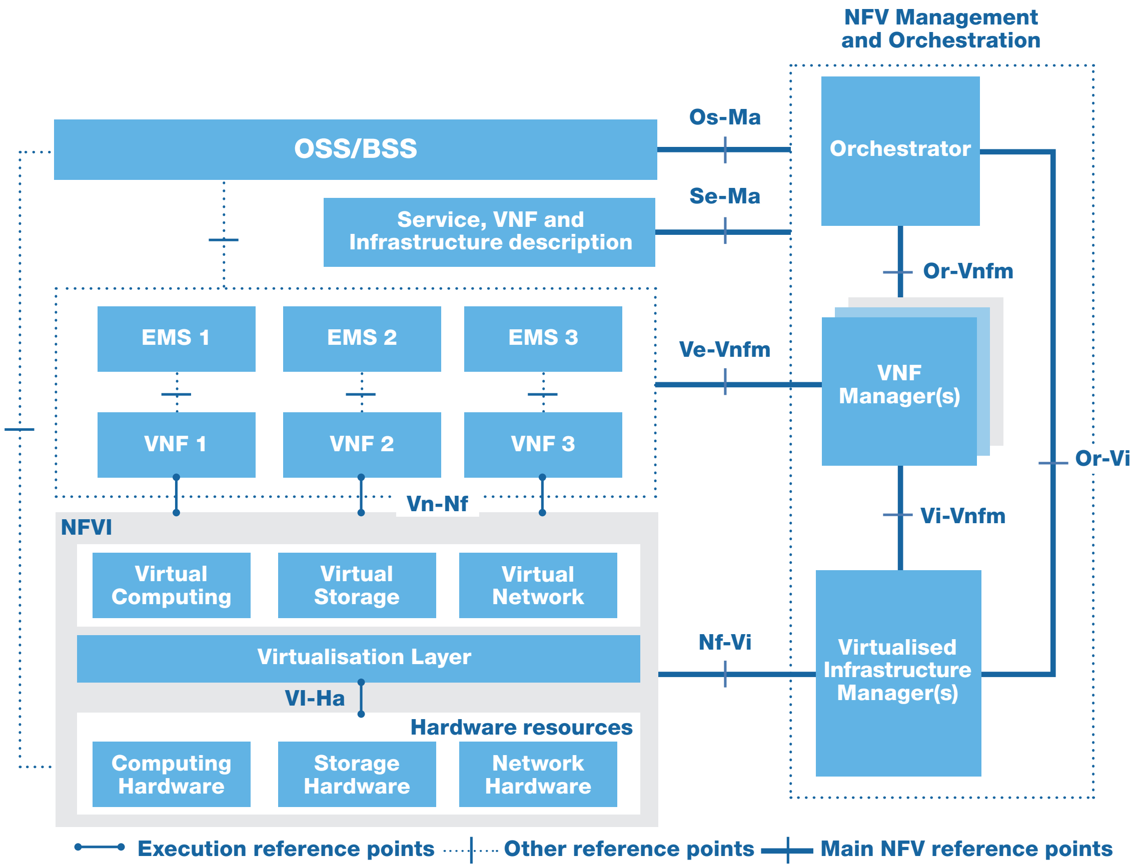

Figure: The ETSI NFV architecture

From an O&M point of view the main part of the NFV architecture is the NFV Management and Orchestration (NFV-MANO) domain which is divided into the functional blocks NFV Orchestrator (NFVO), Virtual Network Function (VNF) Managers (VNFMs), and Virtual Infrastructure Managers (VIMs). These are responsible for VNF deployment and scaling, and infrastructure configuration and management. The application specific part of O&M for a VNF is handled by a corresponding EMS functional block. OSS will interface NFVO and different EMSs in order to deploy and configure network services, collect performance data and receive alarms.

Compared with current network elements, NFV adds a new level of O&M concern, namely the NFV Infrastructure (NFVI) which is managed separately from the network functions, possibly by another operator than the VNF operator(s). The hardware is owned by the infrastructure, so any physical repair activities are the responsibility of the infrastructure operator.

Scaling of VNFs can be done in two dimensions, vertical and horizontal. Vertical (or up/down) scaling is about increasing/decreasing the computing/storage/network resources allocated to a VNF component running on a VM. Horizontal (or out/in) scaling is about adding/removing instances of a VNF component, each running on a different VM. Vertical scaling is faster, but typically limited to what extent the scaling can be done. Horizontal scaling is virtually without limitations, but is slower. Horizontal scaling could also be done to spread the application to different locations.

3.3.3 Software Defined Networks (SDN)

SDN decouples network control from data forwarding functions. It was originally intended for IT switches/routers where forwarding rules (based on incoming packet headers) in flow tables could be updated from an SDN controller via the OpenFlow protocol. This concept has been extended with an application layer on top of the control layer, where applications can access services in the control layer via well-defined APIs. Other protocols than OpenFlow is also being used between the controller and the switches.

5G has adopted this architecture as a way to control telecom transport networks in a flexible way. SDN is often mentioned together with NFV, but SDN is not dependent on NFV, or vice-versa, but SDN could be a way to setup transport paths between network functions in a dynamic way. Different entities in the SDN architecture could also be virtualized or be part of the NFVI or NFV-MANO. ETSI has made a report on how SDN could be used in the NFV architecture[5]. It shows a wide variety in SDN component deployments/usage. SDN is being defined by ONF[4].

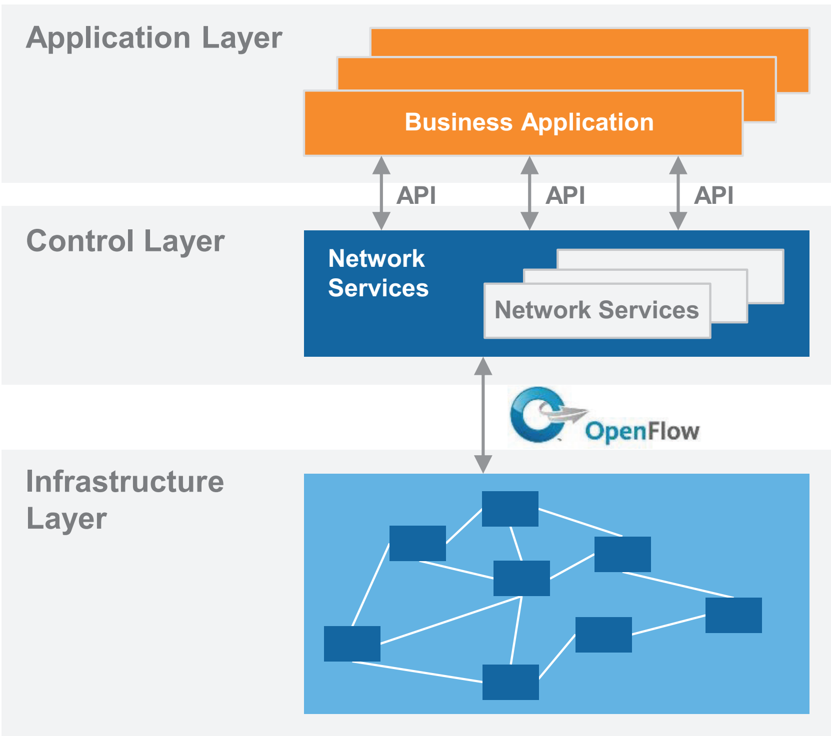

Figure: The SDN architecture

From an O&M point of view, SDN could be used as part of the configuration of a network service, e.g. to setup IP tunnels between data centres. SDN can also be used to monitor the traffic through the controlled switches. This can e.g. be done using the statistical counters defined in the OpenFlow protocol specification[6].

3.3.4 Cloud RAN (C-RAN)

C-RAN is often referred to as Cloud Radio Access Network, but the C may also refer to Clean, Centralized and Collaborative. The basic idea is to split a radio base station into a baseband processing unit and a number of remote radio heads interconnected by means of a standardized optical interface, such as CPRI. This in itself is nothing new. The new thing is that the baseband processing unit can be seen as a shared resource. Parts of the radio stack can also run as VNFs enabling scaling on commodity hardware. The main benefit with this is the ability to scale the baseband processing part according to current needs without having to install new dedicated hardware. Installing new dedicated baseband hardware to meet needs is complex and time consuming, and basically only offers a way to scale up (after installation, downscaling is not feasible). By co-locating the baseband processing, the need for housing and power/climate is reduced. The co-location also facilitates certain carrier aggregation and interference mitigation functionalities. Note that the exact boarder between the radio and baseband functionality is being discussed, mainly due to the stringent requirements on bandwidth and delay/jitter imposed by CPRI. These will be hard to meet in a virtualized environment, especially if Ethernet is used as transport media and new antenna technologies (such as massive MIMO) are taken into account.

From an O&M point of view, a benefit with this architecture is that if the O&M interface is provided by the virtual baseband processing unit, the scope of the base station can easily be extended, thus reducing the number of needed O&M interfaces compared with many physical base stations with their own O&M interfaces.

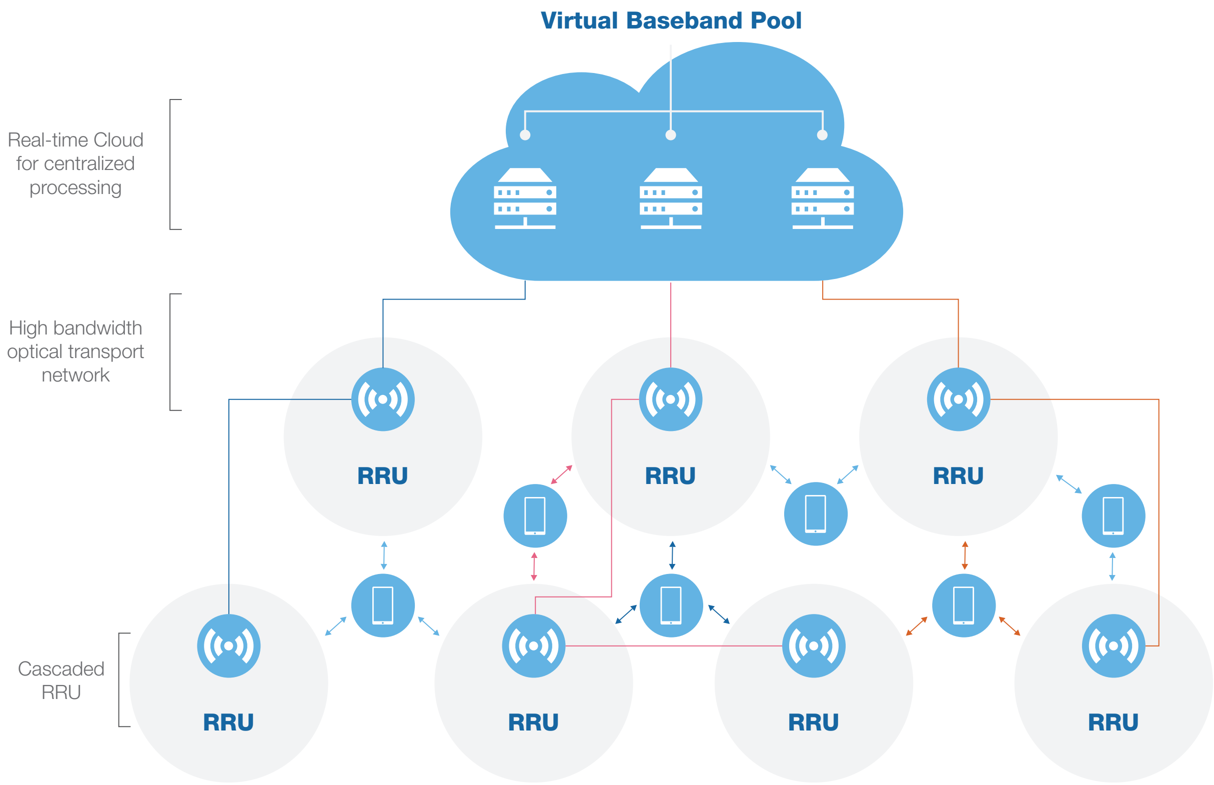

Figure: The C-RAN architecture

3.3.5 Mobile Edge Computing (MEC)

MEC is a platform for deploying applications close to the mobile network edges, that is, within the RAN in close proximity to mobile subscribers. The main benefits are reduction of latencies and offloading of the transport network. It is built on the NFV architecture, where the applications can be viewed as virtual network functions. Examples of applications are IoT servers and video caching. When used for video caching, it can be seen as part of a Content Delivery Network (CDN). MEC is being defined by ETSI[3].

This can be marketed as an Infrastructure-as-a-Service (IaaS). Through this the operator owning the MEC platform can offer the platform to 3rd party service providers, such as video service providers.

MEC is often mentioned in conjunction with fog computing. Both are about pushing intelligence and processing capabilities down closer to where the data originates or is destined. Fog computing can be seen as an intermediate layer between a cloud computing layer and the target devices. So MEC could be one way of implementing fog computing. Fog computing is being defined by the OpenFog Consortium[14].

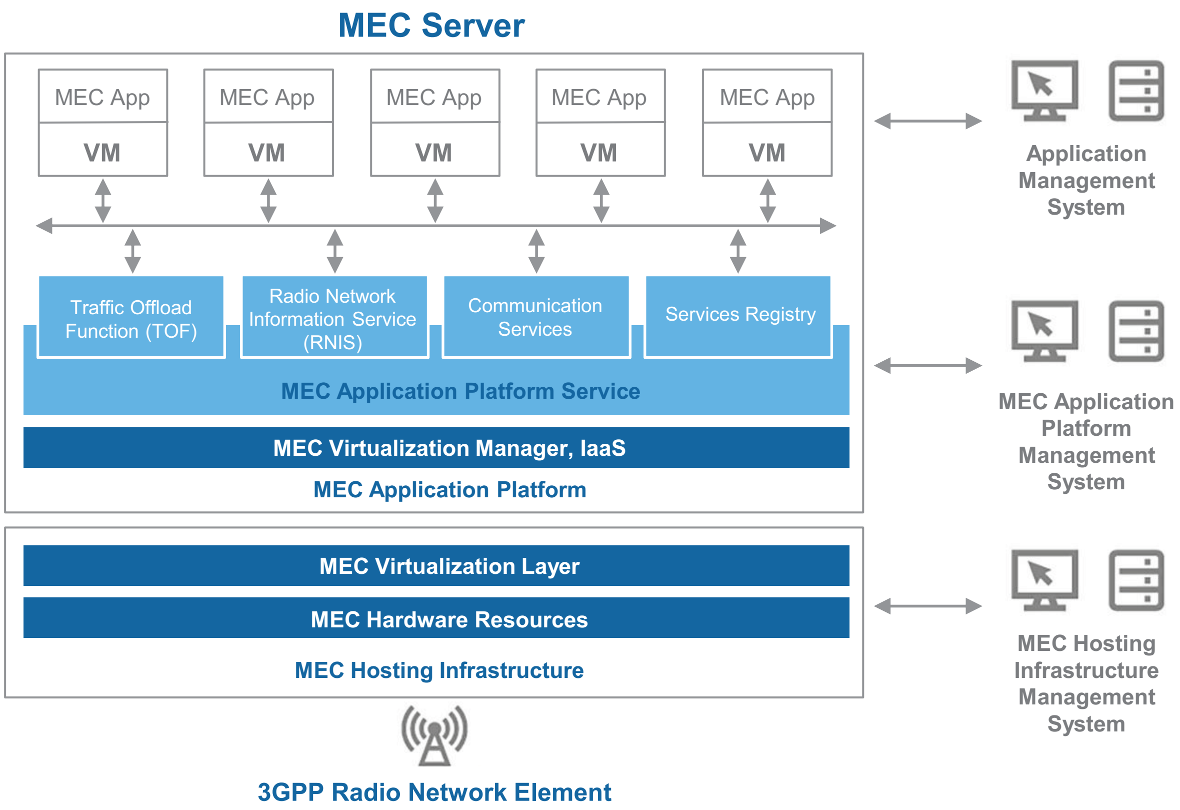

Figure: The MEC architecture

This figure also illustrates where O&M for MEC comes in. MEC Hosting Infrastructure Management is similar to NFV-MANO in the NFV architecture. MEC Application Platform Management covers the MEC platform unique management. And finally, Application Management is about the management of the actual MEC applications, which is application specific and used by the 3rd party service providers.

3.3.6 Internet-of-Things (IoT) Infrastructure

IoT can be divided into massive Machine Type Communication (mMTC) and mission-critical MTC (cMTC). mMTC has focus on massive number of devices, low energy consumption, but low data rates. cMTC has focus on availability, reliability and low latencies. cMTC is sometimes referred to as Ultra-Reliable Low Latency Communications (URLLC).

An IoT infrastructure may include capillary networks. Capillary networks is a way to solve the problem of communicating with a lot of devices, which means that it mainly is applicable to mMTC. In capillary networks, devices are connected to gateways using short-range radio technologies, such as IEEE 802.15.4[10]. The gateways use 3GPP radio links for backhaul between the gateway and the mobile network. Short-range networks enable off-loading the mobile network and aggregating the total number of devices into less numbers, thus making their management easier. In addition, the use of short-range links, compared to long-range links, enables reduction of the transmission power, thus improving energy efficiency and reducing interference. IoT gateways may also be connected directly to the Internet through an Ethernet backhaul.

IoT devices can also communicate directly with the mobile network, without any gateway. For this purpose 3GPP has introduced more lightweight radio interfaces for LTE, namely CAT-0, CAT-M1 and NarrowBand IoT (NB-IoT).

Technologies where IoT devices can communicate directly with wide area base stations in an energy efficient way are often referred to as Low Power Wide Area (LPWA) technologies. So the above mentioned 3GPP interfaces are LPWA technologies[8].

The Constrained Application Protocol (CoAP)[11] and IPv6 over Low power Wireless Personal Area Networks (6LoWPAN)[12] are other lightweight protocols introduced to support IoT.

From an O&M point of view, the gateways need to be configured and incorporated as mobile devices into the mobile network. The gateways and corresponding devices will then communicate with an IoT server application, transparently through the mobile network. Techniques to manage IoT devices include the OMA Light weight M2M protocol (LWM2M)[7].

Special focus must put on security aspects, when a lot of devices are connected to the internet. Such devices may have less protection against unauthorized access, and may be updated with latest software (with security bug fixes) less frequently. This could result in the devices being used e.g. for overload attacks, spy purposes, or purposely inflicting damage. When mission critical devices are connected to the network, such as cars, surgical equipment and industrial robots are hijacked, this may be a threat to human safety. One organization working on these issues is the IoT Security Foundation[18].

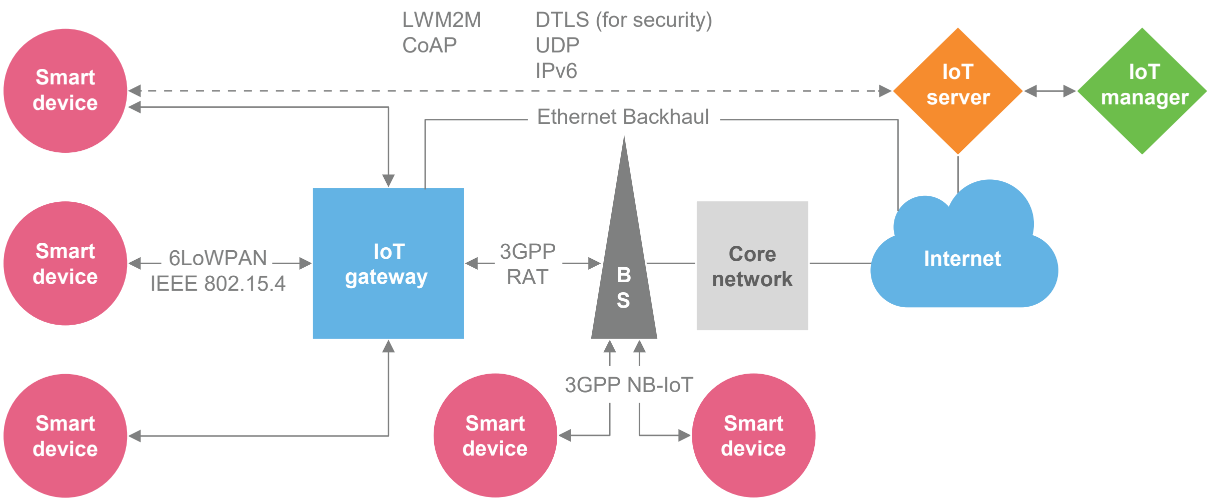

Figure: Example of an IoT infrastructure

3.3.7 Network Slicing

One of the major new architectural concepts in the next generation mobile network is the division of a network into so called network slices. It makes logical divisions of a network depending on the characteristics of different traffic types. It is a way to make one physical network serve different, sometimes conflicting, needs. For instance, mobile broadband has focus on high data rates, mobility and coverage, mMTC has focus on huge number of devices but low data rates, and cMTC has focus on low latency, availability and reliability.

Network slicing can be implemented by having dedicated virtual network functions for the different network slices.

In order to meet the characteristics requirements, the location of the network functions is also of importance. For instance, a mission-critical MTC server needs to be located close to the end user devices in order to reduce the latency, and a video caching server needs to be located close to the end user devices in order to offload the transport network.

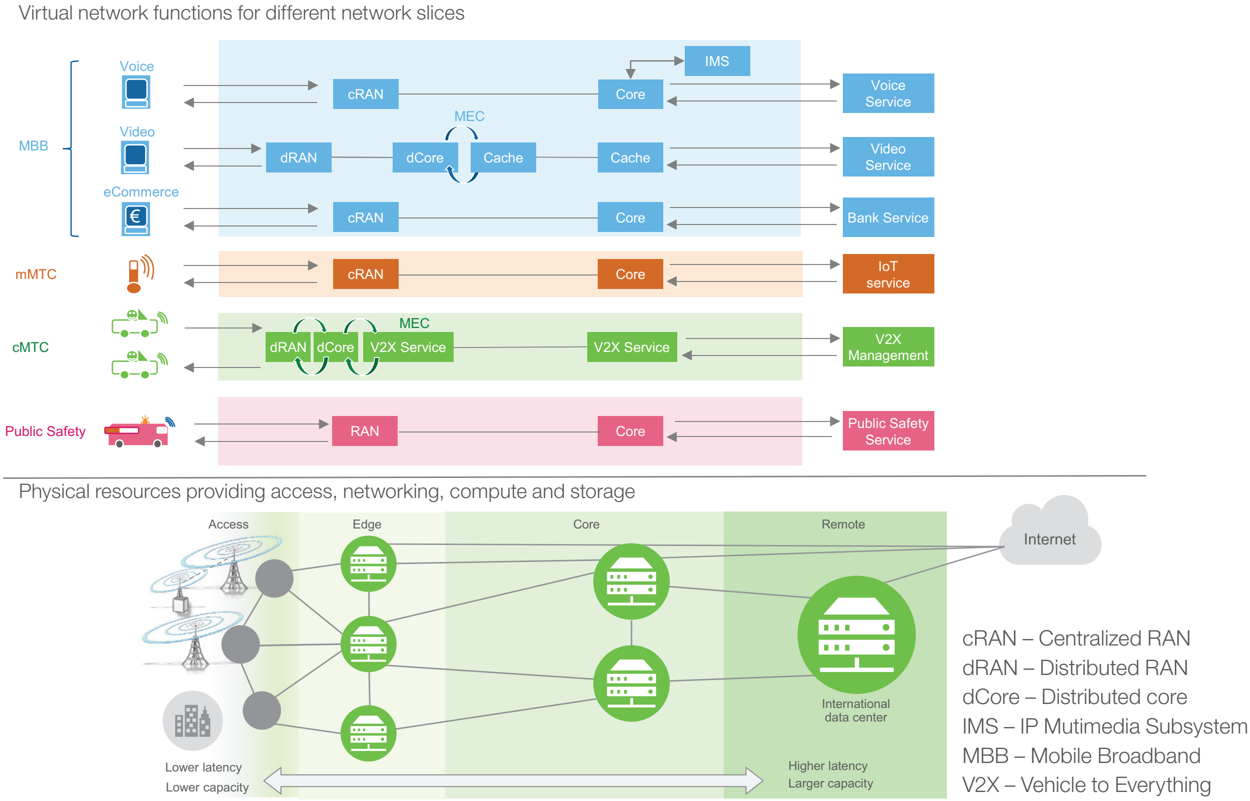

Figure: Examples of some network slices

The figure shows two MEC applications, one for video caching and one for a Vehicle-to-Everything (V2X) service.

The figure also shows an example of a distributed core. Core functionalities can be distributed closer to the RAN in order to reduce latencies.

A network slice for public safety communications is also illustrated. There are standardisations efforts in 3GPP to provide public safety communication as part of LTE[9], thus providing an alternative to dedicated public safety communications network standards, such as TETRA. The extra features include proximity services enabling device-to-device (D2D) communication, coverage extension through device to network relay, and group calling services enabling one-to-many communication. The characteristics of a public safety communications network has focus on availability, reliability and coverage.

O&M for network slices includes deployment and orchestration of the network functions, but also network slice unique (context-aware) monitoring and optimization ensuring that the required characteristics are met.

3.3.8 Network Sharing

Network sharing is a way of utilizing a network more efficiently. There are basically four levels/ways of sharing a network:

- Passive sharing of site equipment, such as buildings, masts, power and climate.
- Active RAN sharing, including sharing of radio access and core network functions.
- Roaming-based sharing.
- Mobile Virtual Network Operator, i.e. just a buy-in of network services from a mobile network operator, which independently are sold to end customers.

All these sharing models enable more efficient usage of the network equipment. Each operator do not have to build a completely separate network to get the desired coverage and capacity. These sharing models are already used, but 5G accentuates the need for sharing to reduce costs while still fulfilling the required capabilities. 5G will also add another kind of sharing, namely sharing of cloud infrastructures.

4. Challenges and Their Mitigation at NGMN Deployment

4.1 Challenges

The main challenges operators currently are faced with can be summarized as:

- Heavy network investments to meet bit-piping capacity demand.
- Declining voice and messaging revenues.
- New services take long time to implement in the network.
- O&M is complex and time consuming.

The next generation mobile network will, unless mitigated, result in additional challenges, such as:

- Heavy investments to meet the requirements for the next generation mobile network.
- All new architectures used resulting in a more complex network.
- More stakeholders involved (primary network operator, network sharing operators, cloud infrastructure operators, 3rd party service providers, equipment and SW vendors, open source SW communities, etc.).
- The elasticity and flexibility resulting in new optimization decisions.

4.2 Potential Solutions

4.2.1 General Solutions

The major ways of coping with the challenges are the following:

- Finding new sources of revenues.
- Reducing TCO.

This is of course easier said than done. But they can be broken down into the following potential solutions. Regarding finding new sources of revenues, this may include:

- Offering the network as a service platform, e.g. via MEC marketed as an IaaS.
- Introducing other subscription models, where the amount of data is paid for (today fixed rate subscription models are common).
- Sharing network investment and operating costs with other operators and 3rd party service providers.
- Getting new services faster in operation so that they can start generating revenues.

Reducing TCO may include:

- Providing end-to-end (E2E) service management.
- Increasing the level of automation in the O&M of the network.
- Using the equipment more efficiently by allocating resources according to when and where they are needed.
- Reducing energy consumption, e.g. by centralizing processing units.
- Running some network functions on COTS hardware.

4.2.2 Some Specific O&M Solutions

4.2.2.1 General

There are a number of ways to mitigate operator's challenges in the O&M area. The following potential solutions will be examined deeper:

- E2E service management
- Self-Organizing Networks (SON)
- Active monitoring including virtual probes
- Big data analytics including machine learning and context awareness

4.2.2.2 E2E Service Management

E2E service management is about deploying and managing a service through the lifetime of the service from the end user's point of view. E2E service management is also about hiding the complexity of the underlying network providing the service, maybe involving different operator networks and technologies. It is also a major shift from managing network elements to managing E2E services. There are many efforts along these lines. One example is Life-cycle Service Orchestration (LSO). LSO is being defined by the Metro Ethernet Forum (MEF)[15].

The idea behind LSO is that the end customer, via a web interface, orders a certain communication service. This is then effectuated by the LSO functionalities by interfacing different network functions through standardized interfaces. LSO also makes sure that the service fulfils the required characteristics as defined in a Service Level Specification (SLS), during the life-time of the service. LSO can be divided into the following sub-functions (with some example functionalities within parenthesis to understand the basic scope of the sub-functions):

- **Fulfilment** (provisioning and initial verification of the service based on a service order)
- **Control** (allows subscribers to actively control the elastic behaviour of their service instances)
- **Performance** (performance monitoring and SLS conformance verification)
- **Assurance** (fault management, but also handling of subscriber complaints)
- **Usage** (recording of service usage)
- **Analytics** (for predictions and anomaly detection)
- **Security** (ensuring that the service and it's data is protected against different attacks)
- **Policy** (set of rules under which the LSO management and control logic must operate)

LSO-Lifecycle Service Orchestration

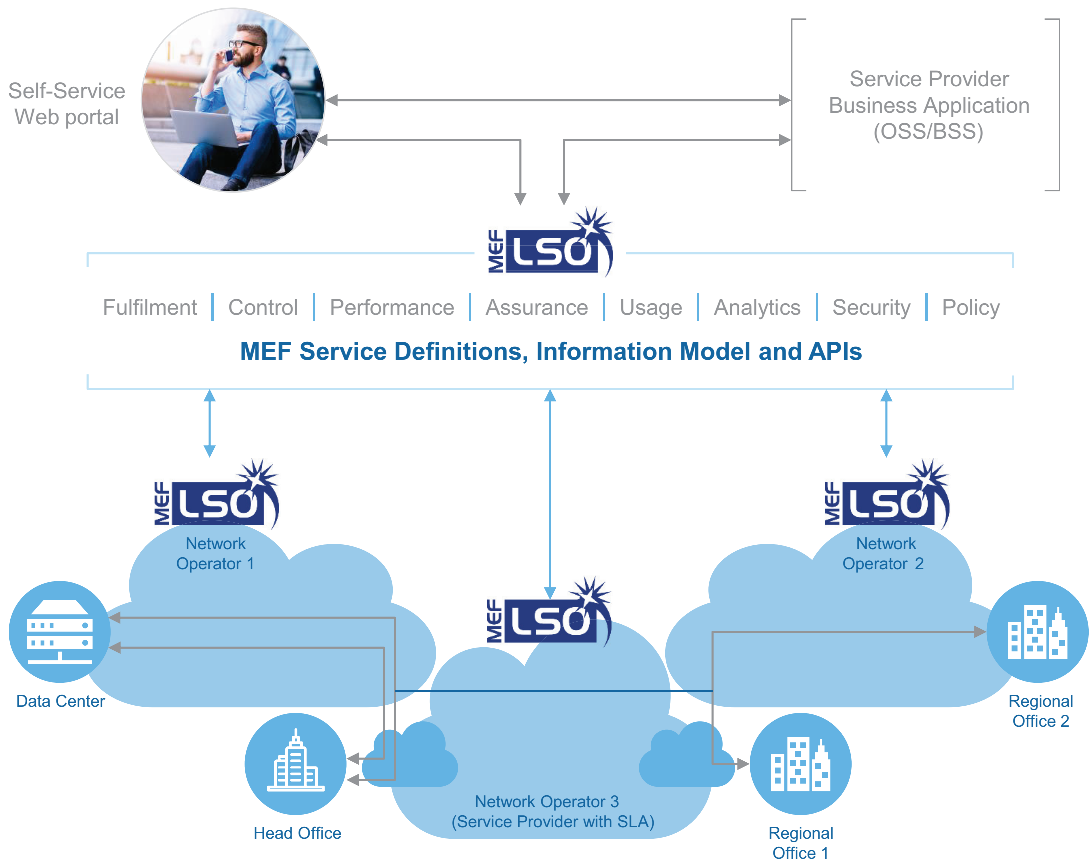

Figure: LSO

ETSI and MEF have initiated a collaboration to advance NFV for Carrier Ethernet 2.0 services enabled by LSO[17].

Another example of E2E service management is the Open Network Automation Platform (ONAP)[21].

For the next generation mobile network based on NFV/SDN; E2E service management could be used for management of network slices, such as a slice for a video service, a slice for an IoT service, or a slice for a public safety communication service. E2E service management would then as part of the fulfilment phase, to deploy instances of corresponding virtual network functions in the appropriate places in the network, and setup needed transport paths using SDN.

E2E service managment is a way to mitigate the problem of having a lot of stakeholders involved in the delivery of a service. But this will require standardized interfaces through which services can be deployed and managed. It will also require well defined Service Level Agreements (SLAs) between service providers and service users.

4.2.2.3 Self-Organizing Networks (SON)

One of the major ways of automating O&M is to provide a self-organizing network (SON). SON features deals with self-configuration, self-optimisation and self-healing of the network. The SON functionality can be centralized in higher order network elements or on OSS level, distributed to the edges of the network, or a combination of those (hybrid). A number of SON features have already been defined, such as:

- Automatic Neighbour Relations (ANR) which automatically finds neighbour base station relations.
- Coverage and Capacity Optimization (CCO) which provides continuous coverage and optimal capacity.
- Mobility Robustness Optimization (MRO) which reduces the number of handover-related radio link failures.
- Mobility Load Balancing (MLB) which copes with unequal traffic load.
- RACH optimization for minimization of access delays.
- Minimization of Drive Tests (MDT) which minimizes the need of manual drive-tests.
- Turning off cells during low traffic periods.

Many of these are standardized by 3GPP[13], but there are also vendor unique variants.

In the future network, another dimension of this will come in, namely the virtualization of network functions. The elasticity this offers, will enable automatic scaling of network functions depending on traffic load, but also moving of network functions in the network to provide capacity where needed.

SDN will also offer a new level of flexibility where automatic transport path configuration can be seen as SON features.

4.2.2.4 Active Monitoring including Virtual Probes

Active monitoring involves insertion of probes in the network which can generate test traffic and monitor the generated traffic. A probe can also be used to passively monitor real traffic. In the NFV architecture, virtual probes can be provided. ETSI is working on an active monitoring framework[16] where the virtual probes are called Virtual Test Agents (VTAs). They are managed from Test Controllers, and test results are collected and analysed in Test Results Analysis Modules (TRAMs). As part of the framework there may also be Virtual Impairment Generators (VIGs), which are used for injecting faults. The network behaviour resulting from the injected faults can then be observed.

The main benefit with this architecture is that it makes physical traffic generators and monitors more or less redundant. They can also easily be deployed where needed without site visits. Virtual probes will also be cheaper than physical ones, and easier to upgrade. Active monitoring may be a way to verify a service as part of the fulfilment phase of an E2E service deployment, but also to find bottlenecks or other problems in a network.

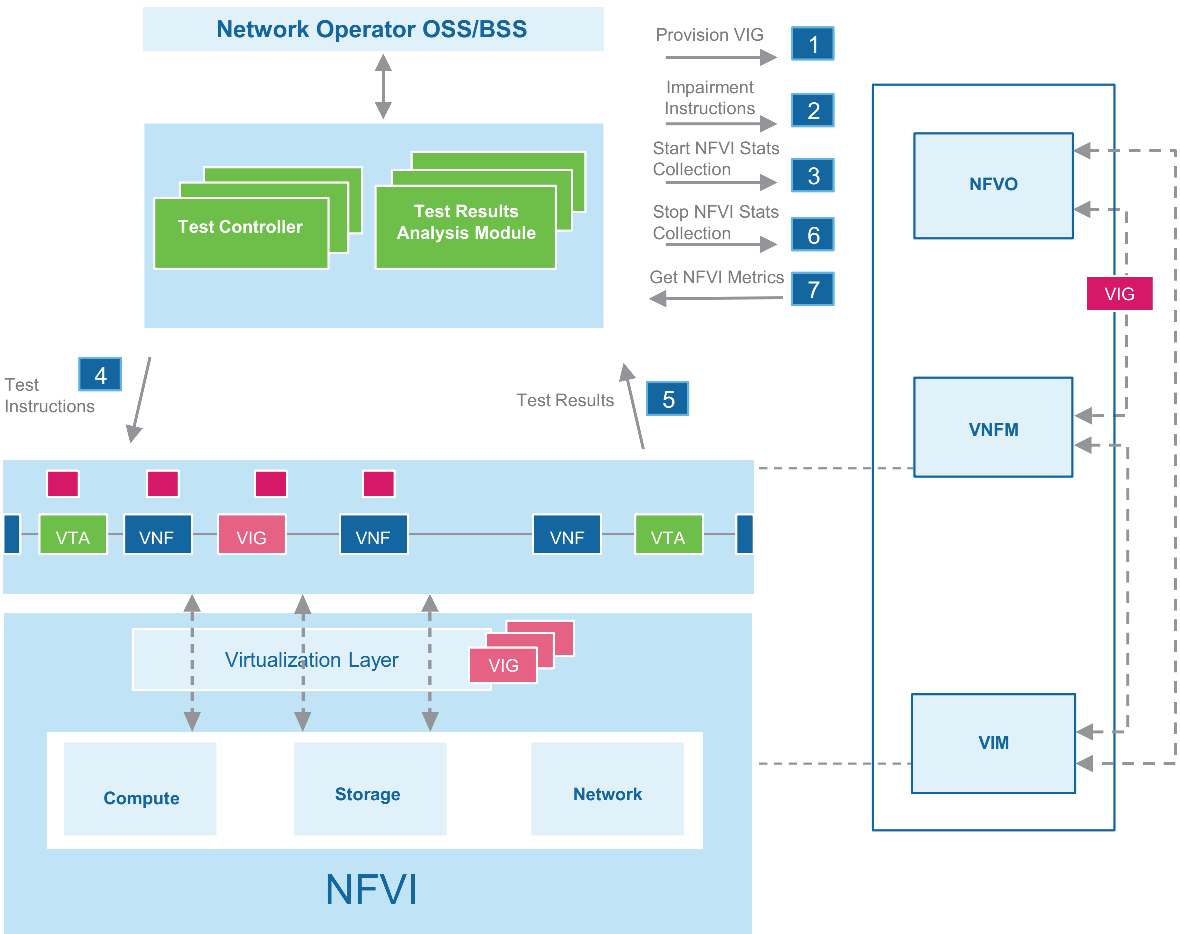

Figure: The active monitoring framework

4.2.2.5 Big Data Analytics including Machine Learning and Context Awareness

With many different services using the network, it may be hard to manually analyse performance data and find root causes of problems. With big data analytics; performance data, alarms, and possibly other external data, such as weather data, can be analysed to detect anomalies and find root causes of these.

Analysis of big data would typically be done on OSS/BSS level where data from many network elements/functions can be collected. But intelligent data filtering and aggregation can also be done on lower levels to improve performance and reduce network load.

Big data analytics often includes machine learning. Machine learning starts with a learning phase in which a model describing the data as accurately as possible is determined, such as a linear model or a cluster model. This model can then be used to do predictions and detect anomalies.

Another dimension of big data analytics is to make it context aware, that is, to be aware of what kind of traffic that is flowing in the network. This is especially important in networks where the operator mainly offers bit-piping. By being context aware the network can be optimized so that different services are handled in the most efficient way. Making sure that the network complies with Service Level Agreements (SLAs) is an important aspect of this. Context awareness may be implemented through Deep Packet Inspection (DPI) which does inspections of the data part of packets to determine the service conveyed, such as web browsing, video streaming, voice calls, etc.

5. Conclusions

The next generation mobile network will introduce many new network architectures and functionalities, which means that the complexity of the network will increase significantly. So the main goal regarding O&M for the next generation mobile network will be to hide this complexity from the operator. The main ways are to automate the O&M as much as possible, and to go from management of network elements to management of E2E services.

The scaling as part of NFV and the network configuration as part of SDN must be made as automatic as possible, otherwise the operators are faced with new dimensions of complexity that will be hard to manage manually.

E2E service management not only solves the complexity issue, it is also a way to improve service agility, that is, a way to quickly get new or updated services into operation.

Interoperability between systems and operators will also be of big importance. E2E service management will require that different systems run by different operators provide standard/well defined interfaces through which the service can be managed from a central place. When different service providers and service users are involved, it will also be important to have SLAs for which compliance can be verified.

Use of virtual probes instead to physical test equipment will simplify and reduce the cost of verifying network capabilities and finding root causes of problems.

Big data analytics and machine learning will be a way to go from a reactive to a proactive mode of operation. By also including context awareness, the ability to provide a good user experience will be even better.

In general, virtualization, network slicing and different sharing models will be very important in order to increase network utilization and keep down network investment costs.

6. Tieto Offerings

Tieto has a long history of developing O&M solutions in telecom nodes, OSS/BSS systems, cloud platforms and cloud applications.

Tieto is also an active contributor to the RECAP project (<http://recap-project.eu/>) focused on reliable capacity provisioning and remediation of cloud services, where services are elastically instantiated and provisioned close to the users, e.g. in Radio Access Networks. Tieto is providing an infrastructure and network management use case applied to Tieto's 5G/NFV testbed. Big data analytics and machine learning principles will be applied.

In telecom, Tieto offers product development services as well as selected solutions. In O&M, Tieto offers an O&M framework. It consists of

- an O&M component; a data driven and scalable solution with a small footprint and easy integration into different products, that provides north-bound interfaces to management systems (currently SNMP, Netconf and CLI are supported, but other, such as REST APIs, can also be offered),
- a MOM tool through which information model code for the O&M component and test scripts can be generated,
- an O&M validator that runs test scripts towards the O&M component, and
- an element manager that interfaces the O&M component.

This framework can be used to provide O&M functionality in the NFV, SDN, MEC and active monitoring architectures. It is currently used in widely deployed base station products, in solutions for vRAN, in the RECAP project, and was also used in the NFV proof-of-concept[20) done jointly by Intel, Qosmos and Tieto.

7. About Tieto

Tieto is the largest Nordic IT services company providing full life-cycle services for both the private and public sectors and product development services in the field of communications and embedded technologies. The company has global presence through its product development business and global delivery centres. Tieto is committed to developing enterprises and society through IT by realizing new opportunities in customers' business transformation. At Tieto, we believe in professional development and results.

Founded 1968, headquartered in Helsinki, Finland and with approximately 14 000 experts, the company operates in over 20 countries with net sales of approximately EUR 1.6 billion. Tieto's shares are listed on NASDAQ OMX in Helsinki and Stockholm.

8. References

1) NGMN 5G White Paper,
http://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf

2) ETSI - Network Functions Virtualisation,
http://www.etsi.org/technologies-clusters/technologies/nfv

3) ETSI – Mobile-Edge Computing – Introductory Technical White Paper,
https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1%2018-09-14.pdf

4) ONF - Software-Defined Networking (SDN) Definition,
https://www.opennetworking.org/sdn-resources/sdn-definition

5) ETSI - Report on SDN Usage in NFV Architectural Framework,
http://www.etsi.org/deliver/etsi_gs/NFV-EVE/001_099/005/01.01.01_60/gs_NFV-EVE005v010101p.pdf

6) ONF - OpenFlow Switch Specification Version 1.0.0,
https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.0.0.pdf

7) OMA LightweightM2M,
http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/oma-lightweightm2m-v1-0

8) 3GPP Low Power Wide Area Technologies,
http://www.gsma.com/connectedliving/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf

9) 3GPP - LTE Standards for Public Safety – 3GPP view,
http://www.3gpp.org/IMG/pdf/2013_05_3gpp_ccw.pdf

10) IEEE 802.15 WPAN™ Task Group 4 (TG4),
http://www.ieee802.org/15/pub/TG4.html

11) IETF - The Constrained Application Protocol (CoAP),
https://tools.ietf.org/html/rfc7252

12) IETF - Transmission of IPv6 Packets over IEEE 802.15.4 Networks,
https://tools.ietf.org/html/rfc4944

13) 3GPP - Self-Organizing Networks,
http://www.3gpp.org/technologies/keywords-acronyms/105-son

14) OpenFog Consortium,
https://www.openfogconsortium.org/

15) MEF Third Network Lifecycle Service Orchestration Vision,
http://www.mef.net/Assets/White_Papers/MEF_Third_Network_LSO_Vision_FINAL.pdf

16) ETSI GS NFV-REL 004 - Network Functions Virtualisation (NFV); Assurance; Report on Active Monitoring and Failure Detection,
http://www.etsi.org/deliver/etsi_gs/NFV-REL/001_099/004/01.01.01_60/gs_NFV-REL004v010101p.pdf

17) MEF and ETSI NFV ISG Collaborate To Advance NFV For Carrier Ethernet 2.0 Services Enabled By Lifecycle Service Orchestration,
http://www.etsi.org/index.php/news-events/news/1011-2015-10-news-mef-and-etsi-nfv-isg-collaborate-to-advance-nfv-for-carrier-ethernet-2-0-services-enabled-by-lifecycle-service-orchestration

18) IoT Security Foundation,
https://iotsecurityfoundation.org/

19) MQTT Version 3.1.1 Plus Errata 01,
http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html

20) Realising the Benefits of Network Functions Virtualisation in Telecoms Networks,
https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/benefits-network-functions-virtualization-telecoms-paper.pdf

21) Open Network Automation Platform (ONAP), https://www.onap.org/

Tieto aims to capture the significant opportunities of the data-driven world and turn them into lifelong value for people, business and society. We aim to be customers' first choice for business renewal by combining our software and services capabilities with a strong drive for co-innovation and ecosystems.

www.tieto.com

tieto