Question 8/12 – Virtualized deployment of recommended methods for network performance, quality of service (QoS) and quality of experience (QoE) assessment

(Continuation of Question 8/12)

1 Motivation

As network service providers seek to take advantage of the scale, flexible deployment, and cost reductions first realized in cloud computing, they have begun to define new architectures for their infrastructure in order to realize network function virtualization (NFV). ETSI NFV has developed an architectural framework that illustrates how virtual network functions (VNF) will be supported and managed when they replace their physical counterparts with dedicated resources.

Following the completion of Y.1550, additional study of virtualized network performance, QoS and QoE monitoring and assessment as it applies to the modelling and measurement methods recommended by the Study Group is warranted.

The implementation of metrics, models, and their methods of measurement is usually beyond the scope of SG12 Recommendations, except for Implementers' guides. Therefore, considerations developed in this work must emphasise how the metrics, models, and their methods would change or be augmented in the case where their implementation is virtual. Further, new methods to characterize the deployment environment and adapt the measurements to better suit the current circumstances are desirable.

2 Question

Study items to be considered include, but are not limited to:

- When considering the trade-offs between Hypervisors and Containers, the investigation needs to include a very important issue: security. It has been proven that an adversary attack on containers could cause direct damage to all containers present inside the pod, while the same attack on a hypervisor, though the impact on the service itself is similar, would cause lighter damage to VNFs located on other servers. This could be addressed in more detail in a future version of this Recommendation.
- The question of port mirroring, addressed in Y.1550 clause 6.3 of the Recommendation, needs to be deeply understood. There are several types of virtual switches available (Open vSwitch – OVS, Vector Packet Processor – VPP). Port mirroring is possible on all, but with different constraints and impact in terms of traffic filtering or timestamp accuracy. The use of SDN techniques is also a possibility to modify flow paths in a more flexible and efficient way, and thus add a monitoring opportunity for a VMS.
- The question of VMS management is also addressed in Y.1550 clause 6.3 of the Recommendation. This is a very crucial point. For the time being, the use of existing features in MANO architecture is certainly not enough, and dedicated management appears to be needed. This separated management is justified by the observation that management must be reliable and trusted. As a result, a measurement system must remain independent of what it is measuring, and so must its management. There is further study required to examine the details behind this need, such as the degree of separation and specific methods used.

– There are questions regarding the deployment strategies of VMS. Can be such deployment be independent of other VNFs (and thus vProbes are VNFs like the others, integrated in the orchestration process) or does deployment depend on other VNFs (e.g. when a new VNF is created, is there a rule in NFVO to create a VMS in association? but then isn't NFVO service-aware?). This is a crucial question that this Recommendation should address in the future, since VMS can be service specific and then managed through service orchestration, i.e. outside NFV concepts. It is believed that VMS deployment cannot be completely independent of the service, except for some generic VMS like "packet capture and store for later analysis". The metrics the VMS measures are very likely dependent on the specific service, including the locations where they are deployed in the service path.

– In Y.1550 clause 7.1 on time-stamp accuracy, future versions of this Recommendation should go beyond global considerations and propose solutions. Although hardware probes are in general quite accurate in terms of timestamping (sub microsecond time stamp, GPS synchronization, etc.), in some cases, a loose time stamping (Linux time) could be sufficient for exploiting the collected data. For virtualized monitoring, extremely accurate time stamping may be not required and less accurate time stamping (say, in the millisecond range) may be sufficient for many applications (e.g., traffic volume estimation). Solutions based on PTP protocol exist that allow accurate-enough time stamping.

– The specific role of measurement and supervision systems in telecommunication networks deserves some deeper thinking on their evolution when we consider virtualized network functions. For this topic, study is required beyond the current scope.

– Classical network, QoS and performance measurement systems are generally NOT network functions. These are most of the time systems installed and operated in parallel to the network, with their own specific hardware (TAPs, probes), data collection interfaces and management systems. Some of these systems provide APIs or northbound interfaces allowing operating systems (part of OSS) to collect and analyse the measurement results and to take decisions based on them. As far as now known, such systems are not considered by SG12 as an area for standardization.

– With virtualized network functions, the situation becomes radically different and may require new consideration. Probes cannot rely on physical interfaces to collect data at the edge of a given network function. The information is now available through temporary logical interfaces inside virtual machines. Three possibilities can then be envisaged (this list is not exhaustive):

  - either specific functions are developed inside or on top of the Infrastructure as a Service (IaaS) to provide a port mirroring (ingress/egress traffic) of logical interfaces to a physical interface where a probe can be connected,
  - or the probe itself becomes a virtual function of the virtual machine (the port mirroring is still needed but the traffic is duplicated towards a logical interface),
  - or else the probe is a virtual function hosted outside the system and connected to it through virtual port mirroring functions.

  The current scope of Recommendation Y.1550 takes the second option as assumption: the probe becomes virtual, because access will be difficult without this virtualized form, and part of the system. This choice can seem obvious at first, and in practice corresponds to the target deployment of many network operators. This approach requires new skills, like how to isolate the VMS from the bad-actor VNFs in the host to isolate the measurements and maintain integrity. The same skills can then be applied to isolate other critical VNFs, and so on.

However in reality, supervision of VNFs with physical probes (in particular when such tools are already in place and running, and if the number of servers involved in the virtualized architecture to supervise is limited) is not necessarily a bad idea when starting with NFVI. Mixed solutions combining hardware and virtual probes exist also.

The alternatives of mixed virtual and physical measurement systems, and all physical measurements have their advantages and disadvantages. The physical ports are costly, and the measurement path between the host and the probe will likely include a switch – and the traffic on the switch can (or will) influence the measurement.

The different measurement deployment options require further consideration and examination of their trade-offs.

– The scope of this Recommendation is focused on practical implementation issues (and provides very good insight). However, the Scope could be expanded with a 6th study area on data collection and usage. Future versions of this Recommendation should address questions like:

  - How is the link built and managed between VMS and data analysis functions like DCAE (see ONAP architecture)?
  - Can VMS be kept outside VNF architectures with their own data collection and processing features (construction of CDRs, recording of pcap files), as this is the case with hardware supervision systems, and how?
  - Is there a need for specific rules for connecting VMS to network supervision functions like Alerting and Troubleshooting?
  - Is data collection with VMS dimensioned and secured in order to feed properly Big Data analytics tools?

  This area is for further study in other Recommendations to develop, unless Y.1550 clause 6.3 can be expanded in the future to cover this wider scope.

3 Tasks

Tasks include, but are not limited to:

– Revise Recommendation Y.1550 on considerations for virtualized measurement systems.

– Develop new Recommendations as needed.

An up-to-date status of work under this Question is contained in the SG12 work programme http://www.itu.int/ITU-T/workprog/wp_search.aspx?q=8/12.

4 Relationships

WSIS Action Lines

– C2

Sustainable Development Goals

– 9

Recommendations

- P.564, P.863, P.1200, P.1201, P.1202

Questions

- 9/12, 11/12, 12/12, 13/12, 14/12, 16/12, 17/12

Study Groups

- ITU-T SG2, SG13, SG15, SG16, SG17

Other bodies

- MEF, IETF working groups on performance issues, IEEE 802 LAN/MAN Standards Committee, 3GPP, Broadband Forum, ETSI, ANSI, GSMA