Final draft ETSI EG 203 341 V1.1.1 (2016-08)

Core Network and Interoperability Testing (INT); Approaches for Testing Adaptive Networks

Reference
DEG/INT-00127

Keywords
conformance, interoperability, methodology

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This final draft ETSI Guide (EG) has been produced by ETSI Technical Committee Core Network and Interoperability Testing (INT), and is now submitted for the ETSI standards Membership Approval Procedure.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The characteristics of "adaptive networks" such as virtualization, self-organization, self-configuration, self-optimization, self-healing and self-learning, dynamic network slicing promise to offer huge advantages in future networks. While technologies such as Network Functions Virtualisation (NFV), Self-Organizing Networks (SON), Mobile Edge Computing (MEC) and Autonomic Management and Control (AMC) of Networks and Services may not each exhibit all the characteristics they do have one thing in common: they are all dynamic rather than static, reacting to dynamic traffic conditions, applications, service demands as well as to changes in the eco-system environment.

By incorporating one or several of the technologies mentioned above, Adaptive Networks (AN) have the ability to automatically and dynamically manage and control network resources, configuration parameters or the network structure, with limited human intervention, in order to meet functional targets or operational policies. However, to achieve this type of autonomic behaviour, it has to be ensured that any modification that is performed automatically in the network does not produce undesired effects, e.g. instability or lower performance with respect to the end-user perspective.

Comprehensive testing, both on a general level as in type approvals and related to acceptance testing of a particular deployment, is therefore even more important than it is for conventional networks. Due to the fact that the components of an AN may interact in a more complex and interdependent way than in a conventional network, appropriate testing methodologies are required in all phases of operation. For instance, the effect of software updates in network components can be amplified by the more connected nature of these components in an AN.

The rest of the present document is organized as follows:

- Clause 4 gives the definition of an adaptive network, as used in the context of the present document.
- Clause 5 defines the entities and interactions that may be encountered in an adaptive network.
- Clause 6 defines the general functional targets that should be met by adaptive networks.
- Clause 7 defines the methods that may be used to test adaptive networks.

- Annex A gives an overview of the relation of the present document to other work performed in this area, e.g. NFV TST, NTECH-AFI.

1 Scope

The present document, "Approaches for Testing Adaptive Networks" defines a framework of testing principles and guidelines that may be used to test networks that exhibit some form of autonomic adaptive behaviour, which allows them to dynamically change their configuration, structure or operational parameters. The (re)-configuration is performed in response to stimuli such as changes in workload, operator policies that govern their operation, context (the network is context-aware and may have a degree of self-awareness); and challenges in the environment (i.e. conditions under which the network is operating, e.g. manifestations of faults, errors, failures in various parts of the network and its hardware and software components).

The functionality of individual components and basic interoperability can be ensured at design time. However, the complex interactions between various components or functions deployed in a live Adaptive Network (AN) may not be fully assessed or foreseen. Consequently, the document addresses methodologies to test ANs towards meeting their functional targets or policies, and ensuring a minimum trust level for autonomic operation of such networks.

NOTE: In the literature, both the terms "autonomous" and "autonomic" are being used in this context, whereas "autonomous" appears to indicate a higher level of automation. As adaptive networks are, at the time of writing, surely a technology still at its beginnings, "autonomic" may be a less ambitious and therefore more appropriate term for the time being. On the other hand, the NGMN 5G White Paper (V1.0) uses the term combination "autonomic/self-management functions" which points, clearly towards a level beyond "autonomic". As mobile networks are complex systems, it is most likely that the degree of automation will increase in the course of technical evolution, but not in an isotropic way; there will be areas with higher and others with lower levels of automation, and sophistication of respective functions. For these reasons, the present document will use the term "autonomic".

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS AFI 002: "Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture (An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management)".

[i.2] ETSI TS 102 250-4: "Speech and multimedia Transmission Quality (STQ); QoS aspects for popular services in mobile networks; Part 4: Requirements for Quality of Service measurement equipment".

[i.3] Recommendation ITU-T P.10/G.100 Amendment 2 (07/2008): "Vocabulary for performance and quality of service Amendment 2: New definitions for inclusion in Recommendation ITU-T P.10/G.100".

[i.4] Recommendation ITU-T E.800 (09/2008): "Definitions of terms related to quality of service".

[i.5] ISO/IEC 9646: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework".

[i.6] ETSI GS NFV-TST 001 (V1.1.1): "Network Functions Virtualisation (NFV); Pre-deployment Testing; Report on Validation of NFV Environments and Services".

[i.7] ETSI GS NFV-TST 002: "Network Functions Virtualisation (NFV); Testing Methodology; Report on Interoperability Testing Methodology".

[i.8] Dar, K.: "Autonomic Computing: An introduction to MAPE-K reference model".

NOTE: Available at http://www.uio.no/studier/emner/matnat/ifi/INF5360/v13/undervisningsmateriale/mape-k.pdf.

[i.9] IBM (2005):"An architectural blueprint for autonomic computing".

NOTE: Available at http://www-03.ibm.com/autonomic/pdfs/AC%20Blueprint%20White%20Paper%20V7.pdf.

[i.10] Hayan, Z.: "A novel autonomic architecture for QoS management in wired network".

NOTE: Available at http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5700376&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5700376).

[i.11] Strassner, J., Agoulmine, N., & Lethihet, E. (2006): "FOCALE - A Novel Autonomic Networking Architecture".

NOTE: Available at http://repository.wit.ie/189/1/2006_LAACS_Strassner_et_al_final.pdf.

[i.12] Clark, D. C., Partridge, C., Ramming, J. C., Wroclawski, J. T.: "A knowledge plane for the internet".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

aggregation hierarchy: description of how detailed (granular) performance data will be aggregated into summary data, and vice versa, how to break down the summary data into details

attractor: state or behaviour toward which a dynamic system tends to evolve, represented as a point or orbit in the system's phase space

control loop: mechanism which uses observations of a system to make modifications to the observed system to meet a given target

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AF	Adaptive Function
AFI	Autonomic Future Internet
AMC	Autonomic Management and Control
AN	Adaptive Network
CCO	Coverage and Capacity Optimization
DE	Decision Element
eNB	evolved Node B
FUT	Function Under Test
GANA	Generic Autonomic Network Architecture
IBM	International Business Machines
ISG	Industry Specification Group
ITU-T	International Telecommunication Union - Telecommunication standardization sector
KPI	Key Performance Indicator

LTE	Long-Term Evolution
MEC	Mobile Edge Computing
MRO	Mobility Robustness Optimization
NE	Network Element
NFV	Network Functions Virtualisation
NGMN	Next Generation Mobile Networks
NTECH	Network Technologies
NUT	Network Under Test
OCS	Overall Configuration State (of a network)
ONP	Overall Network Properties
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
SDN	Software Defined Networking
SLA	Service Level Agreement
SON	Self Organizing Networks
UE	User Equipment
VoLTE	Voice over LTE

4 Definition of Adaptive Networks

4.1 Basic Concept

The term "adaptive network" (AN) refers to any network that has the ability to automatically modify its configuration, operational parameters or structure, in order to comply with pre-defined functional targets or operational policies, and with the ability to handle situations that were unknown at its design time (e.g. with predictions and forecasting capabilities as well), thus producing a dynamic environment with multiple potential network states. An adaptive network may include technologies such as Self Organizing Networks (SON), Network Functions Virtualisation (NFV), Software Defined Networking (SDN), Autonomic Management and Control (AMC) or any other technology which enables a network to exhibit the characteristics mentioned above.

Adaptive networks are comprised of one or more Adaptive Functions (AF) that dynamically and adaptively manage and control certain network attributes. These functions are fundamentally characterized by exhibiting control-loops which can be embedded at different layers e.g. protocol level, node level, network level, and exert different degrees of influence over the network. Similarly, the management and control of the AFs can be aggregated at different levels depending on the information required for their operation. Furthermore, ANs may function on different time scales and with different levels of complexity and views on which they operate on, depending on the type of AFs that are deployed. However, from an end user perspective, the presence or absence of AFs in a network is transparent, meaning that end users can only observe the functionality of the network service. Similarly to conventional networks, the internal structure and operation of the network is not visible from this perspective.

Depending on the type of AFs and the level where they are deployed, the frequency of changes performed throughout an AN can differ. In general, low level AFs can operate at faster time scales, i.e. fast control loops as they utilize information collected locally. On the other hand, high level AFs require information about the overall state of the network and thus typically operate in slow control loops. The architecture of an AN, in terms of the hierarchical placement of AFs and aggregation levels is important from a testing perspective and determines if and how the particular network can be tested. Figure 1 illustrates the different architectures of ANs and the associated control loops.

Two extreme cases can be distinguished:

- Fully distributed adaptive network, where all AFs operate at lower levels, e.g. at the protocol or node level, with no management and control aggregation at higher levels.
- Fully centralized adaptive network, where AFs operate at higher levels, e.g. network level and aggregate network wide information.

The fully distributed architecture poses higher challenges from a testing perspective, since the effect of AFs that operate in fast control loops may not be easily translated into functional KPIs that can be observed by a test system. Furthermore, their policies and functional targets are managed and executed locally, at an aggregation level where information may not be available for a test system. On the other hand, the fully centralized architecture is the most attractive from a testing perspective, since it operates using slow control loops and uses information that is aggregated at network level.

A typical AN will incorporate several types of AFs, that operate and aggregate information at different levels. Hence, from an architectural perspective it may use a hybrid model, which includes distributed, and centralized AFs or AFs that are aggregated at an intermediated level. Additionally, a peer-to-peer relationship may be formed between AFs operating at the same hierarchical level.

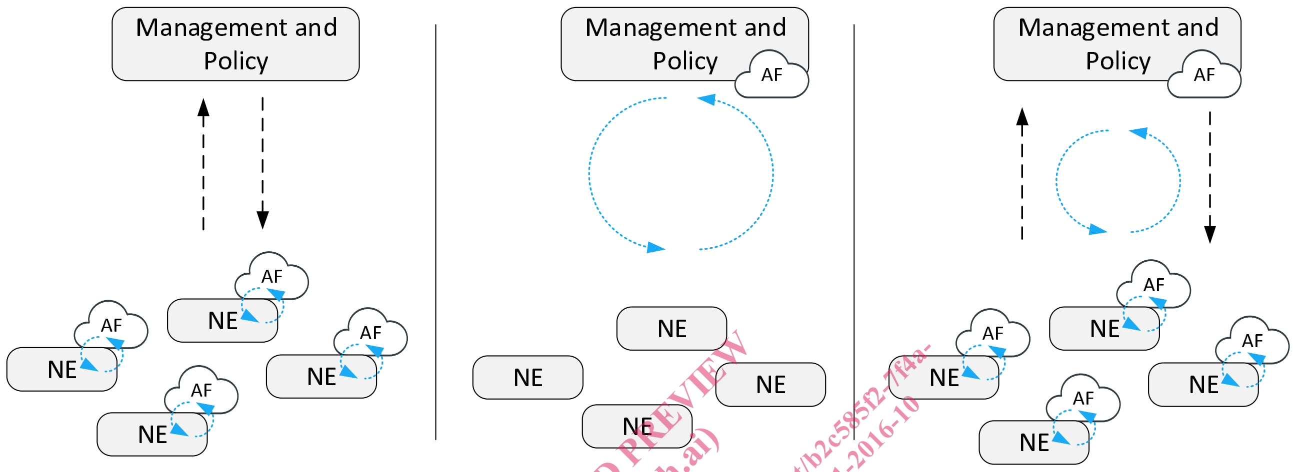

Figure 1: Adaptive Network Architectures: distributed, centralized and hybrid

The detailed internal structure and algorithms of the AN may not be known to an external test environment. However, a minimum set of information regarding the operation and structure of the AN may be required in order to interpret results generated from end-to-end functionality testing. This information can include details about the functional targets of the AN, the capabilities of AFs that are deployed, their operational status, e.g. active, idle, disabled, the network attributes that they control and their influence on the functional target being measured. Part of the information may be obtained out of band, i.e. be provided as external input to the test system, while part of the information may be obtained from the Network Under Test (NUT).

An adaptive network typically functions in a closed loop manner, with minimum human intervention using sensor information to make decisions and perform actions, according to policies set by the network operator. These actions can be categorized in:

- Actions that are performed on network configuration parameters or network resources, e.g. Transmission Power, antenna tilt, routing policies, bandwidth allocation.
- Actions that are performed on the network structure, e.g. adding/removing network elements (either physical or virtualized instances). These actions imply configuration changes in order to accommodate the structural change.

The events that can trigger an adaptive network to dynamically change its properties vary also depending on the specific AFs deployed in the network and the level at which they operate. They can be split in two categories:

- Externally generated events - when the adaptive behaviour is triggered by an external factor, e.g. increase in user traffic that creates unbalanced load in the network, detecting service-level performance degradation, failure of network elements.
- Internally generated events - when the adaptive behaviour is triggered as a result of an internal policy, independent of external activity, e.g. power savings mode, configuration of network properties to provide QoS for certain traffic types, e.g. low latency traffic, delay-tolerant traffic, low-bandwidth traffic.

NOTE: These events can occur in a chain like fashion, e.g. policy change can trigger several secondary events in lower level functional units.

4.2 General Terminology

4.2.1 Introduction

A fundamental characteristic of ANs is the ability to dynamically change their configuration and properties. In order to describe the testing methodology some basic concepts (configuration states, state transitions and attractors) have to be introduced, as their meaning is new or goes beyond well-known definitions for conventional networks.

4.2.2 Network States

A network is characterized by its hardware and software components, together with the configuration of these components. This configuration is given by control elements, which can be on hardware level (e.g. elements determining physical orientation of antennas) or on software level (parameters determining the functional behaviour of a component). A component can have multiple control elements which define its overall state. Similarly, the overall network state is defined by the overall states of each component. The total number of these controls - counting each degree of freedom separately - is typically large, but finite and a fixed property of a given network.

Each degree of freedom can be:

- a discrete value, out of a given set of choices or a range of integer values; or
- a continuous (analogue) value.

The totality of all degrees of freedom represents the settings space. Each combination of settings can be described as an N-dimensional vector, where N is the number of degrees of freedom, also called the dimension of the settings space. An individual control setting is then the i-th element of this settings vector.

Each possible combination of settings is represented by the corresponding vector. For the purpose of the present document, such a vector is termed Overall Configuration State (OCS).

A change of settings - regardless if done by human operators as in conventional networks or by automatic processes in AN - means a transition between an initial OCS S_1 to a new OCS S_2.

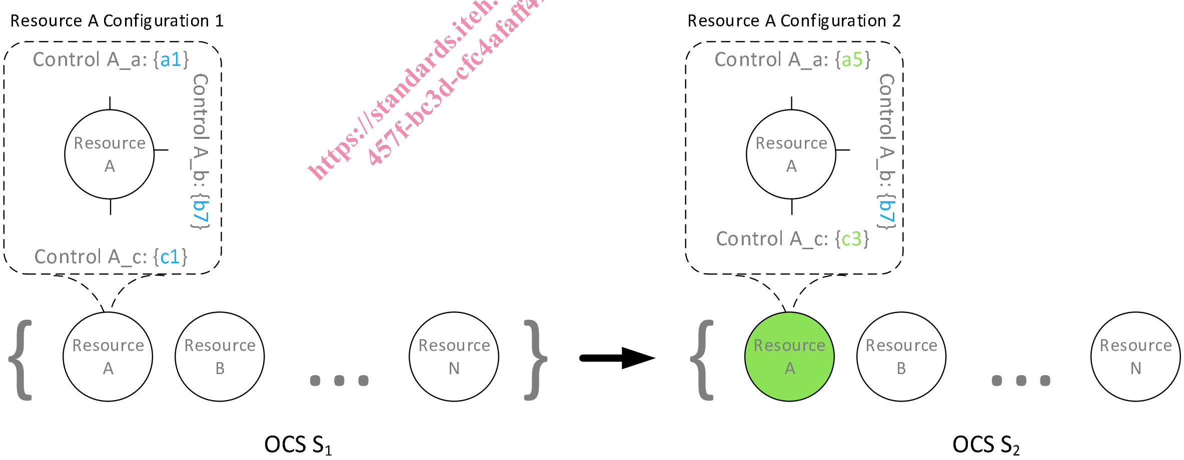

Figure 2: Concept of controls and Overall Configuration State (OCS) transitions

Also for this purpose and later usage, the term overall network properties (ONP) is defined which describes the appearance of the network as perceivable from the end user point of view or through other interfaces to the network operator (see also clause 5.1). Each OCS leads to a specific ONP.

NOTE: This relation is not symmetric; several OCS can lead to the same ONP, but the assumption is that the same OCS cannot lead to different ONP. If this was the case it would mean that some aspect of the network shows random behaviour which is a primarily unwanted condition.