ETSI TR 103 473 V1.1.2 (2018-12)

TECHNICAL REPORT

Evolution of Management towards Autonomic Future Internet (AFI); Autonomicity and Self-Management in the Broadband Forum (BBF) Architectures

Reference
RTR/INT-007_0016-GANA-BBF

Keywords
architecture, autonomic networking

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Core Network and Interoperability Testing (INT).

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.

1 Scope

The present document aims at providing recommendations for the introduction of autonomics (management and control intelligence) into the fixed broadband access and aggregation networks specified in the Broadband Forum (BBF) Architecture specifications. To this effect, it covers the instantiation of the reference model for Autonomic Networking, Cognition and Self-Management, called GANA (Generic Autonomic Networking Architecture) [i.1], starting from the reference architecture defined in BBF TR 101 [i.6], and considering also BBF TR 178 [i.7] and BBF TR 317 [i.28] reports. It superimposes GANA Decision Elements (DEs) into nodes/devices and the overall BBF network architecture, so that the DEs and their associated control-loops can be further designed to perform autonomic management and control of the specific resources (Managed Entities) in the target architecture.

Based on this, the present document identifies the requirements for autonomic behaviours (Autonomics Functions/DEs) across the fixed broadband access and aggregation network segments of the BBF reference architecture and provides recommendations on where and how the GANA Functional Blocks (including DEs) should be instantiated. It further extends these recommendations to the virtualized manifestation of these segments considering their virtualized evolution in conjunction with SDN and NFV technologies. Finally, it also provides recommendations on the interworking and coordination between autonomic functions among GANA-BBF and GANA-3GPP (Core Network) domains, as well as recommendations on the Interworking and coordination between virtualized GANA-BBF and virtualized GANA-3GPP (Core Network) domains.

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 White Paper No 16: "GANA - Generic Autonomic Networking Architecture - Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services".

NOTE: Available at http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp16_gana_Ed1_20161011.pdf.

[i.2] 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)".

NOTE: This GS is now undergoing a transformation to an ETSI TS 103 195-2 [i.30] that has been published by ETSI in 2018: http://www.etsi.org/deliver/etsi_ts/103100_103199/10319502/01.01.01_60/ts_10319502v010101p.pdf.

[i.3] Ranganai Chaparadza, Tayeb Ben Meriem, John Strassner, Steven Wright and Joel Halpern: "Industry Harmonisation for Unified Standards on Autonomic Management & Control of Networks and Services, SDN, NFV, E2E Orchestration, and Software-oriented enablers for 5G", Report from the Joint SDOs/Fora Workshop hosted by TMForum during TMForum Live 2015 Event Nice, France (June 4th, 2015).

NOTE: Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7063423 [i.4] ETSI TS 103 194: "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet".

[i.5] ETSI TR 103 404 (V1.1.1): "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Autonomicity and Self-Management in the Backhaul and Core network parts of the 3GPP Architecture".

[i.6] BBF TR 101: "Migration to Ethernet-Based Broadband Aggregation", Issue: 2, Issue Date: July 2011.

[i.7] BBF TR 178: "Multi-service Broadband Network Architecture and Nodal Requirements", Issue: 1, Issue Date: September 2014.

[i.8] BBF TR 359: "A Framework for Virtualization", Issue: 1, Issue Date: October 2016.

[i.9] BBF TR 134: "Broadband Policy Control Framework", Issue: 1, Issue Date: July 2012.

[i.10] Chaparadza R., Wodczak M., Ben Meriem T., De Lutiis P., Tcholtchev N., Ciavaglia, L. (2013): "Standardization of resilience & survivability, and autonomic fault-management, in evolving and future networks: an ongoing initiative recently launched in ETSI", In: Proceedings of the 9th international conference on design of reliable communication, networks (DRCN), pp 331-341.

[i.11] Nieminen M., Tcholtchev N., Schieferdecker I. et al.: "Robust architecture for distributed intelligence in an IP-based mobile wide-area surveillance system", The Journal of Supercomputing (2014) vol. 70: pp 1120-1141. doi:10.1007/s11227-014-1160-7.

[i.12] Tcholtchev N., Chaparadza R. (2010): "Autonomic fault-management and resilience from the perspective of the network operation personnel", In: Proceedings of the GLOBECOM workshops, 2010 IEEE, pp 469-474. doi:10.1109/GLOCOMW.2010.5700364.

[i.13] Chaparadza R., Tcholtchev N., & Kaldanis V. (2010, November): "How autonomic fault-management can address current challenges in fault-management faced in it and telecommunication networks", In: International Conference on Access Networks (pp. 253-268). Springer Berlin Heidelberg.

[i.14] Wendong Wang, Ye Tian, Xiangyang Gong, Qinglei Qi, Yannan Hu: "Software defined autonomic QoS model for future Internet", Elsevier Journal of Systems and Software, Volume 110, December 2015, Pages 122-135.

NOTE: Available at http://dx.doi.org/10.1016/j.jss.2015.08.016.

[i.15] Wendong Wang; Xiangyang Gong; Xirong Que: "Context-aware autonomic QoS model for future Internet", Published in: GLOBECOM Workshops (GC Wkshps), 2011 IEEE. doi: 10.1109/GLOCOMW.2011.6162534.

[i.16] Constantinos Marinos, Christos Argyropoulos, Mary Grammatikou, Vasilis Maglaris: "An Autonomic Monitoring Framework for QoS Management in Multi-service Networks", Published in Mobile Networks and Management: Volume 68 of the series Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering pp 79-86: DOI: 10.1007/978-3-642-21444-8-8.

[i.17] Liakopoulos Athanassios et al.: "Applying distributed monitoring techniques in autonomic networks", GLOBECOM Workshops (GC Wkshps), 2010 IEEE.

[i.18] Anastasios Zafeiropoulos, Athanassios Liakopoulos, Alan Davy, Ranganai Chaparadza: "Monitoring within an Autonomic Network: A GANA Based Network Monitoring Framework: Service-Oriented Computing", ICSOC/ServiceWave 2009 Workshops: Volume 6275 of the series Lecture Notes in Computer Science pp 303-313: DOI: 10.1007/978-3-642-16132-2-29.

[i.19] Sandra Scott, Sriram Natarajan and Sakir Sezer: "A Survey of Security in Software Defined Networks", In IEEE Communications Surveys & Tutorials: DOI: 10.1109/COMST.2015.2453114.

[i.20] Software Defined Access Networking (SDAN): "Taking NFV and SDN to the "Edge", White Paper by ASSIA™.

[i.21] Heavy Reading & SaS White Paper: "Advanced Predictive Analytics: Optimize your Network & Transform Customer Experience".

[i.22] Mestres Albert, Alberto Rodriguez-Natal, Josep Carner, Pere Barlet-Ros, Eduard Alarcón, Marc Solé, Victor Muntés et al.: "Knowledge-Defined Networking", arXiv preprint arXiv:1606.06222 (2016).

[i.23] Ren Quinn et al.: "KnowNet: Towards a knowledge plane for enterprise network management": In proceedings of NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium: 10.1109/NOMS.2016.7502819.

[i.24] Bruno Cornaglia, Vodafone Group Services: "Fixed Access Network Virtualization", Broadband Forum Contribution bbf2014.084.00, February 14th, 2014.

[i.25] Cornaglia Bruno, Young Gavin and Marchetta Antonio: "Fixed Access Network Sharing", Elsevier publication: 10.1016/j.yofte.2015.07.008.

[i.26] BBF TR-370: "Fixed Access Network Sharing - Architecture and Nodal Requirements", Issue: 1, Issue Date: November 2017.

[i.27] Appledore Research Group White Paper: "Closed Loop Automation and the new role of Assurance": 9/1/2016.

[i.28] BBF TR 317: "Network Enhanced Residential Gateway", Issue 1, Issue Date: July 2016.

[i.29] NTECH-AFI TR Draft: "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Impact of Generic Autonomic Network Architecture (GANA) on other paradigms: NFV and SDN How GANA integrates with SDN, NFV, E2E Service Orchestration and Big-Data Analytics for Autonomics".

[i.30] ETSI TS 103 195-2 (V1.1.1): "Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management".

NOTE: Available at: http://www.etsi.org/deliver/etsi_ts/103100_103199/10319502/01.01.01_60/ts_10319502v010101p.pdf.

[i.31] Alexej Starschenko, Nikolay Tcholtchev, Arun Prakash, Ina Schieferdecker and Ranganai Chaparadza: "Auto-Configuration of OSPFv3 Routing in FixedIPv6 Networks", In 2015 7th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT): DOI: 10.1109/ICUMT.2015.7382427.

[i.32] gRPC protocol.

NOTE: Available at https://grpc.io/about/.

[i.33] Chaparadza R., Petre R., Prakash A., Németh F., Kukliński S. and Starschenko A. (2011): "IPv6 and Extended IPv6 (IPv6++) Features That Enable Autonomic Network Setup and Operation". Szabó R., Zhu H., Imre S., Chaparadza R. (eds) Access Networks. AccessNets 2010". In: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 63. Springer, Berlin, Heidelberg.

[i.34] A. Prakash et al: "Auto-Discovery and Auto-Configuration of Routers in an Autonomic Networks", Conference: Access Networks - 5th International ICST Conference on Access Networks, AccessNets 2010 and First ICST International Workshop on Autonomic Networking and Self-Management in Access Networks, SELFMAGICNETS 2010, Budapest, Hungary, November 3-5, 2010 DOI: 10.1007/978-3-642-20931-4-24.

[i.35] V. Kaldanis et al: "Methodology Towards Integrating Scenarios and Testbeds for Demonstrating Autonomic/self-managing Networks and Behaviors required in Future Networks", SELFMAGICNETS'10: Proc of the International Workshop on Autonomic Networking and Self-Management. ICST ACCESSNETS'10, Budapest, Hungary, November 2010.

[i.36] BBF TR 203: "Interworking between Next Generation Fixed and 3GPP Wireless Access", Issue: 1, Issue Date: August 2012.

[i.37] ETSI TS 123 139 (V14.0.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP system - fixed broadband access network interworking; Stage 2 (3GPP TS 23.139 version 14.0.0 Release 14)".

[i.38] ETSI TS 123 401: "LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401)".

[i.39] ETSI TS 123 402: "Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for non-3GPP accesses (3GPP TS 23.402)".

[i.40] ETSI TS 123 261 (V10.1.0): "Universal Mobile Telecommunications System (UMTS); LTE; IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2 (3GPP TS 23.261 version 10.1.0 Release 10)".

[i.41] ETSI TS 122 278 (V12.6.0): "Universal Mobile Telecommunications System (UMTS); LTE; Service requirements for the Evolved Packet System (EPS) (3GPP TS 22.278 version 12.6.0 Release 12)".

[i.42] BBF TR-304: "Broadband Access Service Attributes and Performance Metrics", Issue: 1, Issue Date: February 2015.

[i.43] F. Leitão, R. David Carnero Ros and J. Rius i Riu: "Fixed-mobile convergence towards the 5G era: Convergence 2.0: The past, present and future of FMC standardization", 2016 IEEE Conference on Standards for Communications and Networking (CSCN), Berlin, 2016, pp. 1-6.

[i.44] H. Kim, L. Kim and A. Kunz: "Enhanced 3GPP System for Interworking with Fixed Broadband Access Network, IEEE Commun", Mag., vol. 51, no. 3, March 2013.

[i.45] Fi-Ware System: "European Commission (EC)-funded Future Internet Core Platform".

NOTE: Available at https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/.

[i.46] IETF RFC 6241: "Network Configuration Protocol (NETCONF)".

[i.47] BBF TR 058: "Multi-Service Architecture & Framework Requirements".

NOTE: Available at https://www.broadband-forum.org/technical/download/TR-058.pdf.

[i.48] BBF TR 145: "Multi-service Broadband Network Functional Modules and Architecture".

NOTE: Available at https://www.broadband-forum.org/technical/download/TR-145.pdf.

[i.49] BBF TR 144: "Broadband Multi-Service Architecture & Framework Requirements".

NOTE: Available at https://www.broadband-forum.org/technical/download/TR-144.pdf.

[i.50] ANSI/IEEE 802.1ad™-2005: "IEEE Standard for Local and Metropolitan Area Networks --Virtual Bridged Local Area Networks -- Amendment 4: Provider Bridges".

NOTE: Available at https://standards.ieee.org/findstds/standard/802.1ad-2005.html.

[i.51] Void.

[i.52] IEEE 802.1X™-2010: "IEEE Standard for Local and metropolitan area networks -- Port-Based Network Access Control".

[i.53] BBF TR-384: "Cloud Central Office Reference Architectural Framework".

[i.54] R. Chaparadza, Tayeb Ben Meriem, Benoit Radier, Szymon Szott, Michal Wodczak, Arun Prakash, Jianguo Ding, Said Soulhi, Andrej Mihailovic: "SDN Enablers in the ETSI AFI GANA Reference Model for Autonomic Management & Control (emerging standard), and Virtualization Impact": In the proceedings of the 5th IEEE MENS Workshop at IEEE Globecom 2013, December, Atlanta, Georgia, USA.

[i.55] Kenneth J. Kerpez, John M. Cioffi, George Ginis, Marc Goldburg, Stefano Galli, and Peter Silverman: Software-Defined Access Networks: Article in IEEE Communications Magazine September 2014; DOI: 10.1109/MCOM.2014.6894466.

[i.56] ONF TS-025: "OpenFlow Switch Specification" Version 1.5.1 (Protocol version 0x06) March 26, 2015.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 195-2 [i.30] and the following apply:

access network: network that encompasses the elements of the broadband network from the NID at the customer premises to a Broadband Network Gateway

NOTE: This network typically includes one or more types of Access Node and can include an Ethernet aggregation function.

Access Node (AN): network node located in the access network, which can implement one or more access technologies based on copper, fibre or wireless

aggregation network: network segment that stretches from the Access Nodes to the Broadband Network Gateway(s)

NOTE: In the context of the present document the aggregation network is considered to be Ethernet based, providing standard Ethernet interfaces at the edges, for connecting the Access Nodes and Broadband Network Gateway(s), and some transport for Ethernet frames (e.g. Ethernet over SONET, MPLS, RPR, etc.) at the core.

autonomic networking: networking paradigm that enables network devices or elements (physical or virtual) and the overall network architecture and its management and control architecture to exhibit the so-called self-managing properties

NOTE 1: Autonomic networking includes: auto-discovery of information and entities, Self-configuration (auto-configuration), Self-diagnosing, Self-repair (Self-healing), Self-optimization, and other self-* properties.

NOTE 2: Autonomic Networking can also be interpreted as a discipline involving the design of systems (e.g. network nodes) that are self-managing at the individual system levels and together as a larger system that forms a communication network of systems.

NOTE 3: The term "autonomic" comes from the autonomic nervous system (a closed control loop structure), which controls many organs and muscles in the human body. Usually, human are unaware of its workings because it functions in an involuntary, reflexive manner - for example, human do not notice when their heart beats faster or their blood vessels change size in response to temperature, posture, food intake, stressful experiences and other changes to which human are exposed. And their autonomic nervous system is always working [i.4].

autonomically: by virtue of employing a control-loop (including feedback control-loop(s))

Broadband Network Gateway (BNG): access point to the provider's IP network for wireline broadband services

non-aggregated scenario: scenario of 3GPP architecture without the aggregation of other types of networks, e.g. previous generations of mobile networks

self-advertising: capability of a component or system to advertise its self-model, capability description model, or some information signalling message (such as an Ipv6 router advertisement message) to the network in order to enable other entities to discover it and be able to communicate with it, or to enable other entities to know whatever is being advertised

self-awareness: capability of a component or system to "know itself" and be aware of its state and its behaviours. Knowledge about "self" is described by a "self-model"

self-configuration: capability of a component or system to configure and reconfigure itself under varying and unpredictable conditions

self-descriptive: capability of a component or system to provide a description of its self-model, capabilities and internal state

self-organizing function: function that includes processes which require minimum manual intervention

self-protecting: capability of a component or system to be capable of detecting and protecting its resources from both internal and external attack and maintaining overall system security and integrity

self-regulation: capability of a component or system to regulate its internal parameters so as to assure a quality-of-service metric such as reliability, precision, rapidity, or throughput

3.2 Symbols

Void.

3.3 Abbreviations

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

AAA	Access, Authentication and Authorization
ACL	Access Control List
ACS	Access Control System
AF	Autonomic Function
AI	Artificial Intelligence
AMC	Autonomic Management & Control
AN	Access Node
ANEC	Access Node Externalized Control
ANLC	Access Node Localized Control
API	Application Programming Interface
APN	Access Point Name
ARP	Address Resolution Protocol
ASSIA	Adaptive Spectrum and Signal Alignment
BAA	Broadband Access Abstraction
BBF	BroadBand Forum
BNG	Broadband Network Gateway
BPCF	Broadband Policy Control Function
BRG	Bridged Residential Gateway
BS	Base Station
BSS	Business Support System
CEP	Complex Event Processing
CPE	Customer Premises Equipment
DBA	Dynamic Bandwidth Allocation
DE	Decision Element
DHCP	Dynamic Host Configuration Protocol
DMCF	Domain Management Coordination Function
DSL	Digital Subscriber Line
EM	Element Management
EMS	Element Management System
EPC	Evolved Packet Core
ERPS	Ethernet Ring Protection Switching
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FANS	Fixed Access Network Sharing
FB	Functional Blocks
FCAPS	Fault, Configuration, Accounting, Performance, Security
FI-WARE	European Commission funded project (called FI-WARE) under the Commission's R&D Framework Program FP7
FMC	Fixed Mobile Convergence
GANA	Generic Autonomic Network Architecture
GRE	Generic Routing Encapsulation
GW	GateWay
HD-TV	High Definition Television

IBM	International Business Machines (Corporation)
IETF	Internet Engineering Task Force
IFOM	IP Flow Mobility
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information eXport
IPoE	Internet Protocol over Ethernet
IPTV	Internet Protocol Television
IPv6	Internet Protocol version 6
KP	Knowledge Plane
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LDAP	Leightweight Directory Access Protocol
LSL	Logical Subscriber Link
LSO	MEF Lifecycle Service Orchestration
MAC	Medium Access Control
MANO	Management and Orchestration
MBTS	Model Based Translation Service
MCO	Management Control Orchestration (MCO)
ME	Managed Entity
MEF	Metro Ethernet Forum
MME	Mobility Management Entity
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
MUX	Multiplexer
NA	Not Applicable
NB	Node-B
NE	Network Element
NERG	Network Enhanced Residential Gateway
NFV	Network Function Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
NFVO	Network Functions Virtualisation Orchestrator
NM	Network Management
NPS	Net Promoter Score
NSWO	Non-Seamless WLAN Offload
OAM	Operations, Administration and Management
ONIX	Overlay Network for Information eXchange
OPEX	OPeration EXpenditure
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSS	Operation and Support System
OTT	Over The Top
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADR	PPPoE Active Discovery Request
PADS	PPPoE Active Discovery Session-confirmation
PADT	PPPoE Active Discovery Terminate
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PNF	Physical Network Function
PON	Passive Optical Network
PPP	Point of Presence Protocol
PPPoE	Point-to-Point Protocol over Ethernet
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RCA	Root Cause Analysis
RFC	Request For Comments
RG	Residential Gateway

RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
SDAN	Software Defined Access Network
SDN	Software Defined Networks
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SON	Self Organizing Networks
SP	Service Provider
SPML	Service Provisioning Markup Language
STP	Spanning Tree Protocol
TCP	Transfer Control Protocol
TCP/IP	Transfer Control Protocol/Internet Protocol
TV	Television
UE	User Equipment
VC	Virtual Circuit
VIM	Virtual Infrastructure Manager
VLAN	Virtual Local Area Network
VNF	Virtual Network Function
VNFM	Virtual Network Function Manager
VNO	Virtual Network Operator
VP	Virtual Path
WAN	Wide Area Network
WI-FI	IEEE 802.11 family of standards
WLAN	Wireless Local Area Network
WT	BBF Working Text
XML	eXtensible Markup Language
YANG	Yet Another Next Generation

4 Background and Introduction to the ETSI GANA Reference Model

4.1 Background

Autonomic Networking & Services Management is intended to help operators and enterprises in reducing OPEX and handling the increasing complexity of network Management. The ETSI AFI WG of TC NTECH produces specifications for the Autonomic Networking & Services Management, namely the Generic Autonomic Network Architecture (GANA) Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management; and its instantiations onto various reference network architectures and their associated management and control architectures to enable the implementation of autonomics, cognition and self-management in the architectures. The TC is now progressing in producing technical reports on instantiation of the GANA Reference Model onto existing reference network architectures and emerging ones to embed self-management capabilities in those reference network architectures and their associated management and control architectures. In GANA empowered autonomic and self-managed networks, self-management capabilities are realized by special autonomic management and control software components (called Decision Elements (DEs) in GANA) that implement cognitive algorithms and dynamically orchestrate and configure resources and parameters of the network to achieve self-configuration, self-diagnosis, self-healing, self-optimization, self-protection, and other self-* features.

Though the GANA model was validated in testbeds, a key step towards adoption of autonomics by the industry is to instantiate it onto a set of representative well-known reference architectures in order to enable launching pilot projects on concrete use cases. This is because many network architectures being deployed today do not intrinsically exhibit autonomicity and self-management capabilities, and industry needs to understand the implication of evolving them towards this technology.

The objective of the present document is to develop a Technical Report on the instantiation of the GANA model on the BBF Architecture specifications. More specifically, it is required to perform a mapping on fixed broadband access, aggregation network architectures and the convergence and integration of GANA with SDN/NFV.

The work has been divided into several tasks which are reflected in the following clauses. The first task consisted in defining the BBF reference architecture to be addressed. This is reported in clause 5. In a second step, a mapping of the

GANA model onto the BBF architecture was defined for the key components of the architecture. This is reported in clause 6. The final task consists in considering SDN/NFV convergence with GANA Functional Blocks in the same architecture consisting of GANA autonomics enabled network architecture and its associated management and control architecture. This will be reported in clause 7.

4.2 ETSI GANA Reference Model in Brief

To enable the reader to understand the GANA instantiation on the BBF network architectures and their associated management control architectures, the present clause provides a short overview of the GANA reference model specified in [i.30] and described in [i.8]. The GANA TS [i.30] is a concise description of the GANA as described in ETSI GS AFI 002 [i.2] but with additional aspects not found in ETSI GS AFI 002 [i.2].

The ETSI Generic Autonomic Networking Architecture (GANA) reference model specifies the concepts and principles defining the domain of autonomic communication, autonomic networking, autonomic and cognitive management and control-all as part of the "big-picture" of Self-Management. Figure 1 presents the GANA abstraction levels for self-management functionality at which interworking hierarchical/nested control-loops and their associated DEs can be designed. Figure 1 defines the key GANA Functional Blocks (FBs) for enabling and implementing autonomics in target implementation-oriented architectures, as described in clause 4.3. A table of a summary of all GANA FB reference points and characteristic information descriptions is given in clause 13 of ETSI GS AFI 002 [i.2]. The Reference points are further described in the present document. The GANA TS [i.30] also includes additional reference points that are not found in ETSI GS AFI 002 [i.2].

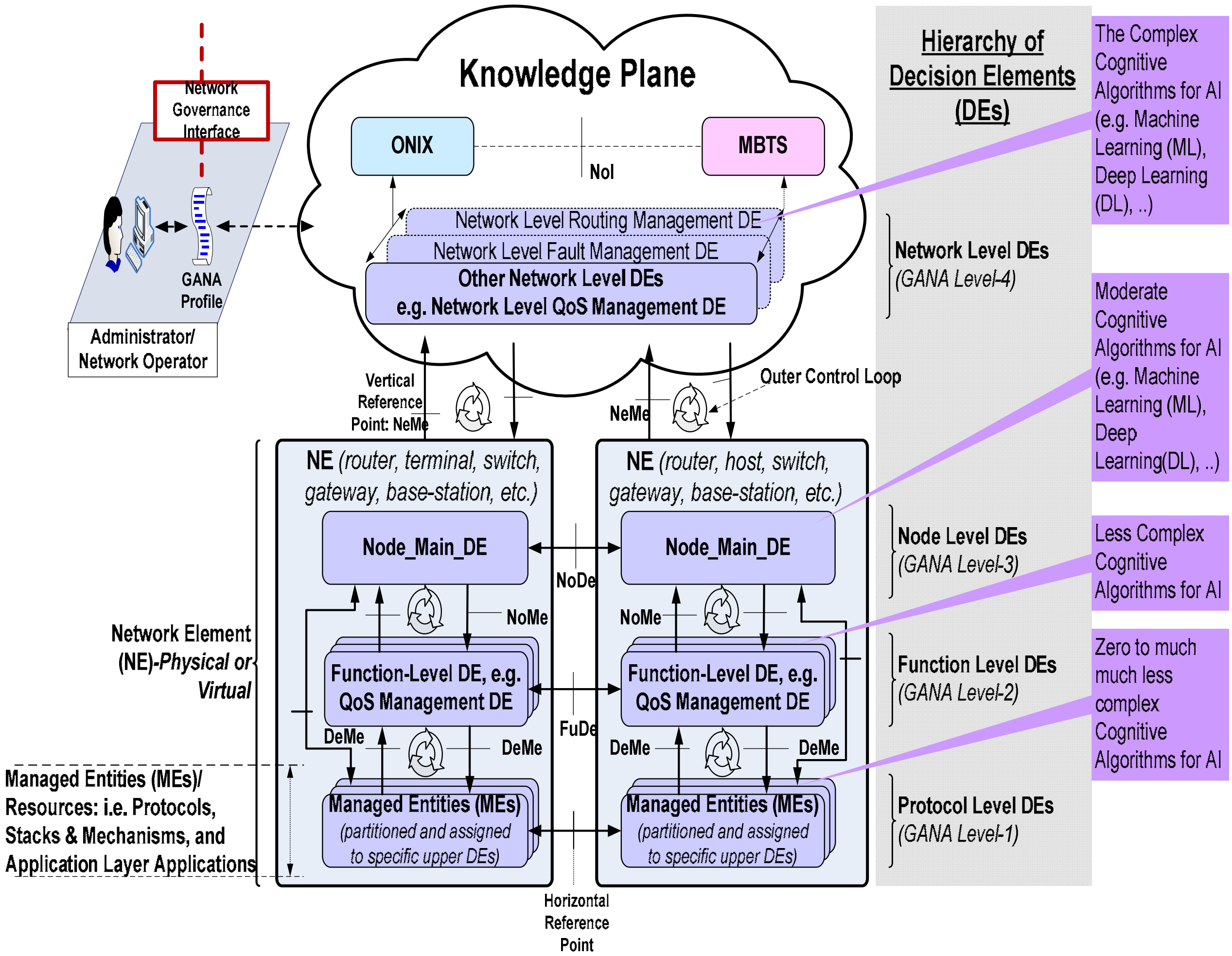


Figure 1: Snapshot of the GANA Reference Model

The GANA is a Reference Model for Autonomic Networking, Cognitive Networking and Self-Management. The aspects of autonomic networking, cognitive networking and self-management of networks and services are covered in GANA collectively as the AMC (Autonomic Management & Control) paradigm. AMC is about Decision Elements (DEs) as autonomic functions (logics that dynamically configure their associated managed entities in respective closed control-loops) with cognition introduced in the management plane as well as in the control plane (whether these planes are distributed or centralized) by virtue of introducing DEs in the planes.

Cognition (learning, analysing and reasoning used to effect advanced adaptation) in DEs, enhances DE logic and enables DEs to manage and handle even the unforeseen situations and events detected in the network.

Control (in "AMC") refers to the control-loop logic kernel of the DE, capable of dynamically adapting network resources and parameters or services in response to changes in network goals/policies, context changes and challenges in the network environment that affect service availability, reliability and quality.

DEs realize self-* features of a functionality or system (self-configuration, self-optimization, etc.) as a result of the decision-making behaviour of a DE that performs dynamic and adaptive management and control of its associated Managed Entities (MEs) and their configurable and controllable parameters. Such a DE can be embedded in a Network Element (NE) or higher at a specific layer of the outer overall network and services management and control architecture-thereby creating AMC architecture (composed of nested and hierarchically stacked DEs that can also collaborate horizontally across management and control planes). An NE can be physical or virtualized (such as in the case of the NFV (Network Functions Virtualisation) paradigm). Network functionality such as routing, forwarding, mobility management, etc. can be made autonomic by embedding a DE. DEs (as software components) are meant to empower the networks and the management and control planes to realize self-* properties: auto-discovery of information/resources/capabilities/services; self-configuration; self-protection; self-diagnosis; self-repair/heal; self-optimization; self-organization behaviours; as well as self-awareness.

Self-manageability in GANA is achieved through the dynamic and context-aware orchestration and management and control of MEs by collaborative Decision Elements (DEs) (see definition of an ME and a DE in clause 3.1). GANA defines a hierarchy of such DEs in four basic levels: the *"protocol", "function", "node", and "network*" levels. The levels are described in more detail in ETSI White Paper No.16 [i.1] and in ETSI GS AFI 002 [i.2]. At each level, a DE manages one or more lower-level DEs through a control loop. The lower-level DEs are therefore considered as Managed Entities (MEs) by the DE that controls them. Over the control loop, a DE sends commands, objectives, and policies to its lower-level DEs and receives feedback in the form of monitoring information or other type of knowledge. The Protocol Level DEs represent protocols, services, and other fundamental mechanisms running in the target network as MEs that can exhibit intrinsic control-loops (DE logic) and associated DE-as is the case for some of today's protocols such as OSPF, which can be considered an example of the instantiation of a protocol-level DE (though such autonomic-like feature in OSPF is not cognitive (learning and reasoning) in its operation and by design). Figure 1 indicates the levels (degree) of complexity in cognition (algorithms for Artificial Intelligence (AI)) that should be exhibited by DEs at a particular GANA Level (more details on this subject of cognition in DEs at the various GANA levels are found in [i.30]). As discussed in ETSI White Paper No.16 [i.1], the GANA Specification puts forward a recommendation to primarily focus on the three higher GANA levels of hierarchical control-loops (Level2 to Level4) when introducing autonomics in architectures and considers the protocol level DEs as MEs. The GANA hierarchy emphasizes only the three other levels, which should collaboratively work together. The argument, put forward in the ETSI White Paper No.16 [i.1] and ETSI GS AFI 002 [i.2], is that three levels of hierarchical control-loops (GANA level-2 to level-4) demonstrate how AMC can be gracefully (non-disruptively) introduced in today's existing networks and architectures and even in new network architectures that follow the approach of designing and employing protocols to build protocol stacks in which individual protocols are rather simple and do not embed any intrinsic control-loops.

At the lowest level in the management hierarchy in GANA is the resource layer in the Network Elements (NEs), which can be physical or virtual, that consists of Managed Entities (MEs) such as protocols or stacks, OSI layer 7 or TCP/IP application layer applications and other types of resources or managed mechanisms hosted in a network element (NE). They are managed by Function Level DEs (present in every Network Element, or NE) e.g. Routing Management DE. The orchestration of the Function Level DEs is performed by the Node Main DE. A Node_Main_DE is present in every NE, for example a router. At the highest DE level, the Network Level DEs address similar aspects as the Function Level DEs but on a wider scope. Therefore there is a Network Level Routing Management DE, Network Level Monitoring DE, Network Level QoS Management DE, etc. The GANA Knowledge Plane (KP) is constituted by the Network Level DEs, together with a distributed, scalable Overlay Network system of federated information servers for Information eXchange (ONIX) and a Model-Based-Translation Service (MBTS) for translating information and commands/responses towards NEs. The ONIX is useful for enabling auto-discovery of information/resources of an autonomic network via "publish/subscribe/query&find" protocols. DEs can make use of ONIX to discover information and entities (e.g. other DEs) in the network to enhance their decisions. More details on ONIX are given in the ETSI GS AFI 002 [i.2]. The ONIX itself does not have network management & control decision logic (as DEs are the ones that exhibit decision logic for AMC). MBTS (Model-Based Translation Service) is an intermediation layer between the GANA Knowledge Plane (KP) and the NEs (physical or virtual) for translating vendors' specific and technology specific raw data onto a common data model for use by network level DEs, based on an accepted and shared information model.

The GANA Knowledge Plane (GANA KP) enables advanced management & control intelligence at the Element Management (EM), Network Management (NM) and Operation and Support System (OSS) levels by interworking with them through their northbound interfaces or enhancing and evolving the intelligence of the systems at these levels by way of replaceable and (re)-loadable autonomics modules (DEs) that can be loaded at specific abstraction levels of management and control operations (more details in ETSI White Paper No.16 [i.1] and ETSI GS AFI 002 [i.2]).

Moreover, governance is implemented through the Network Governance Interface. The network administrator uses this interface to manage the operation of the whole autonomic network by authoring, validating and submitting conflict-free policies, high-level network objectives and some configuration data to the KP, all encapsulated together in the form of a "GANA Network Profile" that is generated using automation tools. This GANA Profile is then used by the Network Level DEs to configure themselves and issue commands and lower level policies that are issued to lower level DEs for enforcement (including relaying sub-profiles that are used by lower level DEs to configure themselves and their MEs). More details on the GANA Network Profile creations and use can be found in the ETSI GANA White Paper No. 16 [i.1] and ETSI GS AFI 002 [i.2]. The GANA Profile can be augmented/extended with run-time related information by the Network Level DEs and MBTS and stored/maintained in the ONIX.

4.3 Characterization of the GANA Knowledge Plane

1) The Knowledge Plane (KP) is an integral part of Management & Control Systems that provides for the space to implement complex network analytics functions performed by Decision Elements (DEs) that run as software in the Knowledge Plane and drive self-* operations such as self-adaptation, self-optimization objectives for the network and services by programmatically (re)-configuring Managed Entities (MEs) in the network infrastructure through various means possible: e.g. through the NorthBound Interfaces available at the OSS, Service Orchestrator, Domain Orchestrator, SDN controller, EMS/NMS, NFV Orchestrator, etc. In such interactions the Knowledge Plane DEs can employ the services of an MBTS (Model-Based Translation) set of software libraries as discussed in ETSI White Paper No.16 [i.1], as the MBTS enables management-protocol agnostic, control-protocol agnostic, and vendor-agnostic management and control of physical or virtual Network Elements (NEs) by the GANA Knowledge Plane. An *Intent-based language* for programming the network through the SDN controller that can provide such a northbound intent-based interface can also be applied by the GANA Knowledge Plane DEs in (re)-programming the network.

2) Various types of GANA Knowledge Plane's Decision-Elements (DEs) can be designed to perform autonomic management and control operations (the self-* operations) on various types of Managed Entities (MEs) in the network infrastructure network elements (virtualized (VNFs) or physical (PNFs)). DEs are representative of cognitive management & control "domains" of reasoning regarding specific management and control aspects. Example DEs that can be designed in the Knowledge Plane are:

   - Fault-Management-DE.
   - Resilience_&_Survivability-DE.
   - Auto-Configuration-DE.
   - QoS_&_QoE_&_Performance-Management-DE.
   - Security-Management-DE; Monitoring-DE.
   - Routing-Management-DE; etc.

A DE *monitors* Managed Entities (MEs) assigned to it by design, uses the monitoring data and any other input data from other data/information or policy sources in the environment to *analyse and compare the state of the MEs against the desired state* that is adaptively computed from certain objectives meant to be enforced by the DE (which can change any time based on e.g. context and policy changes, network conditions, manifestations of faults in the network, etc.), and then *creates a plan of actions or strategies to dynamically change the state and operations of the MEs*, and then *executes the actions/plans* to effect changes on the MEs. Such DE operations are performed reactively and/or proactively to meet desired objectives regarding the state or behaviours of MEs. Cognitive algorithms of a DE e.g. Machine Learning, Deep Learning, Computational Intelligence and other types of AI (Artificial Intelligence) algorithms, etc., drive the operations of the DE. ETSI GS AFI 002 [i.2] provides insights as to which levels in GANA should the DEs at that level need to have a higher degree of cognitive properties (cognition), as DEs at the Level-1 need to implement fast control-loops possibly with little or zero cognitive properties (cognition). Moving higher up the GANA levels-at DEs at Level-2, control-loops are fast in contrast to control-loops at Level-4 (outside of a GANA Node/NE) but slower than those at Level-1. However a certain degree of cognitive properties can be introduced in the Level-2 DEs. Moving higher up the GANA levels-at DEs at Level-3, control-loops are fast in contrast to control-loops at Level-4 (outside of a GANA Node/NE) but slower than those at Level-2 to some extent. However a much higher degree of cognitive properties than GANA Level-2 and Level-1 can be introduced in the Level-3 DEs. Moving higher up the GANA levels-at DEs at Level-4, control-loops become slower in contrast to control-loops at GANA Levels in the GANA Node/NE level, but the highest degree of cognitive properties than GANA Level-3, Level-2 and Level-1 collectively, can be introduced in the Level-4 DEs. So, in general, control-loops within the NE are fast control-loops (in terms of timescale of reactions to changes) while those outside, at the network-level (GANA Knowledge Plane level), are slower than those at NE level but with much very high degree of cognitive properties and wider (network-wide) views as scope on which the corresponding Network Level DEs operate on. ETSI GS AFI 002 [i.2] provides more insights on such design principles for DEs. GANA, as described in ETSI White Paper No.16 [i.1] and ETSI GS AFI 002 [i.2] and in the present document, provides guidelines on how to design DEs such that they coordinate their operations to avoid conflicts.

3) The GANA Knowledge Plane can perform the functions of traditional management and control systems usually performed by traditional OSS, NMS/EMS. If such a scenario is commercially viable e.g. for cases where no such traditional management systems are required anymore by a network operator, otherwise the Knowledge Plane should interwork with such traditional systems in driving the re-configuration (e.g. to realize Self-Optimization objective or Self-Healing Objective) of the network and services as can be deduced and deemed necessary by DE algorithms during the operation of the network. Another implementation option could involve DEs implemented to run as loadable modules of an OSS, otherwise the Knowledge Plane can integrate with the OSS via an OSS Northbound Interface.

4) The GANA Knowledge Plane should fulfil the combined role of Network Analytics Driven Service Orchestration and Network Analytics Driven Closed-Loop (Autonomic) Service Assurance:

- Network Analytics Driven Service Orchestration should be performed by the Knowledge Plane DEs in response to network or resource capacity demands and resilience targets/objectives.

- Network Analytics Driven Closed-Loop (Autonomic) Service Assurance should be performed by the Knowledge Plane DEs with the target of improving customer experience. Autonomic (Closed-Loop) Service Assurance involves the Knowledge Plane as an Analytics Platform equipped with engines (DEs) that collects and analyses data from various data sources such as traditional Service Assurance Platforms (e.g. Performance management systems), network service functions/nodes, SDN Controllers, etc., and detect any service degradations and SLA violations. The Analytics Platform then closes the loop by communicating monitor results to Orchestrators and triggering remediation and corrective operations via a combination of Service Orchestrators, SDN Controllers, and Service Functions/Nodes such as CPE (Customer Premises Equipment), Access Node, BNG in Broadband Forum (BBF) architectures, and other types of service function nodes of other types of architectures. The Knowledge Plane DEs should be able to communicate to a Service Orchestrator Results obtained from Monitoring a Service such as SLA violations and generate Recommendations (actionable insights) on how the problems can be solved. For example humans could make use of the generated Recommendations, e.g. making use of the Recommendations to perform the actions if the Knowledge Plane DEs are configured to operate in an "Open-Loop" Mode. At the same time in a "Closed-Loop" mode, the DEs should go further on their own accord to trigger operations on the Service Orchestrators (which include orchestrator types like the NFV Orchestrator) in a "Closed-Loop" (autonomic) service assurance goal based on what the DEs determine to trigger on an orchestrator or any other management and control system such as an SDN controller, so as to realize Self-Healing of the Service(s)-thanks to autonomics of the Knowledge Plane operations. While Service Assurance should now evolve towards "Closed-Loop" (Autonomic) Service Assurance, rather that the Service Assurance Function computing Recommendations as actionable insights and operate in a an open loop as discussed in [i.21] and in [i.27], the GANA Knowledge Plane is meant to be an implementation of a Service Assurance Function that is *autonomic* in its operation, acting in a Closed-Loop fashion that drives Self-* behaviours (performed on the Managed Entities (MEs) of the network) such as *Self-Healing, Self-Organizing, Self-Optimizing, Self-Protection, Self-Repair, etc., and exhibiting Self-Awareness*.

- Offer insights that help the Operator to create and launch new types of services that could be offered to customers based on the Recommendations that the Analytics performed by DEs in the Knowledge Plane can produce with respect to the types of services (e.g. connectivity services) that can be provisioned over the capacity deduced to be available without compromising QoE (Quality of Experience) of end users currently served by the network. The Recommendations should be based on converged and aggregate analytics that are collectively correlated by the various DEs in the Knowledge Plane over historical usage trends of the E2E network capacity and other information such as performance trending data, etc.

5) The GANA Knowledge Plane (KP) is meant to provide the realm in which Decision Elements (DEs), as software, can be designed and implemented to perform and realize the following functions:

- Network Analytics should be performed in the Knowledge Plane (KP) using various types of algorithms for reactive and predictive analytics, including Machine Learning, Deep Learning, Computational Intelligence and others types of cognitive algorithms such as Artificial Intelligence (AI) algorithms, in augmenting any network analytics performed at systems and platforms such as Data Collectors that feed generated knowledge into the Knowledge Plane. Some cognitive algorithms can also run on the ONIX Information Servers for further correlation of information stored in the ONIX, to maintain an updated view on knowledge pertaining to current state of the network and also knowledge pertaining to historical network state and decisions performed by DEs as historical traces. The analytics performed by KP DEs can then drive network maintenance operations, but can also be used to drive marketing campaigns that can help the network operator to automatically innovate new service offering to customers based on the Knowledge Plane's recommendations(as also discussed in [i.20]). Sources such as [i.22], [i.23] and many other sources in literature provide insights on data-sources for network analytics that can be performed on analytics platforms such as Data Collectors or at some management systems to generate some knowledge that can be supplied to the Knowledge Plane. The Knowledge Plane DEs can augment the knowledge by consolidating such knowledge and further performing aggregate analytics of information and knowledge from various input sources on a more global level. Cognitive algorithms discussed in [i.22] and many other sources on Knowledge Plane related topics, including results from research projects on autonomics and cognitive network management, and also some real implementations already achieved to some degree in the industry in the areas of Service Assurance and Big-Data Analytics Driven network management can also be applied in implementing the GANA Knowledge Plane and its interfaces described in [i.1].

- Complex Event Processing (CEP) techniques are employed by DEs in the Knowledge Plane, as discussed in [i.1].

- Data collected in the network by probes in the NEs or probes specially instrumented to collect data such as traffic captured through means such as link tapping, should be made available to the Knowledge Plane DEs for the purpose of enabling their algorithms to perform optimization and diagnostics.

6) The ONIX Information Servers and services can be employed for realizing a **Real-Time Inventory**.

7) The GANA KP should be aware and make of the following items:

    - SLAs, for use in determining SLA Violations and autonomically programming the network in order to guarantee and sustain acceptable levels of QoS and QoE for user traffic.

    - Application policy/Profile profiles.

    - Network Service Designs/graphs.

Other characteristics of the GANA Knowledge Plane: KP Multi-Tenancy can be required for some networking scenarios that require multi-tenancy in the management and control software responsible for portions, slices and administrative domains in the End-to-End network architecture.

5 Instantiation of the GANA model onto the BBF reference network and management & control architectures

5.1 BBF Reference architectures considered

The identification of the reference architecture for the BBF is based on BBF TR 101 [i.6]. It provides an architectural/topological model of an Ethernet based aggregation network that supports the business requirements in BBF TR 058 [i.47]. In doing so it describes requirements for protocol translation and interworking, QoS, multicast, security, and OAM for a DSL aggregation network.

Figure 2 shows the BBF reference architecture.

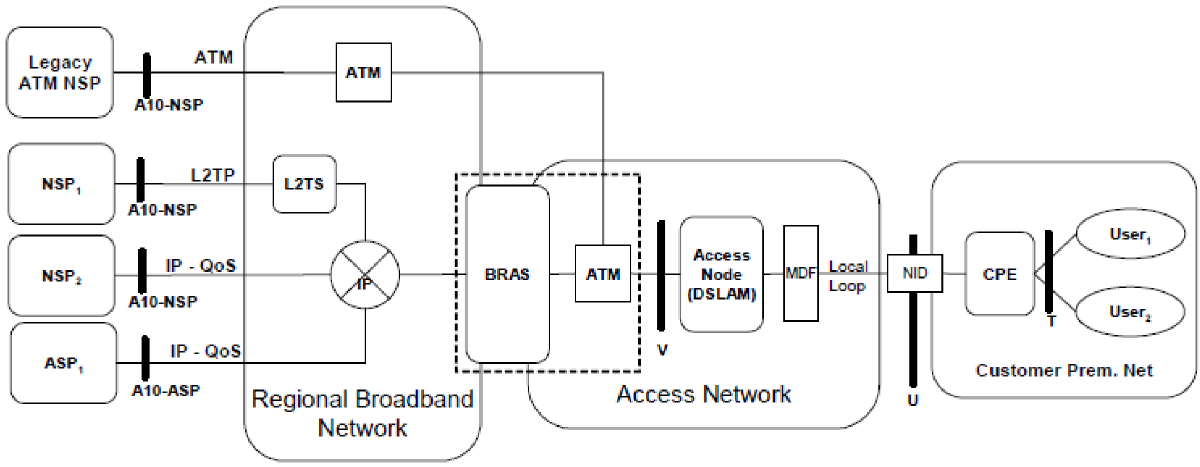


Figure 2: Reference BBF architecture

Moreover, BBF TR 145 [i.48] extends the BBF TR 101 [i.6] architecture with new technical requirements needed to fulfil the business requirements laid out in BBF TR 144 [i.49] Broadband Multi-Service Architecture and Framework Requirements. It defines an architectural framework based upon functional modules and the logical interfaces between them, the high-level common network service requirements as well as end-to-end operational functions, such as control and OAM. It focuses on the data plane between the T and A10 reference points and provides the interfaces and connectivity to Policy Control and Management Systems via interfaces across the R and M reference points, respectively. It results to the generic Functional BBF model depicted in Figure 3.

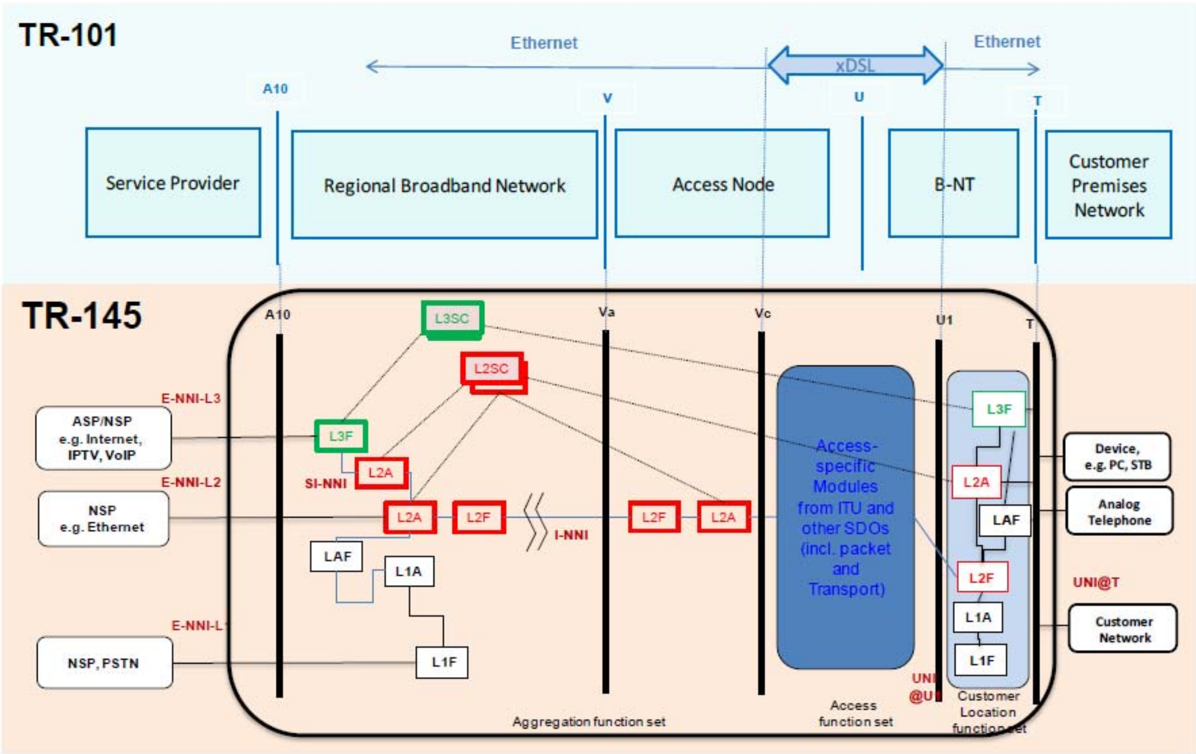


Figure 3: Generic Functional BBF model

6 Instantiation of GANA model concepts onto BBF architecture key functional entities

6.1 General considerations derived from BBF Specifications for introducing autonomics in BBF architectures

6.1.1 Requirements for autonomic features in BBF functional entities

The key requirements for autonomic features in BBF entities are summarized in the following tables namely, Table 1, Table 2 and Table 3. The tables refer to requirements extracted from BBF TR 101 **[**i.6**]**, related to CPE, BNG and AN, respectively, and can be addressed/automated through autonomic means by DEs.

Table 1: Identification of CPE related requirements [i.6]

R1	Bandwidth on Demand and QoS on demand can be supported by leveraging policy at the CPE
R2	Multicast upstream IGMP messages to all or a configured subset of the WAN interfaces
R3	Forward messages to all provisioned interfaces
R4	Configure which ports are allowed to have IGMP hosts
R5	Configurable Customer maintenance domain level
R6	Auto-configuration of CPE
R7	All the Functional Entities of the node that require that Reactive and Proactive Resilience and Survivability should be reasoned about and handled on the node-level: • Software/firmware image management • Software module management • Dual homing
R8	Security and authentication of CPE with ACS/OSS/Service configuration, subscriber isolation
R9	Diagnostics
R10	Auto-configuration of CPE
R11	Software/firmware image management Software module management Dual homing
R12	Security and authentication of CPE with ACS/OSS/Service configuration, subscriber isolation
R13	Diagnostics
R14	Status and performance monitoring
R15	Session Control - Connection request, Subscriber management function, Scheduling and Traffic Filtering function
R16	Marking on tunnels, QoS Interworking between fixed and 3GPP networks, per customer QoS
R17	VLAN management, multicast resource control, L1/L2 Adaptation and Forwarding
R18	Multicast routing, selection of duplicate streams, separation of customer traffic
R19	Dynamic service provisioning, service integrity, service instance tags used, traffic profiles, service association

Table 2: Identification of BNG related requirements [i.6]

R1	Auto-configuration of DHCP relay (makes it possible for DHCP (responsible for broadcasting messages to be sent over routers that do not support forwarding of DHCP messages) on selected interfaces.
R2	QoS support mechanisms: a) Hard partitioning of bandwidth among the Broadband Network Gateways. b) Distributed precedence and scheduling - mark services according to a Layer 2 precedence relationship so lower classes will be dropped under congestion. c) Hierarchical Scheduling (HS) within a BNG-allotted bandwidth partition.
R3	Policy Management. Configuration of RADIUS server.
R4	ARP processing. Configuration of "Local Proxy ARP" mode: routing IP packets received from host X on this interface to host Y (X and Y are in subnet Z) back via the same interface.
R5	Subscriber Session Establishment and Verification.
R6	Source IP spoofing: only respond to user ARP requests when they originate with the proper IP source address.
R7	Monitoring Tools and Mechanisms of the device: Status and performance monitoring.
R8	Network Management: define constraints on the range of VLAN, auto-sense PPP/PPPoE as well as IPoE, auto-sense S-VLAN-tagged and C-VLAN-tagged frames Ethernet frames.
R9	Support dynamic adjustment of the user-facing QoS shapers (Multicast).
R10	IEEE 802.1.ad [i.50] support.
R11	Multicast resource control, L1/L2 Adaptation and Forwarding.
R12	Policy: ingress policing per: user, VLAN, session/flows.

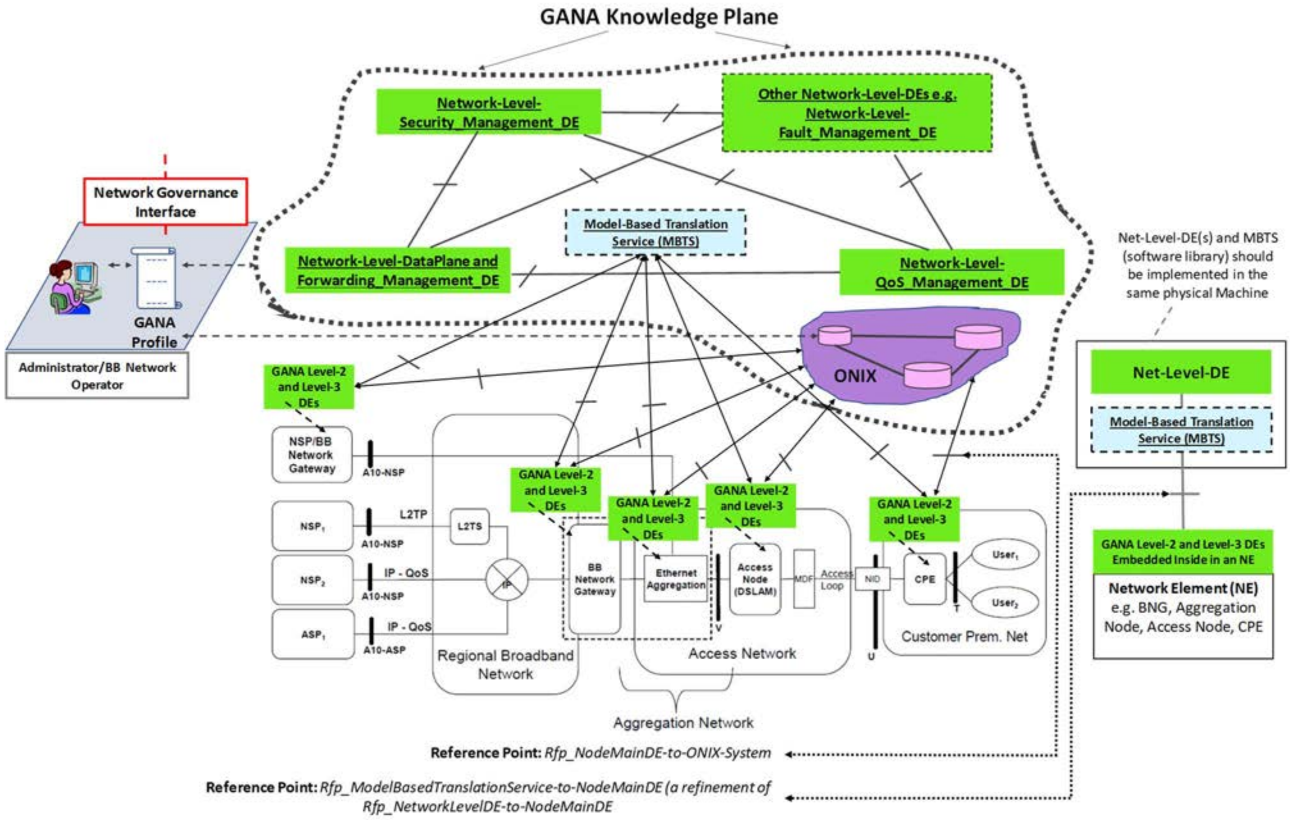
Table 3: Identification of AN related requirements [i.6]

R1	Auto-configuration of the access nodes
R2	Auto-discovery of access nodes and other nodes
R3	Bulk provisioning (default configuration of customer ports)
R4	Ethernet interfaces configuration
R5	PON interfaces (DBA configuration)
R6	xDSL port (profiles configuration)
R7	Software upgrade
R8	Dual-homing
R9	Link-Aggregation
R10	ACL configuration & traffic filtering (broadcast, mac address filtering & flooding)
R12	Control-plane protection
R13	Diagnostics/Hardware fault detection and report
R15	Ethernet OAM
R16	Synchronization
R17	DHCP/PPPoE relay
R18	IGMP snooping/proxy for multicast forwarding
R19	Traffic classification
R20	Queue configuration (buffer allocation)
R21	MTU
R22	Auto-sensing of protocol encapsulation
R23	VLANs handling & forwarding
R24	Multicast forwarding
R25	MPLS adaptation module
R26	Routing protocols

6.2 GANA instantiation onto BBF architectures

6.2.1 Instantiation (Mapping) of GANA DEs onto BBF key architecture Network Elements (NEs)

Following the main approach for the mapping of the GANA model onto BBF architecture, there is a high-level view for the instantiation of the GANA Knowledge plane and network level DEs that can be depicted in Figure 4.



NOTE: The Reference Points on the diagram are defined in clause 13 of ETSI GS AFI 002 [i.2].

Figure 4: Generic overview for the mapping of GANA to BBF architecture

6.2.2 Enabling Autonomic behaviour of the CPE (Autonomic CPE)

In order to enable the CPE to exhibit autonomic capabilities the mapping (instantiation) of GANA DEs at the node and function levels of abstraction of self-management functionality defined in GANA is required. The mapping follows the requirements analysis and links the GANA DEs to node operations, functions and managed entities (e.g. protocols) for the CPE node. Table 4 addresses the mapping.

Table 4: Mapping of GANA DEs to CPE node functions and managed entities

Decision Element (DEs)	The CPE Functions - Managed Entities (MEs)
NODE_LEVEL_AC_DE - Node-Level Auto-Configuration Decision-Element	Auto-configuration of CPE
NODE_LEVEL_R&S_DE - Node-Level Resilience & Survivability Decision-Element	All the Functional Entities of the node that require that Reactive and Proactive Resilience and Survivability should be reasoned about and handled on the node-level: • Software/firmware image management • Software module management • Dual homing
NODE_LEVEL_SEC_DE Decision-Element	Security and authentication of CPE with ACS/OSS/Service configuration, subscriber isolation
NODE_LEVEL_FM_DE - Node-Level Fault-Management Decision-Element	Diagnostics
FUNC_LEVEL_MON_DE - Function-Level Monitoring Decision-Element	Monitoring Tools and Mechanisms of the device - Status and performance monitoring
FUNC_LEVEL_GCP_M_DE - Function-Level Generalized Control Plane-Management Decision-Element	Initialization and control of the provisioning session flow. **Session Control** - **Connection request,** Subscriber management function, **Scheduling and Traffic Filtering function**
FUNC_LEVEL_QoS_M_DE - Function-Level Quality of Service-Management Decision-Element	Marking on tunnels, QoS Interworking between fixed and 3GPP networks, per customer QoS
FUNC_LEVEL_DP&FWD_M_DE - Function-Level DataPlane&Forwarding-Management Decision-Element	VLAN management, multicast resource control, L1/L2 Adaptation and Forwarding
FUNC_LEVEL_RT_M_DE - Function-Level Routing-Management Decision-Element	Multicast routing, selection of duplicate streams, separation of customer traffic
FUNC_LEVEL_SM_DE - Function-Level Service-Management Decision-Element	Dynamic service provisioning, service integrity, service instance tags used, traffic profiles, service association

The Autonomic CPE is depicted in Figure 5.

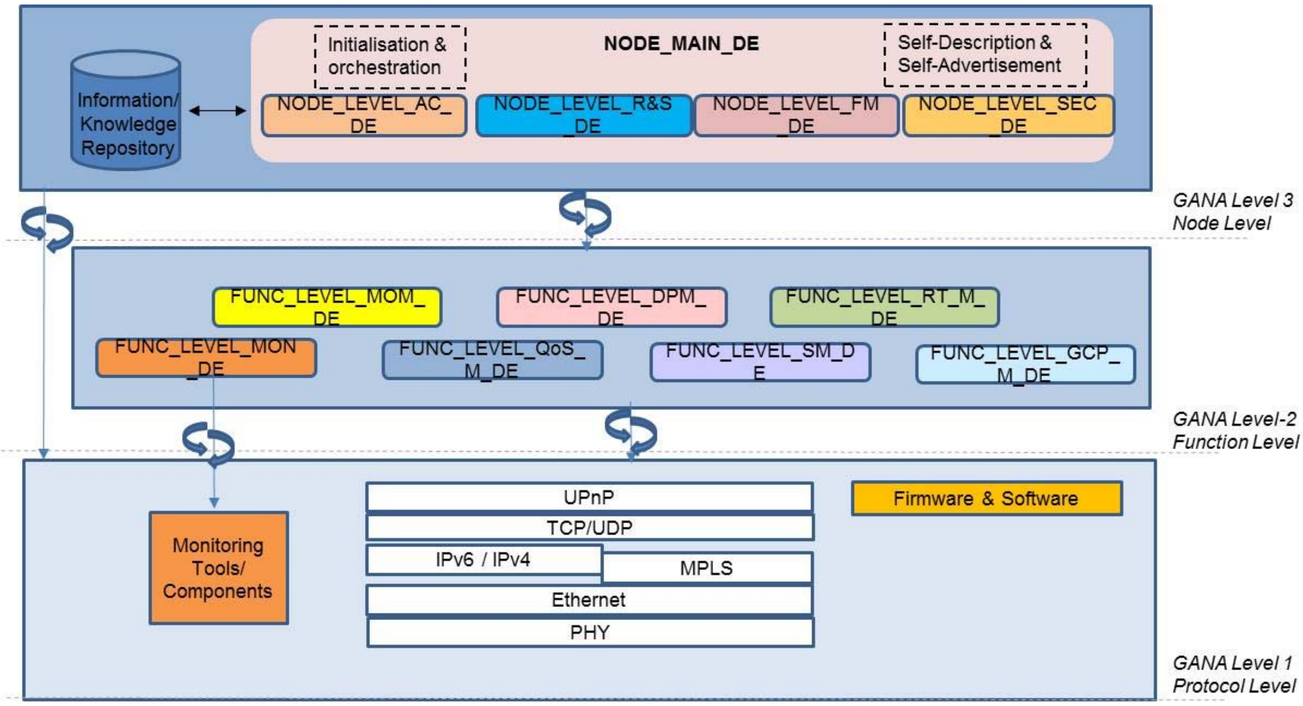


Figure 5: Mapping of GANA DEs to BBF CPE

6.2.3 Enabling the BNG to exhibit au+tonomic behaviours (Autonomic BNG)

In order to enable autonomic capabilities to the BNG the mapping of GANA DEs for node and functional level is required. The mapping follows the requirements analysis and links the GANA DEs to node operations, functions and managed entities (e.g. protocols) for the BNG node. Table 5 addresses the mapping.

Table 5: Mapping of GANA DEs to BNG node functions and managed entities

Decision Element (DEs)	The BNG Functions - Managed Entities (MEs)
NODE_LEVEL_AC_DE - Node-Level Auto-Configuration Decision-Element	Auto-configuration of BNG: • DHCP Relay on/off • ARP processing • OAM messaging • Configuring RADIUS Server • Activating Control Policy • Establishing Subscriber Sessions • Deploying QoS • Configuring Subscriber Features • Verifying Session Establishment
NODE_LEVEL_R&S_DE - Node-Level Resilience & Survivability Decision-Element	
NODE_LEVEL_SEC_DE - Node-Level Security Decision-Element	Source IP spoofing: only respond to user ARP requests when they originate with the proper IP source address
NODE_LEVEL_FM_DE - Node-Level Fault-Management Decision-Element	Diagnostics
-	
FUNC_LEVEL_MON_DE - Function-Level Monitoring Decision-Element	Monitoring Tools and Mechanisms of the device: Status and performance monitoring
FUNC_LEVEL_GCP_M_DE - Function-Level Generalized Control Plane-Management Decision-Element	Initialization and control of the provisioning session flow. DHCP Relay: The Broadband Network Gateway should be able to function as a DHCP relay agent on selected trusted interfaces. Network Management: defines constraints on the range of VLAN, auto-sense PPP/PPPoE as well as IPoE, auto-sense S-VLAN-tagged and C-VLAN-tagged frames Ethernet frames
FUNC_LEVEL_QoS_M_DE - Function-Level Quality of Service-Management Decision-Element	Should be able to perform at least 3-level Hierarchical Scheduling (Session, VC, Group of VCs, VP and port) Support dynamic adjustment of the user-facing QoS shapers (Multicast)
FUNC_LEVEL_DP&FWD_M_DE - Function-Level DataPlane&Forwarding-Management Decision-Element	IEEE 802.1ad [i.50] support multicast resource control, L1/L2 Adaptation and Forwarding ARP proxy
FUNC_LEVEL_RT_M_DE - Function-Level Routing-Management Decision-Element	Multicast routing Policy: ingress policing per: user, VLAN, session/flows

6.2.4 Enabling the AN to exhibit autonomic behaviours (Autonomic AN)

In order to enable autonomic capabilities to the access node (AN) the mapping of GANA DEs for node and functional level is required. The mapping follows the requirements analysis and links the GANA DEs to node operations, functions and managed entities (e.g. protocols) for the access node. Table 6 addresses the mapping.

Table 6: Mapping (Instantiation) of GANA DEs onto AN node functions and managed entities

Decision Element (DEs)	The AN Functions - Managed Entities (MEs)
NODE_LEVEL_AC_DE - Node-Level Auto-Configuration Decision-Element	Auto-configuration of Access Nodes Auto-discovery of Access Nodes and others nodes Bulk provisioning Ethernet interfaces PON interfaces (DBA configuration) xDSL ports (profiles configuration)
NODE_LEVEL_R&S_DE - Node-Level Resilience & Survivability Decision-Element	Software upgrade Dual-Homing Link Aggregation RSTP/MSTP
NODE_LEVEL_SEC_DE - Node-Level Resilience & Survivability	ACL configuration Traffic filtering (broadcast, mac address filtering& flooding) Control-plan protection
NODE_LEVEL_FM_DE - Node-Level Fault-Management Decision-Element	Diagnostic tools Hardware faults detection and report
FUNC_LEVEL_MON_DE - Function-Level Monitoring Decision-Element	OAM Synchronization
FUNC_LEVEL_GCP_M_DE F Function-Level Generalized Control Plane-Management Decision-Element	DHCP relay PPPoE Relay IGMP snooping/ proxy
FUNC_LEVEL_QoS_M_DE - Function-Level Quality of Service-Management Decision-Element	Traffic classification Queue configuration (buffer allocation) MTU
FUNC_LEVEL_DP&FWD_M_DE - Function-Level DataPlane&Forwarding-Management Decision-Element	Auto-sensing of protocol encapsulation VLANs handling VLAN forwarding (1:1 or 1:N) MPLS Adaptation Module Multicast forwarding
FUNC_LEVEL_RT_M_DE - Function-Level Routing-Management Decision-Element	Routing protocols
FUNC_LEVEL_SM_DE E - Function-Level Routing-Management Decision-Element	

The Autonomic AN is depicted in Figure 6.

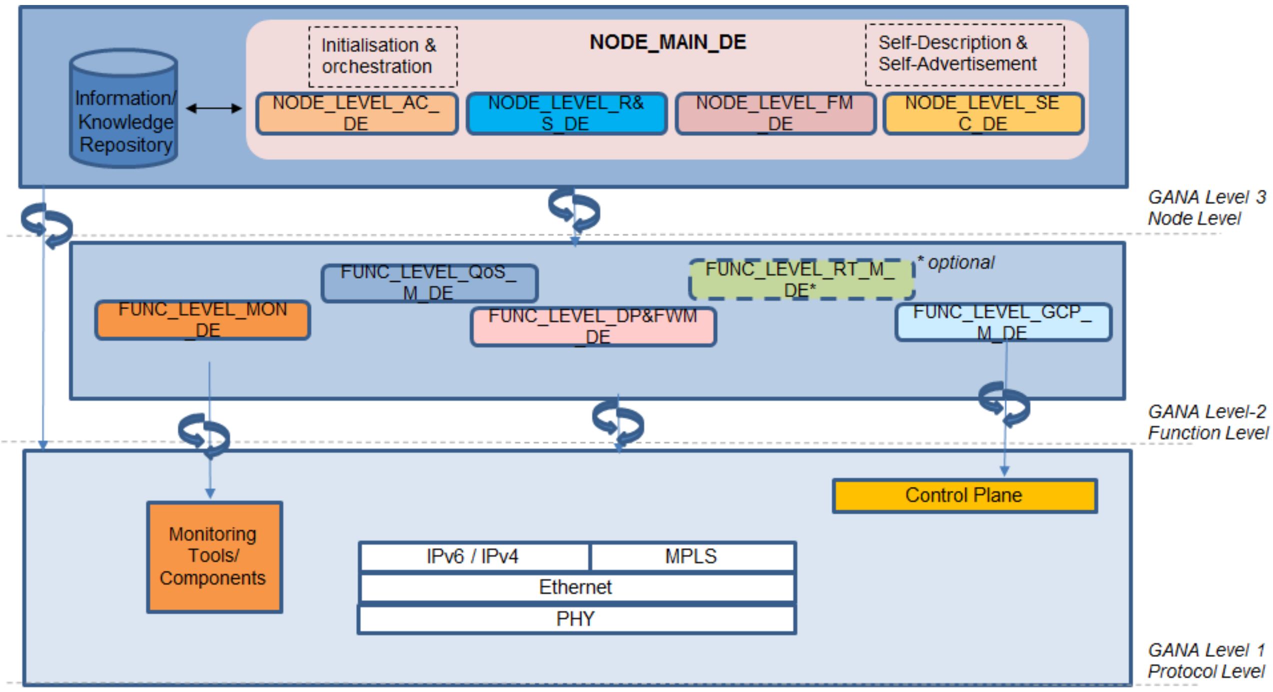


Figure 6: Instantiation (Mapping) of GANA DEs to BBF AN

6.2.5 Use Cases for illustrating the value of autonomic features in BBF network elements

6.2.5.1 Use Case 1 (CPE): QoS interworking between fixed and 3GPP networks, marking of tunnels based on user-specific policy, network policy and QoS setting

A subscriber can want to use an application on his mobile device, while outside the Home Network, and then wishes to change the device he is using to a fixed Home Network attached device. A multimedia call is handed over from the mobility macro network to a home network, but instead of remaining on the same device, the user chooses to transfer the multimedia call to a Media Device connected to a large screen TV display and resumes the call on that device. Bandwidth and QoS is maintained for the large screen experience to be meaningful. Accounting and settlement is supported between the application and network service providers.

It is assumed that the IMS system will initially perform the necessary transfer of the initial UE session from the mobile access network to the Home Network (e.g. WI-FI). The IMS Service Continuity procedures will be initiated.

In order to transfer the multimedia call to the Media device, Inter-UE Transfer procedures will be executed. In this case, the whole IMS multi-media session is transferred from one UE to the other UE with the support of CPE which will have to reallocate the flow to the new device.

CPE will have to:

- Consider the service profile and QoS requirements.
- Enable dynamic service provisioning, service integrity, by using service instance tags.
- Correlate traffic profiles with service association.
- Perform Session Control, Subscriber management, Scheduling and Traffic Filtering.
- Perform Marking on tunnels, QoS Interworking between fixed and 3GPP networks, per customer QoS.

6.2.5.2 Use Case 2 (BNG): BNG termination of PPPoE

The BNG allows hosts with private IP addresses to access the Internet. It mainly includes the following functions:

- Maintains the mapping from the private IP address to the public IP address (auto-configuration).
- Terminates PPPoE subscriber sessions with private IP address to public IP address to access Internet.

PPPoE has two phases, the discovery phase and the session phase:

- Discovery: The client identifies the servers which are available. "To complete the phase the client and server must communicate a session-id". During the discovery phase all packets are delivered to the PPPoE control plane (FUNC_LEVEL_GCP_M_DE).
- PPPoE Active Discovery Initiation (PADI). This packet is broadcasted and used by the client to search for an Access Concentrator (access server), providing access to a service.
- PPPoE Active Discovery Offer (PADO): If the access server is able to provide the service it should respond with a unicast PADO message to signal the client. Multiple servers can respond and the client can choose a server to connect to.
- PPPoE Active Discovery Request (PADR): After the client receives a PADO, this unicast packet will be used to connect to a server and request service.
- PPPoE Active Discovery Session-confirmation (PADS): A server may respond to the client with this unicast packet to establish the session and provide the session-id. Once the PADS was provided the PPP phase begins.

Session: Once the session ID is established connectivity is available for the duration of the session. Either client or server can terminate a session. During the life of the session the packets may be uniquely identified by the client's MAC address and session-id. The session can terminate either by PADT sent by the client or server or by an LCP Terminate-Request packet.

6.2.5.3 Use Case 3 (AN): Configuration of the xDSL ports

DSL technologies are widely used to provide triple-play services including high-speed Internet, voice over IP and television over IP. These services are requiring more and more bandwidth and copper technology is pushed to its limits.

At the same time, quality of service (QoS) is one of the main concerns of telecom operators that aim to find a compromise between line performances and line stability knowing that copper line characteristics may change over time. This comprise is part of a global QoS policy that is defined by each operator and that may also change over time.

As a consequence, DSL profiles applied to each DSL port of access nodes may have to be changed from time to time. This action can be done automatically by access nodes according to both line characteristic and global QoS policies.

NOTE: Changing DSL profiles leads to a desynchronization and resynchronization of the DSL modem. During this time, triple-play services are not available for the customers. As a consequence, this modification should be done at the most appropriate moment of the day.

AN should perform the following in an autonomic fashion:

- Analyse the stability of each xDSL line.
- Choose the best profiles according to global QoS policies (stability vs performances).
- Analyse port traffic statistics in order to determine the most appropriate moment for the modifications.
- Apply the new policy at the most appropriate moment for the modification to be transparent for the customers.

6.2.5.4 Use Case 4 (AN): Buffer configuration

Quality of service (QoS) is one of the main concerns of telecom operators and latency, throughput and packet loss are key performance indicators. Some services require low latencies and can support packets loss. Other services can support bigger latencies but throughput can decrease dramatically in case of packet loss.

In order to ensure a good quality of service, QoS policies (including buffer configuration) should be enforced in the network in an end-to-end approach depending on each service requirements.

AN should perform the following in an autonomic fashion:

- Determine the type of traffic that goes into each queue on each interface.
- Communicate with other devices in the network in order to have an end-to-end buffer configuration policy.
- Configure buffer size per queue depending on services requirements and global network QoS policy.

6.2.6 The role of Monitoring DEs in enabling dissemination of monitoring data to the DEs within NE and DEs in the Knowledge Plane

This clause summarizes the role played by the Function-Level-Monitoring Management-DE (FUNC_LEVEL_MON_DE) and Network-Level-Monitoring Management-DE (NET_LEVEL_MON_DE) in complementarily working together to enable dissemination of monitoring data or Knowledge derived from the monitoring data to the DEs within NE and DEs in the Knowledge Plane.

Role played by the Function-Level-Monitoring Management-DE (FUNC_LEVEL_MON_DE)

As defined and described in the GANA Specification (ETSI TS 103 195-2 [i.30]), the FUNC_LEVEL_MON_DE provides logic and algorithms to orchestrate monitoring MEs or to (re)-configure them, and to retrieve information from various potential sources of monitoring data and information in order to intelligently cause dissemination of monitoring data needed by DEs within the node to the local DEs by causing the Monitoring MEs to disseminate the monitoring data required by the local DEs or to register the DEs to receive monitoring data or information of interest to them if available through the Monitoring DE itself. The Monitoring DE also pushes monitoring data to external Data Collectors of the network.

Within an autonomic NE such as Autonomic CPE, Autonomic AN, or Autonomic BNG, the Function-Level-Monitoring-DE is expected to perform automated configuration and dynamic(adaptive) (re)-configuration or orchestration of Monitoring related Managed Entities (MEs) in order to achieve certain objectives such as the gathering and optimal dissemination of various types of monitoring data to entities that need to act upon the monitoring data in order to effect changes in network behaviours or other objectives (targets). The Monitoring-DE's behaviour is based on reacting to the following dynamics:

- feedback on network and the DE's ME(s) state (continuously observed/monitored) and experienced challenges in the network (manifestations of faults, errors, failures, security attacks);
- changes in human operator policies and operational context;
- monitoring-data demands from other types of entities (e.g. other autonomic manager components); or
- workload changes.

Function-Level-Monitoring Management-DE (FUNC_LEVEL_MON_DE)

Managed Entities (MEs) of the DE:

- Monitoring Protocols, Mechanisms and Tools (e.g. for traffic monitoring, context inference and derivation, etc.). Example of protocols and mechanisms that are mapped as MEs of the DE: IPFIX data collection and dissemination mechanisms, SNMP data collection and dissemination mechanisms, NETFLOW data collection and dissemination mechanisms, Protocol Analysers, Packet Trace creation and dissemination mechanisms. Effective and available bandwidth estimation mechanisms, IPv6 hop-by-hop options for intrinsic monitoring, etc.

NOTE 1: For some insights on how to implement the Function-Level-Monitoring Management-DE (e.g. how to design the DE logic and algorithms, etc.), the GANA Specification (ETSI TS 103 195-2 [i.30]) provides more details.

NOTE 2: A Function-Level-Monitoring Management-DE (FUNC_LEVEL_MON_DE) could be implemented as an integral part of a Probe (e.g. a Passive Monitoring Probe, Active Monitoring Probe or one that combines active probing and passive probing aspects) if the Probe is embedded with an NE and has a scope of being a NE-scoped (node-scoped) Monitoring Probe.

Role played by the Network-Level-Monitoring Management-DE (NET_LEVEL_MON_DE)

As defined and described in the GANA Specification (ETSI TS 103 195-2 [i.30]), the NET_LEVEL_MON_DE provides logic and algorithms to retrieve monitoring data from various sources, to derive context information, to dynamically orchestrate and regulate monitoring mechanisms and tools of the network and the rate (e.g. sampling rate) at which they create monitoring data and disseminate the data to entities that need the monitoring data (e.g. DEs). The granularity and formats in which monitoring data and/or knowledge presentation is created by monitoring mechanisms and tools and disseminated to data collectors and to entities that directly consume the monitoring data or knowledge are all determined by the Monitoring DEs at the Function-Level and Network-Level collaboratively. The Network-Level Monitoring-DE policies the behaviours of Function-Level-Monitoring Management-DEs that dynamically orchestrate and autonomically manage Monitoring Protocols, Mechanisms and Tools of their respective GANA nodes. In orchestrating and managing the mechanisms and tools for disseminating monitoring data, context and knowledge to other DEs in the Knowledge Plane, the Network-Level-Monitoring Management-DE is supposed to orchestrate and dynamically manage and control the kinds of mechanisms and tools for the dissemination of monitoring data, context or knowledge that complement the ONIX and (amc)-MBTS as information/data/knowledge disseminators.

In collaboration with the Function-Level-Monitoring Management-DEs the Network-Level-Monitoring Management-DEs performs automated configuration and dynamic(adaptive) (re)-configuration or orchestration of Monitoring related Managed Entities (MEs) in network nodes (NEs) in order to achieve certain objectives such as the gathering and optimal dissemination of various types of monitoring data to entities that need to act upon the monitoring data in order to effect changes in network behaviours or other objectives (targets). The Monitoring DE's behaviour and actions are computed and executed based on the following aspects:

- policing a node's own autonomic Monitoring management intelligence in form of policy control by the outer logically centralized "autonomic manager" component;
- reacting to feedback on network and the DE's ME(s) state (continuously observed/monitored) and experienced challenges (manifestations of faults, errors, failures, security attacks) in the network;
- changes in human operator policies and operational context, monitoring-data demands from other types of entities (e.g. other autonomic manager components);
- workload changes.

Network-Level-Monitoring Management-DE (NET_LEVEL_MON_DE)

DEs, Protocols and Mechanisms as Managed-Entities (MEs):

- Function-Level-Monitoring Management-DEs (are policy-controlled by the network-level-DE through their respective Node-Main-DEs); and also Monitoring Protocols, Mechanisms and Tools (e.g. for traffic monitoring, context inference and derivation, etc.) that may need to be orchestrated and dynamically managed at the network level by the Network-Level-Monitoring Management-DE rather.

Examples of protocols and Mechanisms that are mapped as MEs of the DE:

- IPFIX data collection and dissemination mechanisms, SNMP data collection and dissemination mechanisms, NETFLOW data collection and dissemination mechanisms, Protocol Analysers, Packet Trace creation and dissemination mechanisms. Effective and Available Bandwidth Estimation mechanisms, IPv6 Hop-by-Hop Options for network-intrinsic monitoring, etc.

NOTE 3: For some insights on how to implement the Network-Level-Monitoring Management-DE (NET_LEVEL_MON_DE) (e.g. how to design the DE logic and algorithms, etc.), the GANA Specification (ETSI TS 103 195-2 [i.30]) provides more details.

NOTE 4: A Network-Level-Monitoring Management-DE (NET_LEVEL_MON_DE) could be implemented as an integral part of a Probe (e.g. a Passive Monitoring Probe, Active Monitoring Probe or one that combines active probing and passive probing aspects) if the Probe is external to an NE and has a scope of being a Network-Wide Monitoring Probe.

NOTE 5: The MBTS, as described in the GANA Specification ETSI TS 103 195-2 [i.30], does transform monitoring data received from NEs into knowledge that it then disseminates to Knowledge Plane DEs and stores into the ONIX as well. Moreover, the Network-Level-Monitoring Management-DE (NET_LEVEL_MON_DE) should complement this knowledge derivation process and could be implemented to also act as a Data Collector in the Knowledge Plane (KP) that collects various monitoring data and derives knowledge that it then disseminates to the other KP DEs. However, Standalone Data Collectors of the network should also implement Analytics Algorithms that derive knowledge from the gathered data (e.g. monitoring data) and supply the knowledge to Knowledge Plane DEs. This can be done by streaming the knowledge, as discussed in the ETSI White Paper No. 16 [i.1], in the context of the architecture on integration of GANA Knowledge Plane with other paradigms, namely, SDN, NFV, E2E Service Orchestrators, and Big-Data, etc.

7 GANA instantiation onto the virtualized BBF architecture with SDN

7.1 Background

The BBF SDN enabled architecture and the BBF and ETSI NFV architectures are addressed in the context of instantiating the GANA model features into the respective virtualized component architectures. The concepts are aligned with the Unified Architecture for the ETSI GANA Model, SDN, NFV, E2E Service Orchestration, Network Analytics, and Big-Data Analytics for Autonomics that is discussed in the ETSI White Paper No.16 [i.1] and [i.3], which offers insights on the integration of the GANA with these paradigms (readers are encouraged to learn more details on this subject in the more elaborate work being done in ETSI NTECH AFI on this subject). Figure 7 is one of the diagrams that show how GANA integrates with the other emerging paradigms, but the focus here is on depiction of where Autonomic Functions (AFs) or Decision Elements (DEs) can be introduced in the ETSI NFV Architectural Framework within the Multi-Tenancy Platform. The green circles in Figure 7 depict AFs (DEs) as embedded Local Closed Control loops, whereas the GANA Knowledge Plane in the light green box is embedding the Network-level DEs (Outer/Centralized Closed Control loops). Hence, GANA Knowledge Plane interacts with ETSI NFV NFVO, MEF/LSO (an example of an E2E Service Orchestrator), SDN controllers (Hybrid SDN) and OSS/BSS for the purpose of empowering them with Autonomics capabilities by allowing the GANA Knowledge Plane to be the realm to implement the complex cognitive algorithms that use knowledge from such systems as information/data sources and program the network infrastructure through those systems. With this respect, GANA Knowledge Plane can be seen as an application interacting with those mentioned components via their Northbound APIs (blue arrows).

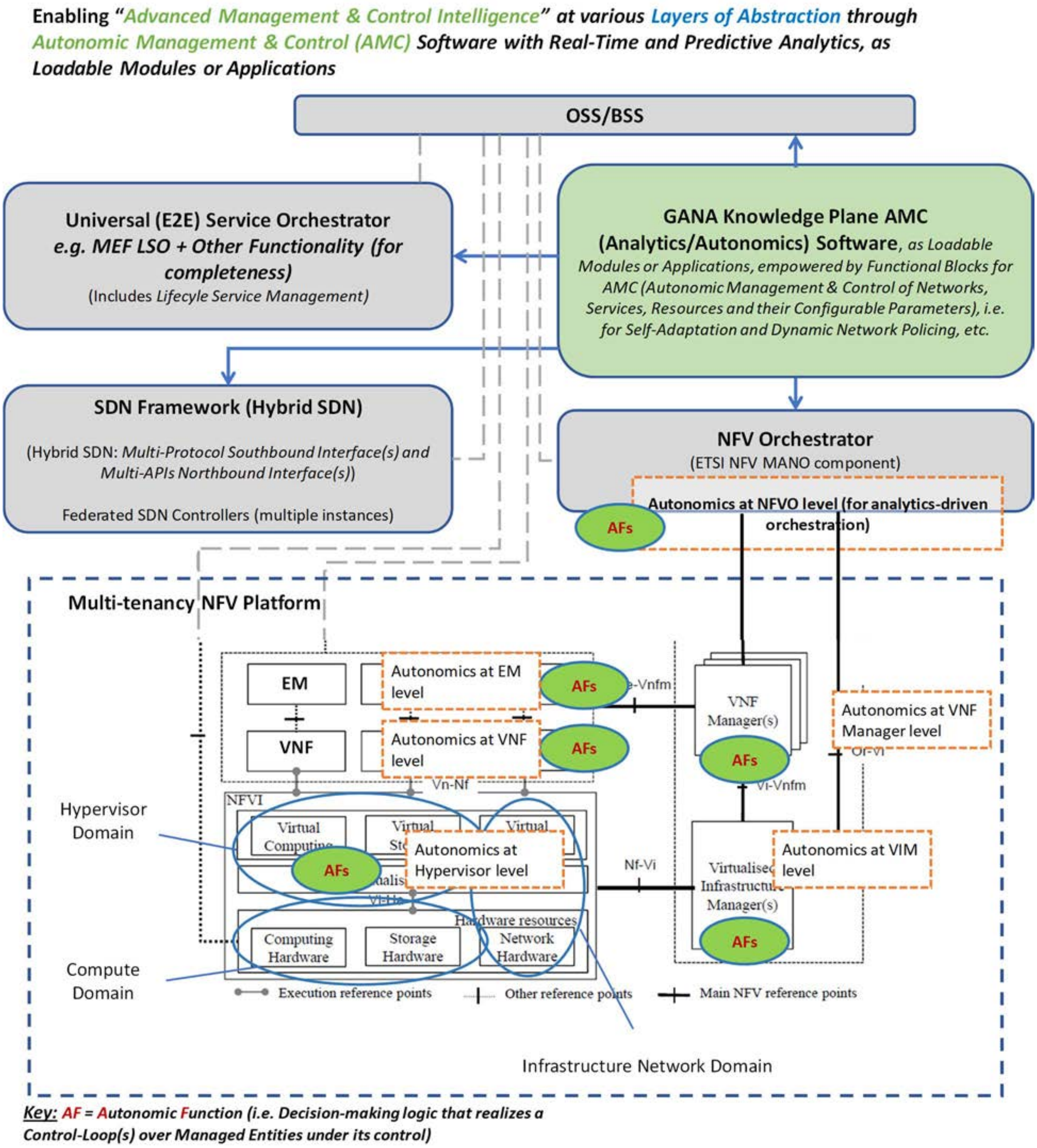


Figure 7: Introduction of GANA Autonomic Functions (Decision Elements) in the ETSI NFV Architectural Framework [i.3]

7.2 GANA instantiation onto the BBF and ETSI-NFV reference model for infrastructure interworking

7.2.1 Combining BBF and ETSI NFV architectures

Figure 8 illustrates a combination of the BBF and ETSI-NFV architectures where the services are hosted in NFVI that has deployed a BBF specified multiservice broadband network. On this scenario, the infrastructure layer(s) will typically be a combination of MPLS and Ethernet augmented with datacentre overlay protocols (e.g. VxLAN) in the services infrastructure domain (e.g. NFVI). The network function view of the network service layer is assumed to be IP based with the selection of the corresponding forwarding graph of the network service layer. As BBF TR 359 [i.8] indicates, the diagram does not account for when NFVI deployments span BBF reference points (i.e. A10, V, U, T). In addition, a NFVI-PoP can exist between reference points (e.g. between U and V).

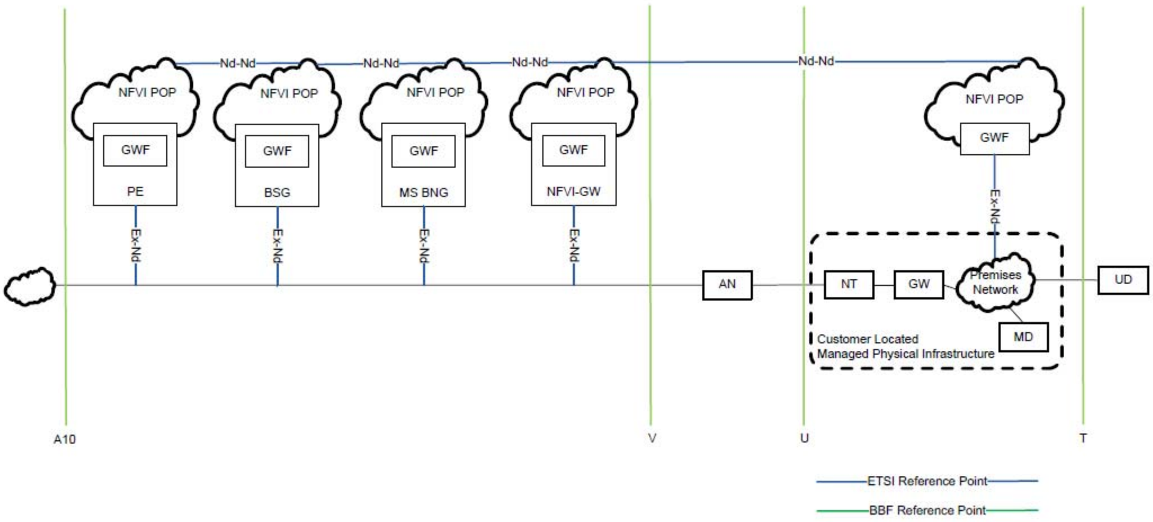


Figure 8: BBF and ETSI-NFV reference model for infrastructure interworking [i.10]

Figure 9 shows an example of Network Enhanced Residential Gateway (NERG) architecture deployed on top of ETSI NFV architecture.

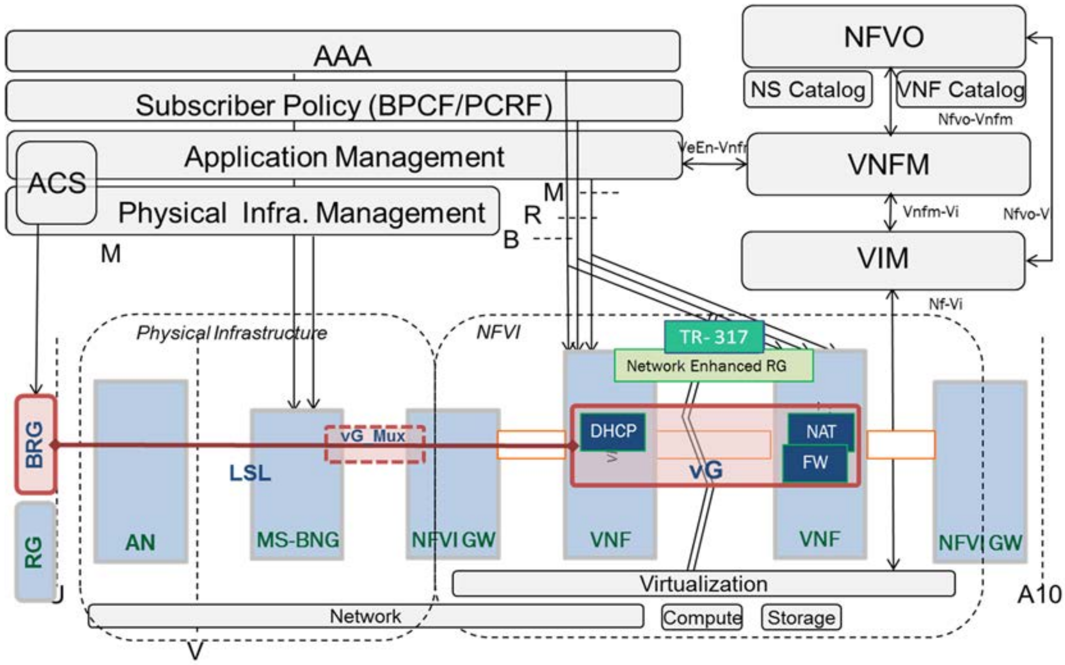


Figure 9: NERG Example (Home Virtualization)

The reference models of the BBF and ETSI NFV can be combined such that the functional components and reference points of the BBF TR 145 [i.48] and TR 134 [i.9] reference models and ETSI NFV reference model are depicted for the management and control of Services along with the interworking of the user/data plane of the BBF reference models with the infrastructure (NFVI) layer of the ETSI NFV reference model.

With the intention of GANA instantiation, in Figure 10, the Managed Entities (MEs) of both BBF and NFV architectures are identified and GANA Network Level and GANA Node Levels MEs are illustrated.

BBF TR 359 [i.8] describes the Domain Management Coordination Function (DMCF), as a set of Customer and Resource Facing services, which provides the management functions needed to maintain the "desired state" of functions within a specified domain.

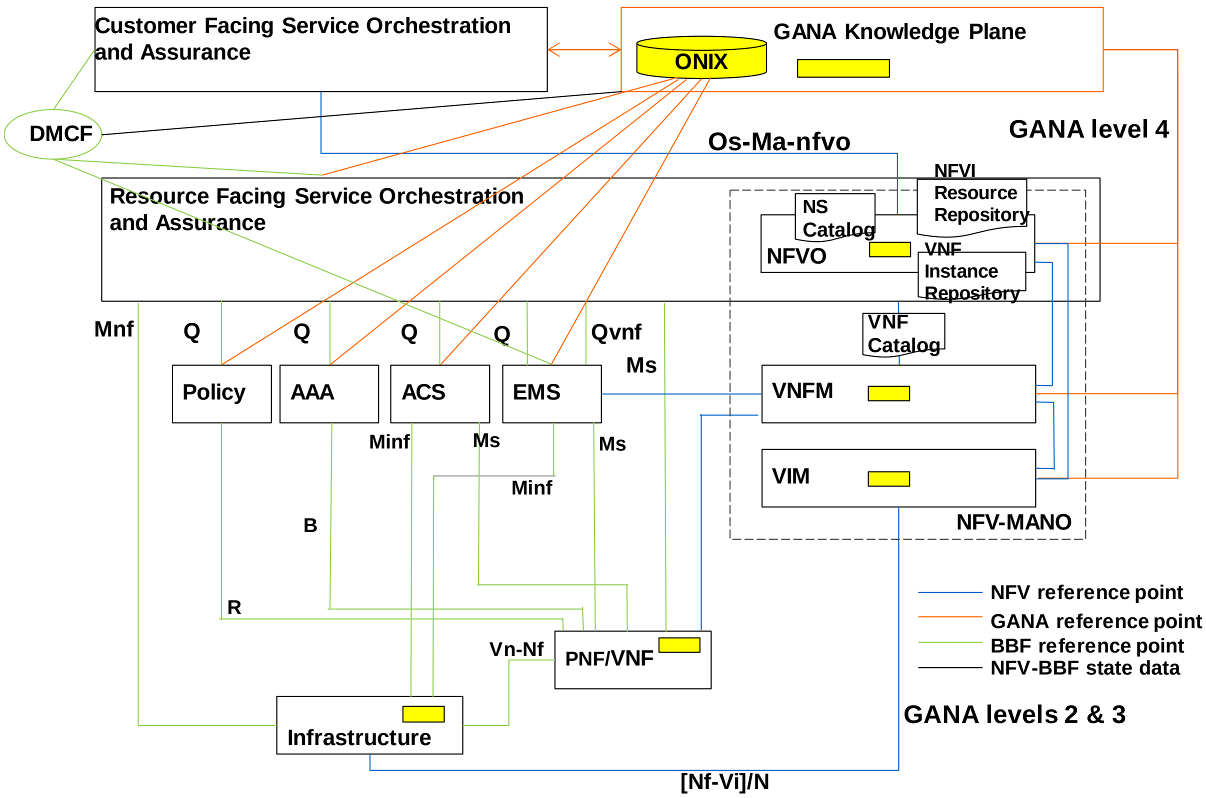


Figure 10: BBF and ETSI-NFV reference model for service management and control

7.2.2 BBF Managed Entities (MEs)

This clause describes the BBF MEs and their assignment to specific GANA DEs to enable DE developers to identify DE to MEs mappings in order to innovate and develop DE algorithms that dynamically and collaboratively manage and control MEs.

Table 7: Correlation of DEs and BBF Managed Entities (MEs)

Decision Element (DEs)	Auto configuration server (ACS) Managed Entities (MEs)
ACS NODE _LEVEL_AC_DE	The first time a BRG contacts the operator's network, not all of the functions associated with the NERG can be activated on the BRG and within the vG. As such, when the BRG contacts the ACS for the first time, the **ACS informs the NERG** management system which then can activate **additional functions**.

Decision Element (DEs)	Authentication Authorization and Accounting (AAA) Managed Entities (MEs)
AAA NODE_LEVEL_SEC_M_DE	AAA is used in NERG architecture at different nodes and for different purposes: • At the MS-BNG: – in the case of the Flat Ethernet LSL, to extend the subscriber's access VLAN to the vG_MUX, by dynamically cross-connecting the Access-VLAN to an L2 network resource such as a VxLAN, an MPLS pseudo-wire or an Ethernet over GRE tunnel; – in the case of the Overlay Ethernet LSL, to provide the BRG with the necessary tunnelling information via DHCP to allow the BRG to connect to vG_MUX. In this case, the tunnelling information is encoded in a set of new RADIUS Attributes and translated into a set of DHCP options. • At the vG_MUX: – to extend the LSL from the vG_MUX to the subscriber's vG, the LSL being either a Flat Ethernet LSL or an Overlay LSL.

Decision Element (DEs)	Policy Managed Entities (MEs)
Policy NODE_LEVEL_SEC_M_DE	For the offering of per device services and policy management (e.g. per device QoS or steering). Out of scope in BBF TR 317 [i.28].

7.2.3 NFV Managed Entities (MEs)

7.2.3.1 Overview of the Mapping of GANA model to ETSI NFV MANO

Figure 11 describes the NFV ME and their relationship with GANA DEs. The DEs of the GANA Knowledge Plane are autonomic functions (AF) that are supposed to autonomically manage and control the Managed Entities (MEs) that determine the services of a network node (e.g. a VNF or PNF), e.g. its protocols/stacks instances and/or other functional entities and their configurable parameters. That means GANA Knowledge Plane DEs can be loaded or integrated as modules of an EMS or implemented as part of EMS or OSS in general (similarly, this could apply as a means to empower MANO components namely, NFVO, VNFM and VIM). EMS and OSS vendors can offer an interface through which GANA Knowledge DEs (as customized or second party control logics that embed autonomics-enabling algorithms) can be loaded or integrated to introduce/enhance autonomics capabilities of the EMS or OSS. Other than DEs, the other GANA Knowledge Functional (FBs) such as ONIX and MBTS, can also be implemented and integrated in order to take advantage of the functions they offer in an autonomic network. Autonomics (AMC) on the Orchestrator Level, VNF Manager level, VIM Level [i.29].

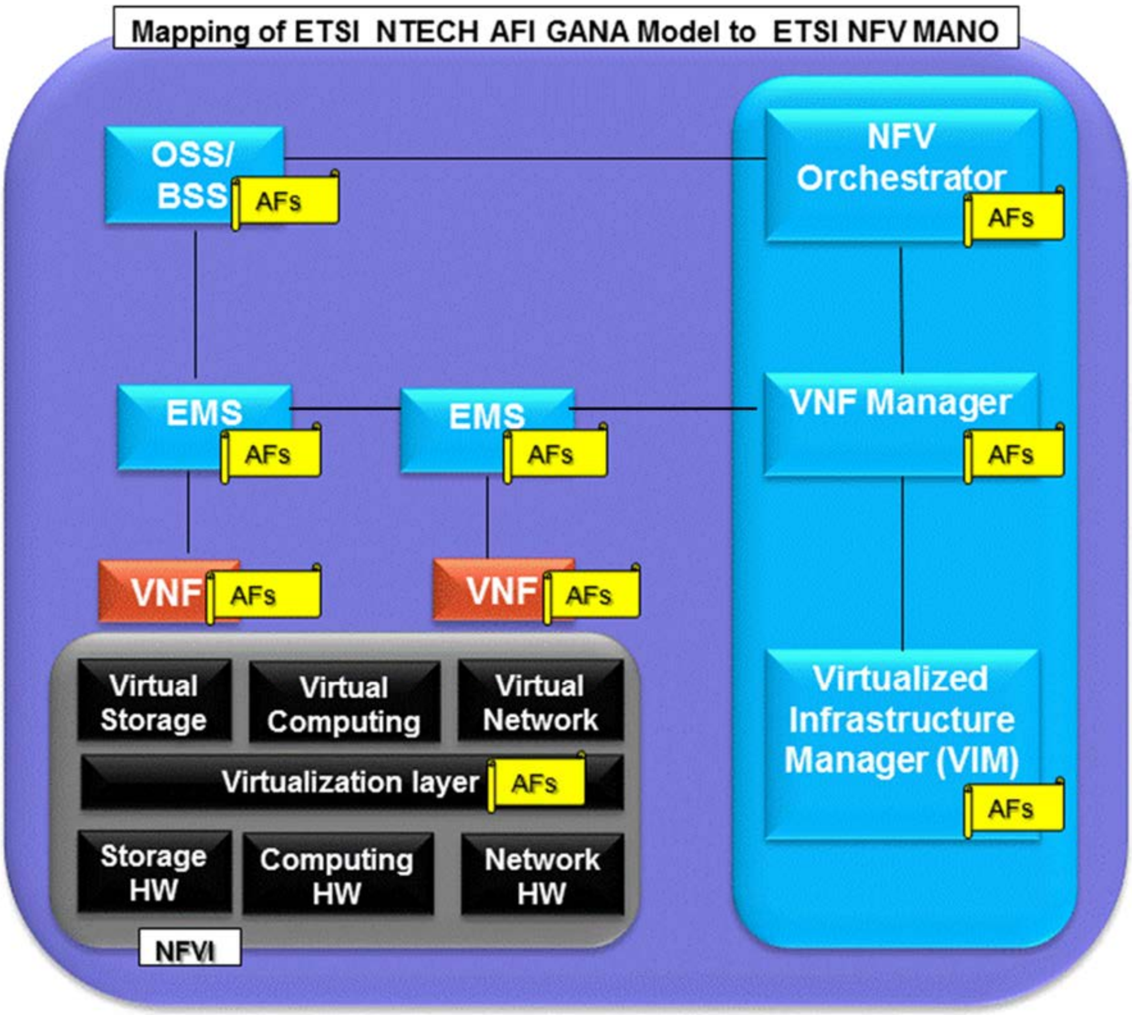


Figure 11: Mapping of GANA model to ETSI NFV MANO

Table 8 provides a global picture of GANA mapping to ETSI NFV MANO architecture with the instantiation of autonomic functions (AF). It includes the following four perspectives:

- Autonomics at ETSI MANO level.
- GANA DE role in terms of performing analytics, creating and executing plans of actions wrt Managed Entities (ME).
- ETSI MANO lower level Components involved (Managed Entities).
- Autonomic Control-loop's operating region (decision making coverage).

Table 8: Diagram of the Mapping of GANA model to ETSI NFV MANO [i.29]

Autonomics at ETSI MANO level	GANA Decision Element (DE) performs analytics, Creates & Executes plans of action that control via Policies/Configurations /Commands lower levels (Managed Entities: MEs)	ETSI MANO lower level components (Managed Entities) (MEs)	Autonomic Control Loop's operating region
OSS	GANA Knowledge Plane (KP) Decision Elements (DEs) are modules that perform the analytics	EMS	Network & Other Views input to OSS level
EMS	GANA Knowledge Plane (KP) Decision Elements (DEs) are modules that perform the analytics	VNFs	Network & Other Views input to EMS level
VNF	GANA-Level-2 and Level-3 Decision Elements (DEs) instrumented in the VNF	e.g. protocols/stacks instances	through its logical-links or to events local to the VNF (e.g. faults/errors/failures
NFVO	GANA-Network-Level Decision Element (DE) (NFVO-DE as module that is *part of Orchestrator SW* and *is controled and augmented by GANA KP DEs' algorithms*	VNFM, VIM	Network & Other Views input to NFVO level
VNFM	GANA-Network-Level Decision Element (DE) (VNFManager-DE as module that is part of VNFManager SW)	VNFs	Network & Other Views input to VNFM level
VIM	GANA-Network-Level Decision Element (DE) (VIM –DE as module that is part of VIM SW)	Infrastructure resources	Network & Other Views input to VIM level
Hypervisor	GANA-Network-level Decision Element (DE) (Hypervisor –DE as module ,part of Hypervisor SW)	Physical resources for Compute, Storage, Network	Platforms views input at Hypervisor level

7.2.3.2 Overview of the Mapping of GANA model to ETSI NFV MANO: GANA Autonomics at NFV-O level and at VIM Level

Table 8a: Correlation of DEs with NFV MEs at NFV-O and VIM Levels

Decision Element (DEs)	NFV-O Managed Entities (MEs)
Data_Plane_and_Forwarding_Management_DE	Service Function Chaining, across multiple network applications.
Security_Management_DE	Tenant session management.
QoS_Management_DE	Generates, maintains and tears down network services of VNF themselves. If there are multiple VNFs, orchestrator will enable creation of end to end service over multiple VNFs.

Decision Element (DEs)	VIM Managed Entities (MEs)
NODE_LEVEL_SEC_M_DE	Security profiles enable scalable deployment through dynamic, template-driven policy management.
NODE_LEVEL_FM_DE, NODE_LEVEL_RS_DE	Fault detection in hypervisors and storage volumes.

7.2.4 GANA Autonomics (Autonomic Management and Control) in the BBF CloudCO Architeture

7.2.4.1 GANA Autonomics in CloudCO Environment in context of end to end service orchestration

Based on BBF TR-384 [i.53], the integration of the GANA autonomics into the CloudCO environment is illustrated in Figure 12. This is based on GANA integration with the CloudCO Environment in context of end to end service orchestration as depicted in figure-8 of BBF TR-384. The focus here is particulary to reveal the integration of the GANA Knowledge Plane (KP) with the systems involved in the management and control of the CloudCO environment, while depicting where GANA Levels 2 and 3 DEs can be injected as software logics that enhance intelligence in a PNF or VNF. The case considered here is one that assumes the involvement of SDN in the CloudCO environment.

The systems shown to be interfacing(integrating) with the GANA Knowledge Plane (KP), as taken from figure-8 of BBF TR-384 [i.53], namely: the legacy mngmt (management); CloudCO Domain Orchestrator; BSS-OSS; other legacy mngmt; E2E Service Orchestrator; and SDN domains, should all be viewed collectively as data sources or events sources by the GANA Knowledge Plane. This is because the GANA KP is supposed to be the center of consolidated knowledge about the network and intelligence for autonomic and cognitive management and control of the network infrastructure based on data and knowledge and events obtained from the various systems by the GANA Knowledge Plane. Also because Complex Event Processing (CEP) over events from the various systems is to be performed by the GANA Knowledge Plane as discussed in ETSI White Paper No.16 [i.1] and GANA Technical Specification [i.30]. And in turn, the GANA Knowledge Plane DEs may dynamically and selectively fire commands (thanks to the cognitive and analytics algorithms employed by the KP DEs) into any or some of the systems. This depends on the target systems the GANA KP DEs determine should be used by the DEs' attempt to adaptively and intelligently instantiate, scale-in, scale-out or program the PNFs and VNFs of the underlying network infrastructure.

For example, the GANA Knowledge Plane can fire commands into the E2E Service Orchestrator in attempts to achieve analytics-driven orchestration, as may be determined by the Decision Elements (DEs) of the Knowledge Plane. Another possibility is that the KP could fire commands through the OSS, or through the SDN Controller, etc., instead, or in combination to firing commands into the E2E Service Orchestrator. As such, the GANA Knowledge Plane is to be viewed as the "*brain*" for which implementers should design and implement advanced Autonomic/Cognitive Management & Control (AMC) DE Algorithms that can program network infrastuture via any of the systems available for that and according to the capabilities available of the systems' interfaces.

Regarding SDN domain involvement, an SDN framework involved may consist of a single SDN controller or a hierarchical federation of SDN Controllers may be involved. Each of the SDN controllers should be viewed as a data source or events source by the GANA Knowledge Plane, and in turn, the Knowledge Plane DEs may dynamically fire commands (thanks to the cognitive and analytics algorithms employed by the KP DEs) into an SDN controller in attempt to adaptively and intelligently program PNF or VNF under the control of the SDN Controller (it is the achievement of analytics-driven control whenever needed as determined by the KP DEs).

MBTS implementation flavors(Options)

As described in GANA Technical Specification [i.30], the GANA Knowledge Plane DEs may be designed to autonomically manage and control Network Elements (PNFs or VNFs) through the use of an MBTS function (as software library) if an MBTS library implementation is available. There are two Options:

a) MBTS function implemented at SDN Controller SouthBand interface.

If an MBTS function implementation is to be used by Knowledge Plane DEs for autonomic management and control of network infrastuture network elements (NEs) the MBTS function may be implemented as an integral part of the SouthBound Interface of an SDN Controller as discussed in ETSI White Paper No.16 [i.1] and in [i.54].

b) MBTS function at Knowledge Plane (KP) level.

This MBTS implementation flavour is that the MBTS Function (software library) may be tightly coupled with the Knowledge Plane DEs.

Figure 12 illustrates those two MBTS implementation flavours:

- If the MBTS function is to be used by KP DEs, and the SDN Controller which is used to manage and control a specific PNF or VNF implements the MBTS function, then the DEs can simply autonomically manage and control the respective PNF or VNF via the SDN Controller.

- If the MBTS function is desired for use by the KP DEs and the SDN controller associated with a target PNF or VNF does not implement the MBTS library as part of its southbound interface, then the GANA Knowledge Plane DEs can program the target PNF or VNF via an MBTS function employed directly by the Knowledge Plane otherwise the KP DEs could program the target PNFs or VNFs through the corresponding SDN controller or even without employing an MBTS function.

NOTE: Within the individual VNFs and PNFs, GANA Levels 2&3 DEs can be inserted/injected into each PNF/VNF to provide for autonomics within the Network Elements (NEs). The type of DEs that can be inserted (implemented or loaded into the target NE as software logics) depends on the type of configurable Managed Entities (MEs) meant to operate within the target NE for which local intelligence by way of the DEs algorithms dynamically and adptively configuring the MEs is desirable (ETSI TS 103 195-2 [i.30] contains a Table that provides insights on the concept of "owenership" in mapping of types of DEs to types of configurable MEs that can be autonomically managed by an "owner DE").

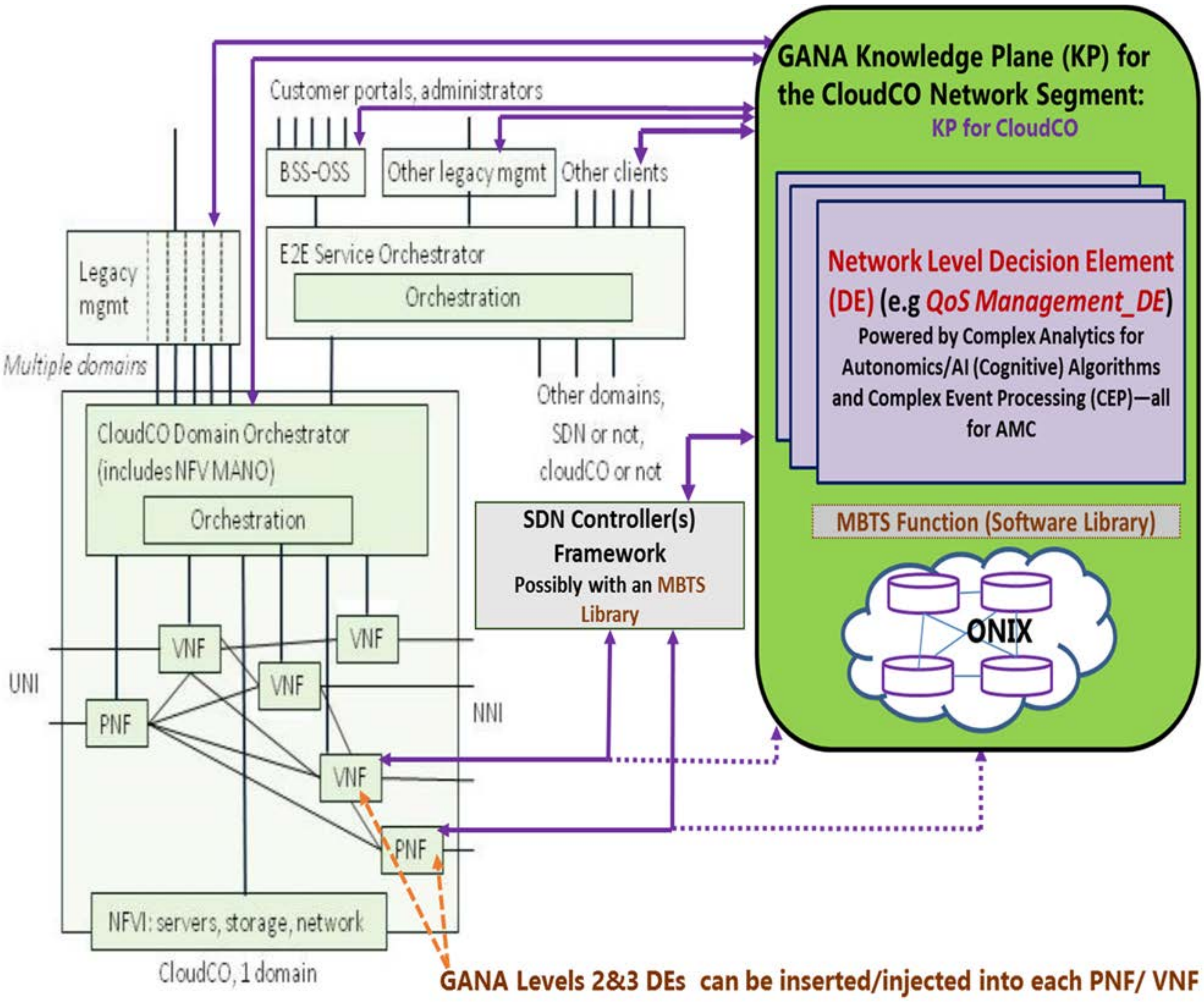


Figure 12: GANA Autonomics in CloudCO Environment in context of end to end service orchestration, with SDN Consideration

7.2.4.2 GANA Autonomics in CloudCO reference architecture

Based on BBF TR-384 [i.53], the integration of the GANA autonomics into the CloudCO reference architecture in general is illustrated in Figure 13 below as derived from Figure 13 in BBF TR-384 [i.53].

As described earlier, the GANA Knowledge Plane integration with the systems/components illustrated on the diagram means that those systems/components are to be viewed by the Knowledge Plane as data sources or event sources that feed into the KP's Decision Elements (DEs) algorithms, and the KP can selectively send commands into any of the systems. The nature of the commands depends on the optimal way it deems to achieve dynamic management and control objectives targeted at any particular time by the GANA Knowledge Plane.

NOTE 1: As some of the functionalities of the MCO Engine component described in BBF TR-384 [i.53] are said to include a "*closed-loop control and optimization of the state of CloudCO resources, on a time-continuous basis*", this aspect implies "autonomics" withing the MCO component, and such autonomics may need to be policy-controlled by higher level autonomics in the associated GANA Knowledge Plane.

NOTE 2: As described in BBF TR-384 [i.53], regarding CloudCO bootstrap dynamics and the "evolutionary" need for "*support of CloudCO enhancements via autonomic networking or other forms of self-learning-based network and service operation*", the GANA autonomics, particulary the GANA Knowledge Plane, can play the key role in addressing this aspect on CloudCO enhancements with autonomics.

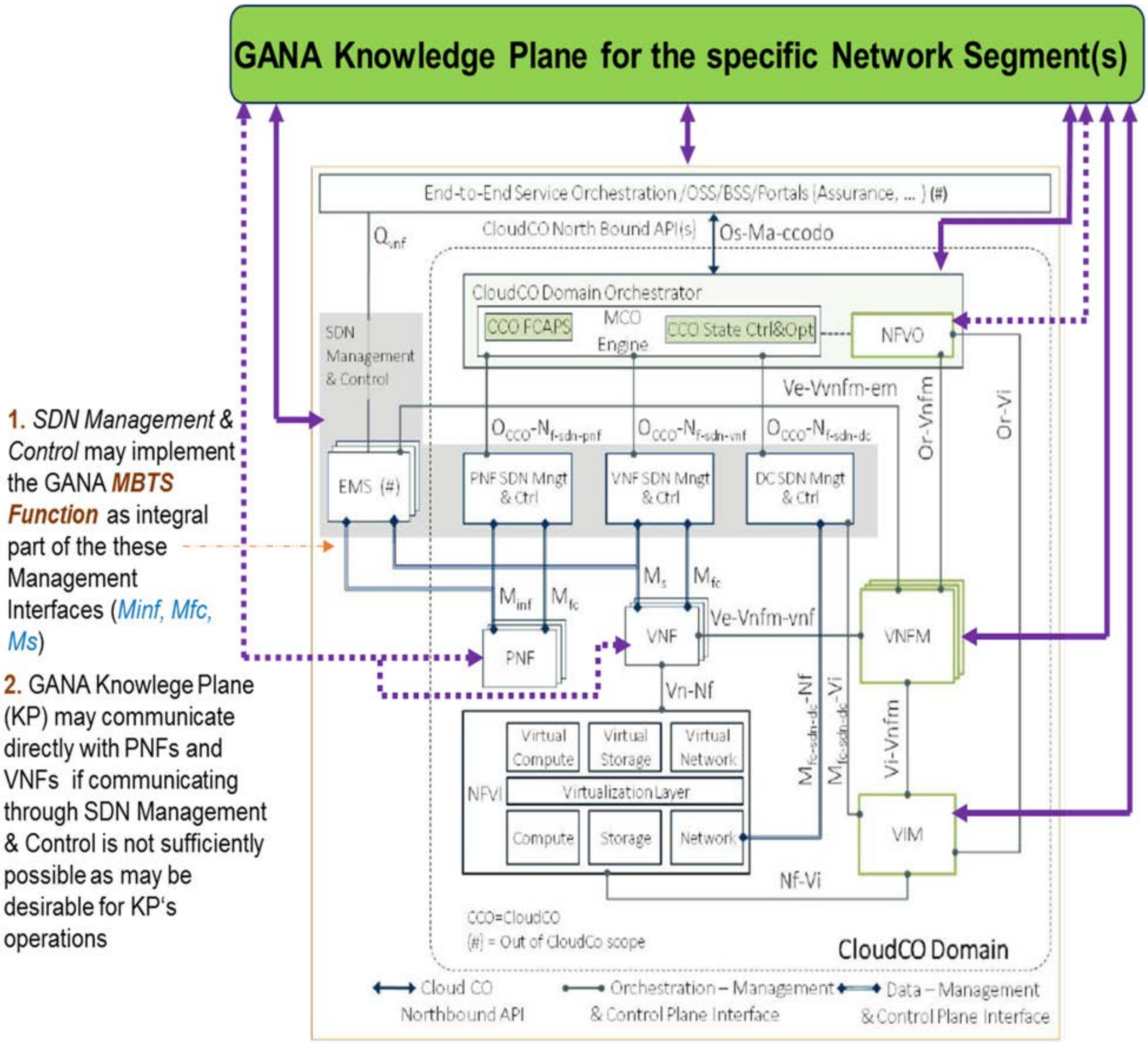


Figure 13: GANA Autonomics in CloudCO reference architecture

NOTE 3: Refering to Figure 13, the GANA Knowledge Plane DEs can go via the CloudCO Domain Orchestrator in its driving of analytics-driven and Artificial Intelligence (AI) driven orchestration-thanks to these capabilities in the Knowledge Plane's DE algorithms, but the GANA Knowledge Plane DEs may also drive some dynamic orchestration operations via the NFVO directly if necessary, otherwise the operations can be realized by the Knowledge Plane through the CloudCO Domain Orchestrator as shown.

7.2.4.3 GANA Mappings with the Broadband Access Abstraction (BAA) layer

Based on BBF TR-384 [i.53], the integration of the GANA autonomics with the Broadband Access Abstraction (BAA) layer is illustrated in Figure 14 as derived from Figure 14 in BBF TR-384 [i.53]. BAA can be viewed as an implementation of the GANA MBTS Library (i.e. the GANA MBTS Function, in a fashion similar to implementation flavour a) described in clause 7.2.4.1, by which the MBTS function is implemented as soutbound interface of an SDN controller or an layer accessible by the SDN controller's southbound interface). And so it can be noted that the BAA actually realizes MBTS Features.

NOTE 1: However, the extent to which BAA implements the MBTS as described in the GANA Technical Specification [i.30] needs to be further studied in order to see if the implementation of a BAA can be made to implement an advanced MBTS for the Access Network as can be guided by the specification of the MBTS function in the GANA Technical Specification [i.30].

NOTE 2: In referring to the BAA, it should also be noted that the MBTS, as described in the GANA Technical Specification [i.30], does not implement management and control logic (i.e. reasoning about when to (re)-configure a particular Network Element (NE). But MBTS is a software library that is rather for handling the translation of data models and associated management & control communications w.r.t. management and control aspects such as Configuration Management, Performance Management and Alarm Management, between the SDN Management & Control Systems and/or the Knowledge Plane, and the Network Elements(NEs). The actual management and control logic is implemented by the management and controls systems (which include the GANA Knowledge Plane).

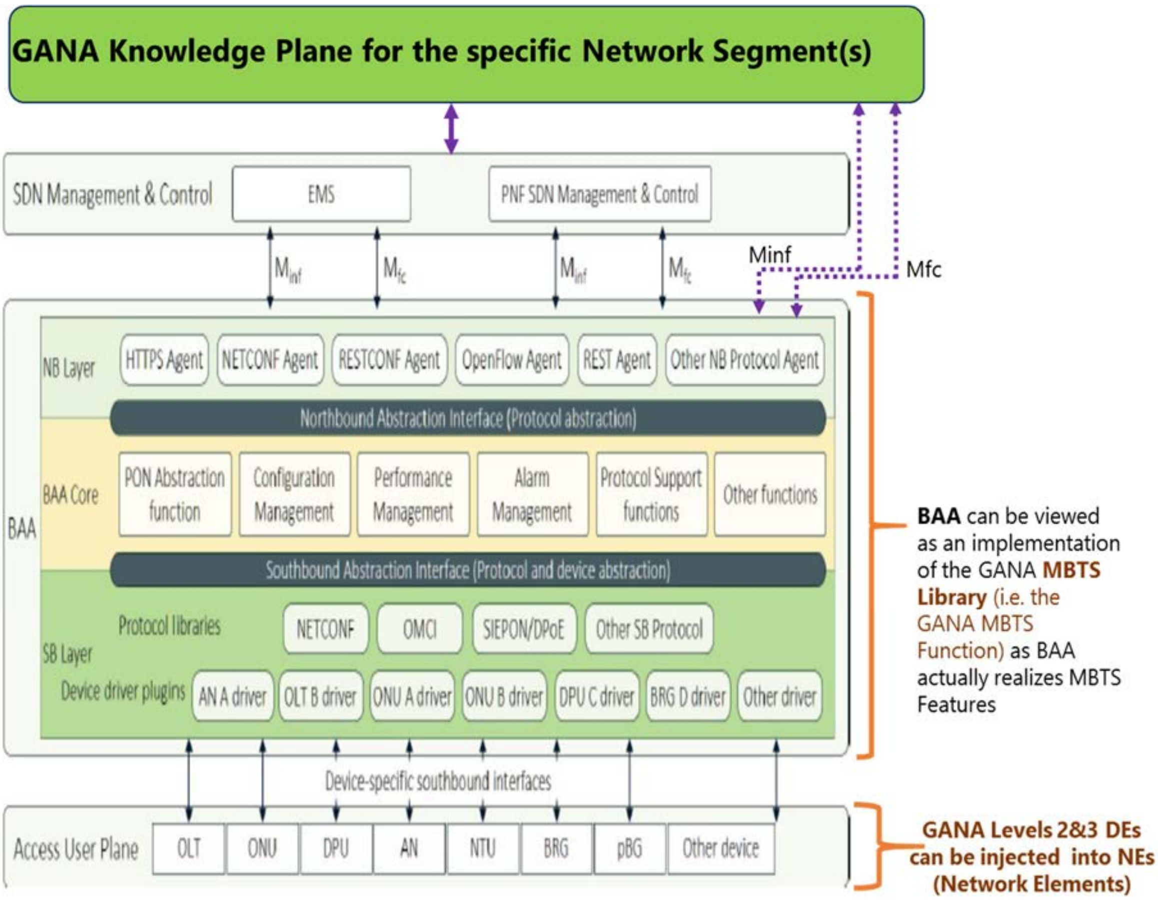


Figure 14: GANA Mappings with the Broadband Access Abstraction (BAA) layer

7.2.4.4 GANA Mappings with the Broadband Access Abstraction (BAA) layer within the CloudCO architecture

Based on BBF TR-384 [i.53], the integration of the GANA autonomics with the Broadband Access Abstraction (BAA) layer is illustrated in Figure 15 below as derived from Figure 15 in BBF TR-384 [i.53]. As the BAA Layer actually does implement features of the MBTS Function, the Knowledge Plane can communicate with PNFs or VNFs via the BAA.

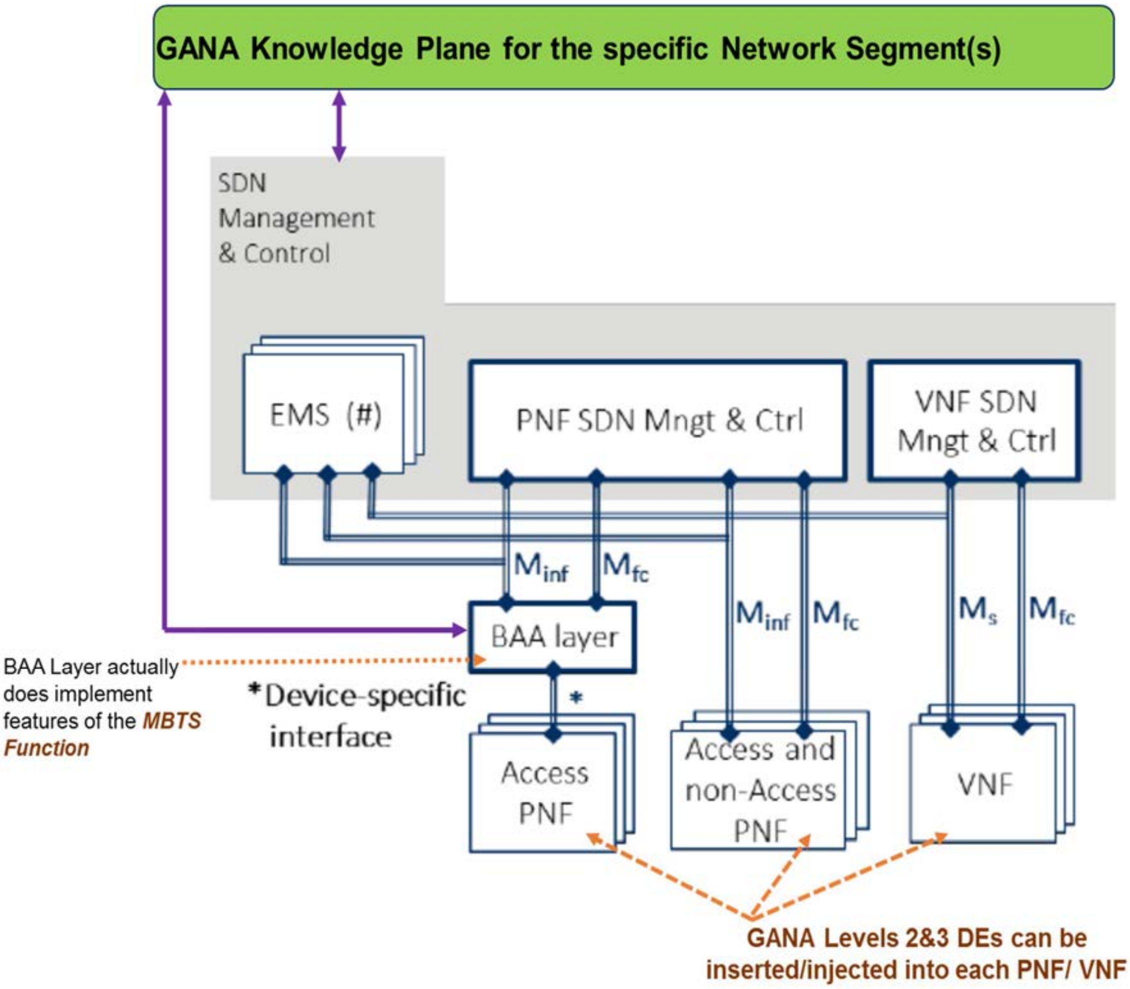


Figure 15: GANA Mappings with the Broadband Access Abstraction (BAA) layer within the CloudCO architecture

7.3 GANA instantiation onto Network Enhanced Residential Gateway

In BBF TR 317 [i.28] and BBF TR 359 [i.8], the residential or customer related node is addressed by the respective SDN and NFV enhanced node, thus called Network Enhanced Residential Gateway or virtual (Business) Gateway.

BBF architectures have typically focused on nodal requirements and geographically sensitive deployments. This is a consequence of the physics of broadband access transmission media. As such, although virtualization is driving both nodal and geographic deployment independence, specific nodes do not go away on the overall architecture, hence the inclusion of the access node and residential gateway/CPE.

The NERG concept involves moving some of the networking and service-related functions from the RG to the NSP's network. The distribution of functions effectively splits the RG into 2 sets of connected functional components as depicted in Figure 16.

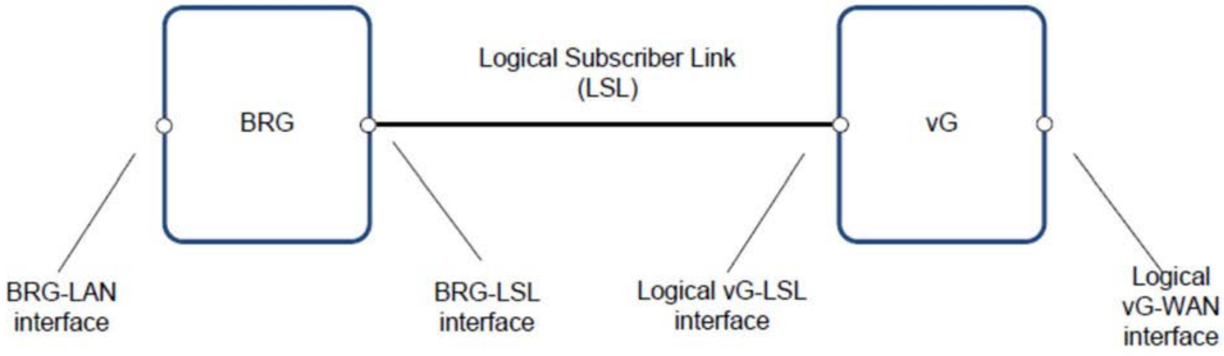


Figure 16: NERG overview

In this context, the physical node BRG: Bridged Residential Gateway - this is the CPE still located at the residential customer premises, configured as a managed bridge connecting its LAN interfaces and the BRG-LSL interface. The separation of logical functions which are operational in the virtualized part provide the main alternative deployments for the vG. The main alternative deployments - use cases are addressing the placement of the vG either "closer" to the BRG in the network nodes (e.g. close to the AN), or further to the network e.g. a cloud infrastructure.

For the GANA instantiation onto the NERG components, the main autonomic capabilities are split between the BRG and vG. The split is depicted in Table 9.

Table 9: Separation of autonomic features and capabilities between BRG and vG

Decision Element (DEs)	The NERG Functions - Managed Entities (MEs)	vG	BRG
NODE_LEVEL_AC_DE - Node-Level Auto-Configuration Decision-Element	Auto-configuration of CPE		X
NODE_LEVEL_R&S_DE - Node-Level Resilience & Survivability Decision-Element	All the Functional Entities of the node that require that Reactive and Proactive Resilience and Survivability should be reasoned about and handled on the node-level: • Software/firmware image management • Software module management • Dual homing	X	
NODE_LEVEL_SEC_DE - Node-Level Security Decision-Element	Security and authentication of CPE with ACS/OSS/Service configuration, subscriber isolation	X	
NODE_LEVEL_FM_DE - Node-Level Fault-Management Decision-Element	Diagnostics		X
FUNC_LEVEL_MON_DE - Function-Level Monitoring Decision-Element	Monitoring Tools and Mechanisms of the device - Status and performance monitoring		X
FUNC_LEVEL_GCP_M_DE - Function-Level Generalized Control Plane-Management Decision-Element	Initialization and control of the provisioning session flow, Session Control - Connection request, Subscriber management function, Scheduling and Traffic Filtering function	X	
FUNC_LEVEL_QoS_M_DE - Function-Level Quality of Service-Management Decision-Element	Marking on tunnels, QoS Interworking between fixed and 3GPP networks, per customer QoS	X	
FUNC_LEVEL_DP&FWD_M_DE - Function-Level DataPlane&Forwarding-Management Decision-Element	VLAN management, multicast resource control, L1/L2 Adaptation and Forwarding		X
FUNC_LEVEL_RT_M_DE - Function-Level Routing-Management Decision-Element	Multicast routing, selection of duplicate streams, separation of customer traffic	X	
FUNC_LEVEL_SM_DE - Function-Level Service-Management Decision-Element	Dynamic service provisioning, service integrity, service instance tags used, traffic profiles, service association	X	

Figure 17 and Figure 18 depict the mapping of the GANA DEs to NERG (BRG - vG). These figures illustrate the GANA Level-3 and Level-2 DEs that add value in the depicted NEs. The two figures correspond to two different options regarding the role of the GANA Knowledge Plane in the Management and Control Systems, namely:

Option 1: Knowledge Plane external to the legacy management and control systems EMS/NMS/OSS (Figure 17).

Option 2: Knowledge Plane as integrated within the management and control systems (Figure 18).

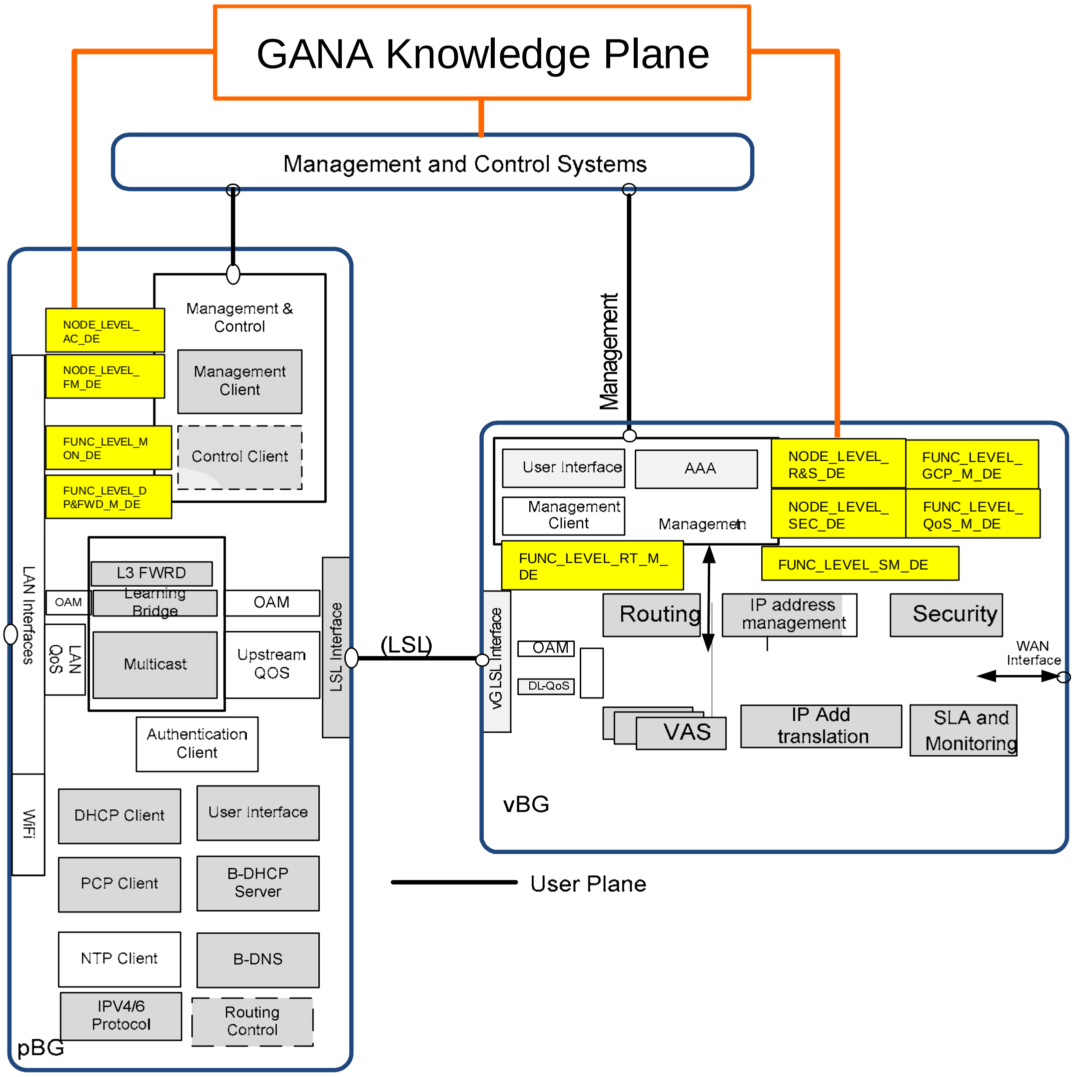


Figure 17: GANA instantiation on SDN/NFV architecture for NERG - Option 1 (KP external to the legacy management and control systems)

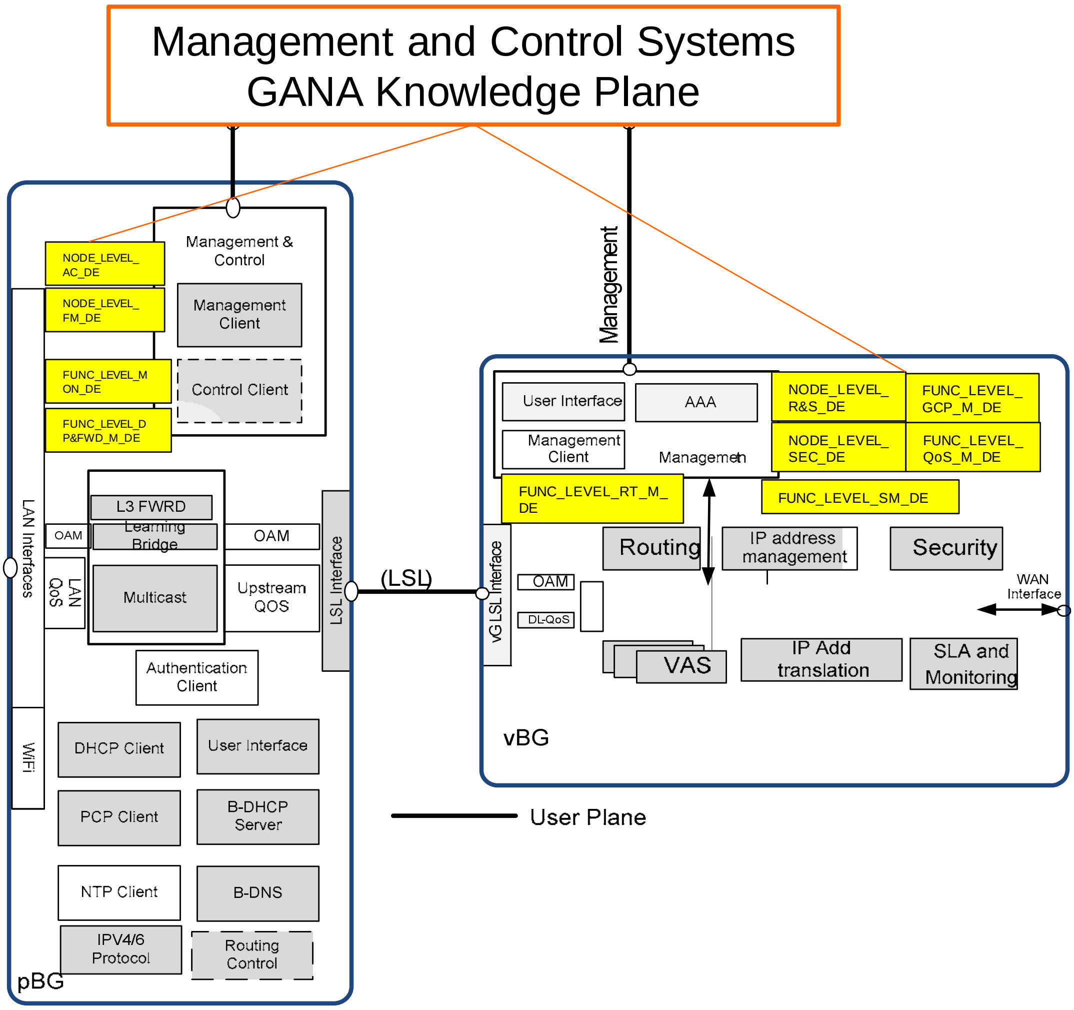


Figure 18: GANA instantiation on SDN/NFV architecture for NERG - Option 2 (KP as integrated within the management and control systems)

Following the main alternative use case deployments for NERG, the mapping of the GANA knowledge plane is addressed. The main GANA Knowledge Plane covers all the network segments operated by the operator. In this case the Knowledge Plane can access all the infrastructure network elements (VNFs or PNFs) without any administrative constraints and can also policy lower level GANA DEs instrumented in the network elements. In this case the knowledge plane interoperates with the vG on the cloud. The other alternative deployment encompasses the instantiation of relevant knowledge closer to the customer premises, e.g. interacting with the vG deployed at the AN.

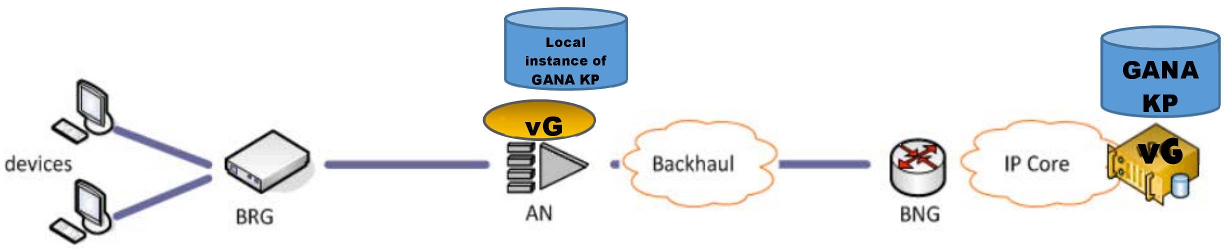


Figure 19: GANA Knowledge Plane instantiation on SDN/NFV architecture for NERG considering alternative deployments

7.4 GANA instantiation onto other Software-Defined Access Network (SDAN) Scenarios that may be applicable if BBF standards already support or would support the Scenarios

7.4.1 Towards Autonomic SDAN

The operations of the DEs introduced into such SDAN architectures should be seen as some degree of self-management intelligence delegated to the SDAN network element (data plane network node) that should complementarily and harmoniously interwork with the logically centralized management & Control Programmatic Operations and Policy control operations performed by either the GANA Knowledge Plane's Decision Elements (DEs) and/or by an SDN Controller towards the network infrastructure element(s). The logically centralized GANA Network-Level DEs in the GANA Knowledge Plane complementarily interwork with DEs instantiated on the node-level in the infrastructure elements as described in [i.1] and [i.2]. For example the Network-Level Fault-Management-DE in the Knowledge Plane complements the Node-Level Fault-Management, as discussed in [i.10], [i.11], [i.12] and [i.13]. But DE algorithm developers have a choice on whether an algorithm is better implemented using "in-network DE-to-DE" collaborations through the horizontal peer DE-to-DE reference points defined in the GANA Model or solely through a combination of centralized algorithm implemented by the collaboration of a DE in the Knowledge Plane and one embedded in network element(s). The Knowledge Plane DEs should have the freedom to drive management & control systems such as the SDN controller, for some operations that program the Network Element, while also being able to dynamically perform policy-control of the lower level DEs in the Network Element using a policy control protocol.

NOTE 1: The industry is encouraged to look into candidate protocols that can be used for this purpose.

Software Defined Networking (SDN) separates the control and data planes to enable coordinated, intelligent control of network resources.

SDAN scenarios standardized by BBF are described in published BBF documents such as BBF TR-384 [i.53] and BBF TR-370 [i.26]. GANA instantiations for such SDAN scenarios are described in earlier clauses of the present document, e.g. the integration of the GANA Knowledge Plane in the CloudCO architecture and environments described in BBF TR-384 [i.53]. However, what can be noted is that there are other SDAN scenarios that could be considered, provided that BBF standards already support such scenarios or would support them at some point.

For example, there is another SDAN approach of having some control functions delegated to an SDAN network element while some control functions are implemented in an SDN Controller, and such an SDAN approach is rather different from what is advocated for in the case of CloudCO environments described in BBF TR-384 [i.53], while it seems BBF TR-370 [i.26] could possibly support such an approach.

NOTE 2: Readers and GANA autonomics implementers should verify this at implementation time in order to ensure compliancy with BBF standards.

NOTE 3: Annex B of the present document provides additional insights into GANA instantiations onto other SDAN scenarios that can also be considered by implementers of GANA autonomics, provided that BBF standards related to SDAN such as BBF TR-384 [i.53] and BBF TR-370 [i.26] already support or would support them at some point.

7.4.2 Towards an Autonomic SDAN Network Element: GANA DEs and MEs Mappings and Characterizations thereof

Table 10: DEs and their mappings to Self-* operations, and the DE mappings to Managed Entities (MEs) that can be autonomically orchestrated or managed by their corresponding DEs

Decision Element (DE)	Self-* realized by the DE	Category of Management aspect addressed by the DE via autonomic means	Managed Entities (MEs) autonomically orchestrated or managed by the DE	Example Data Sources for the DE(s)	Remarks and additional aspects for consideration
Node-Level Fault-Management-DE	Self-Diagnosis, Self-Repair and Self-Healing on Component, Module or System Level during the long term operation of the Network Element (NE) as described in [i.10], [i.11], [i.12] and [i.13].	**Fault Management part of FCAPS**	Mechanisms or Tools dynamically applicable for Fault-Detection, Fault-Localization (Diagnosis) and Fault-Removal	Tools (e.g. monitoring tools) and all entities in the node that can communicate events related to manifestations of faults, errors, failures in the node or in the network	Interworks with the Network-Level Fault-Management-DE implemented in the Knowledge Plane
Node-Level Resilience & Survivability-DE	Auto-Remediation and Reactive & Proactive Self-Healing on Service Level by applying protection and restoration techniques and strategies, while at the same time interworking with the Fault-Management DE to implement Self-healing strategies on the node level as described in [i.10], [i.11], [i.12] and [i.13].	**Fault Management part of FCAPS**	Mechanisms and Tools dynamically applicable for remediation or self-healing of services and for global node resilience to faults/Errors/Failure manifestations in the node or the network	Monitoring Data and Event suppliers, including service impacting events communicated from the protocol stack	Interworks with the Network-Level Resilience& Survivability-DE implemented in the Knowledge Plane

Decision Element (DE)	Self-* realized by the DE	Category of Management aspect addressed by the DE via autonomic means	Managed Entities (MEs) autonomically orchestrated or managed by the DE	Example Data Sources for the DE(s)	Remarks and additional aspects for consideration
Node-Level Auto-Configuration-DE	Auto-Configuration of the network element by applying configuration profiles and applying policies to DEs instantiated in the network element. The dynamic run-time instantiation of the DEs can be performed by the Auto-Config-DE. The configuration aspects covered by the Auto-Config-DE complement configurations performed by agents such as SDN/NETCONF Agents, etc.	**Configuration Management part of FCAPS**	Function-Level DEs and any other entities in the network element that need to be bootstrapped or (re)-configured in response to policy changes and workload changes. Function-Level DEs receive policies from the Knowledge Plane via the Auto-Configuration-DE.	Knowledge Plane DEs, MBTS, ONIX; local DEs; Agents such as SDN Agents (OpenFlow [i.56]) Agents, NETCONF Agents, Legacy Management Agents) can export operational state information such that it is accessible to the DE	To ensure policy consistent network resources configuration, the Auto-Configuration-DE needs to *be aware of all configuration agents* (e.g. SDN Agents, Legacy Management Agent, etc.) operating in the network element. The Auto-Configuration-DE should have access to configuration event that is to occur or has occurred on the network element through a local agent, and may need to access the configuration data (if accessible) and the resultant state change on the element. Interworks with the Network-Level Auto-Configuration-DE implemented in the Knowledge Plane

Decision Element (DE)	Self-* realized by the DE	Category of Management aspect addressed by the DE via autonomic means	Managed Entities (MEs) autonomically orchestrated or managed by the DE	Example Data Sources for the DE(s)	Remarks and additional aspects for consideration
Node-Level Security Management-DE	Self-Protection of the node/element. See note 1.	**Security Management part of FCAPS**	Mechanisms and Tools dynamically applicable for Security Threats- Detection and Self-Protection of the node and possibly for network wide self-protection via the collaboration of Node-Level Security-Management DEs. Traffic Filtering Mechanisms may be employed by the DE during it attempts to block suspicious traffic, and also some security mechanisms such as tunnelling mechanisms may be dynamically employed by the DE the security enforcement of the node	Knowledge Plane's Security Management DE may dynamically policy control the Node-Level Security Management-DE.	The Security Management-DE may require *intercepting (or acting proxy for) certain communications* with the outside world (and this can include from the SDN controller) when self-protection and self-defending algorithms of the DE require it to do so. The DE can apply traffic filtering rules on the interfaces of the network element upon security threat detection and re-adjust traffic filtering rules accordingly. This behaviour can be enforced by Security-Management-DE in the Knowledge Plane. The DE may be required to participate in a network-wide self-protection distributed algorithm that involves the DE and other Security-Management-DEs on node-level (for in-network self-protection behaviour) or the Network-Level Security-Management-DE in the Knowledge Plane, according the algorithm.

Decision Element (DE)	Self-* realized by the DE	Category of Management aspect addressed by the DE via autonomic means	Managed Entities (MEs) autonomically orchestrated or managed by the DE	Example Data Sources for the DE(s)	Remarks and additional aspects for consideration
Function-Level QoS_&_Performance Management-DE	Self-Configuration of QoS guaranteeing mechanisms; Self-Optimization of QoS guaranteeing mechanisms taking into consideration workloads, traffic volume and state of the node and the service impacting factors derived from network conditions. See note 2.	**Performance Management part of FCAPS**	QoS guaranteeing mechanisms such as Traffic Classifiers, Traffic shaping, Queuing, DiffServ Packet (Re)-Marking, bandwidth allocation adjustments, etc.	Monitoring and Measurement (Telemetry) Tools that can provide info on workloads, traffic volume levels, state of the node and service impacting events detected in the network; Knowledge Plane as it can supply new policies that guide the way the DE should operate	This DE can be required only in certain SDAN network elements that operationalize the types of MEs associated with this DE. For example the Access Node, BNG, etc. Interworks with the Network-Level QoS_&_Performance Management-DE implemented in the Knowledge Plane.
Function-Level Monitoring-DE	Self-Configuration of monitoring mechanisms and mechanisms or tools for monitoring data formatting and dissemination to consumer entities such as (local or remote) ; Self-Optimization of monitoring behaviours and tools, and data dissemination methods, frequency, etc. See note 3.	**Performance Management part of FCAPS**	Monitoring or Measurement (Telemetry) Mechanisms and other types of Mechanisms (e.g. traffic filtering, protocols, etc.) or Tools for monitoring data formatting and configurable dissemination to consumer entities such as local DEs and Knowledge/Information Repository or remote/external entities.	Knowledge Plane's Monitoring DE as it can supply new policies that guide the way the DE should operate Local DEs may also need to communicate any monitoring data they gather to the Monitoring-DE	Interworks with the Network-Level Monitoring-DE implemented in the Knowledge Plane.
Function-Level Data Plane_&_Forwarding_Management-DE	Self-Configuration and Adaptive Re-Configuration of Configurable Parameters of Plane and Fowarding Plane functions based on operator policies or management and control inputs supplied by the external management and control systems (e.g. SDN Controller and Knowledge Plane).	**Local Dynamic Management of the Access Node's Localized Control Plane and Fowarding Plane functions (i.e. their configurable parameters)** but in respect of the external governing policies enforced by a management and control system such as the SDN-Controller or the Knowledge Plane	Access Node's Localized Control Plane functions that can be delegated by the SDN controller to run in the SDAN network element, andand any configurable traffic engineering related parameters such as those defined in [i.26].	Various data sources (including local data sources within the SDAN network element) that the DE algorithm developer/innovator may want to use	Interworks with the Network-Level Generalized-Control-Plane Management-DE implemented in the Knowledge Plane.

Decision Element (DE)	Self-* realized by the DE	Category of Management aspect addressed by the DE via autonomic means	Managed Entities (MEs) autonomically orchestrated or managed by the DE	Example Data Sources for the DE(s)	Remarks and additional aspects for consideration
NOTE 1: Principles for designing autonomic Security management based on the GANA as described in [i.14] and [i.15], can be applied to designing the Security Management-DE(s), while taking into account various security aspects in SDN (e.g. using sources such as [i.19]). NOTE 2: Principles for designing autonomic QoS management based on the GANA as described in [i.14] and [i.15], can be applied to designing the QoS_&_Performance Management-DE(s). NOTE 3: Principles for designing autonomic monitoring based on the GANA as described in [i.16], [i.17] and [i.18], can be applied to designing the Monitoring DE(s).					

7.4.3 A General Characterization of the GANA Knowledge Plane instantiated for SDAN

1) Example Autonomic Management & Control (AMC) Use Cases that can be implemented by DE algorithms in the Knowledge Plane in dynamic management operation performed adaptively by the responsible DEs during the network operation phase, after the initial configuration of the aspects (Managed Entities) by either the Knowledge Plane or by other types of management and control systems in place to interwork with the Knowledge Plane:

- Dynamic (Self-) Optimization of the physical layer configuration of the broadband connection, for example by changing parameters such as data rates and power levels.

- Dynamic Access network control by the Knowledge Plane DEs in collaboration with any management and control systems in place to interwork with the Knowledge Plane by being driven by the Knowledge Plane layer involves dynamic (self-adaptive) configuration of e.g. Network Elements (NEs) access nodes, thereby adapting the physical layer configuration parameters such as data rates, transmitted power and spectrum, coding schemes, resilience to noise, and latency, based on various factors such as challenges in the network environment and policy changes by the Operator, etc. (ASSIA™ SDAN White Paper [i.20] provides insights on this subject of examples of configurable parameters).

- Dynamic application of maintenance profiles (see in [i.20]) in adherence to operator's policy should be automated by DEs in the Knowledge Plane. Knowledge Plane DEs can perform profile optimization relying on historical and current data about a subscriber line, and taking into account for the line's service profile as discussed in [i.20].

- Access Network Diagnostics (discussed in sources such as [i.20]) should be performed by the Fault-Management-DE in the Knowledge Plane, and the Knowledge Plane should help resolve service issues and compute remedial strategies and apply them for self-healing of services automatically, and other automations should also be performed by the Knowledge Plane DE algorithms, e.g. automated maintenance and upgrades of the access nodes. The Fault-Management-DE performs Root-Cause Analysis (RCA) and computes self-healing and self-repair strategies that it then applies to the Managed Entities (MEs) in the Network Elements (NEs) that should be effected ((re)-orchestrated or (re-) configured) to help eradicate the problem/fault or reduce its impact on services by invoking remediation strategies in collaboration with other DEs.

- SDAN Diagnostics and Producing Recommendations as discussed in [i.20] should also be performed by the Fault-Management-DE in the Knowledge Plane. The types of Recommendations discussed in [i.20], should be produced by the Knowledge Plane DEs, and can "include the identification of upsell opportunities" as discussed in [i.20].

NOTE: The Knowledge Plane DEs should also dynamically policy (perform policy control of) the lower level GANA DEs instrumented in the network elements (VNFs or PNFs), e.g. CPE, AN, BNG, to complement and tune the autonomic behaviours realized at the lower GANA levels (within the network elements).

2) Impact of some SDAN Scenarios on the nature, multiplicity and responsibilities desired of the GANA Knowledge Plane (KP) instances that should be operated in the various scenarios, and the relationships of the specific Knowledge Plane instances with the Network Elements (NEs) that should be under the control of a specific Knowledge Plane instance. The following scenarios are taken from [i.20], [i.24] and [i.25], but more scenarios and more details can be found in BroadBand Forum (BBF) in Access Virtualization and Fixed Access Network Sharing (FANS) related documents such as BBF TR-370 [i.26]:

- **Scenario 1: Single Operator SDAN**

  Knowledge Plane (KP) characterization: Only a single Knowledge Plane instance can be required to cover all the network segments operated by the operator. In this case the Knowledge Plane can access all the infrastructure network elements (VNFs or PNFs) without any administrative constraints and can also policy lower level GANA DEs instrumented in the network elements. **The Data Sources** for the Knowledge Plane are for example VNF's data, VNFManager, VIM, SDN controller, Service Orchestrators, OSS, Performance Management Systems, Data Collectors, Probes, Information shared through ONIX, etc., if such data sources can be available to the Knowledge Plane. ONIX, a distributed scalable overlay system of information servers and being a part of the Knowledge Plane, should also be instantiated to serve as Real-Time Inventory for various types of information. The ONIX would be useful for enabling auto-discovery of information/resources of an autonomic network via its "publish/subscribe/query&find" protocols. Databases in the Broadband network can be treated as members of ONIX if their information they store could be desirable to have it consumed through the "publish/subscribe/query&find" paradigm and protocols employed by ONIX. DEs can make use of ONIX to discover information and entities (e.g. other DEs) in the network to enhance their decision making capability.

- **Scenario 2: Multiple Operator SDAN**

  Knowledge Plane (KP) characterization:

  ▪ **Sub-Scenario (a):** The Knowledge Plane can be implemented as an integral part of a multi-tenant management & control system that serves the needs for all the operators involved (including the Virtual Network Operators) and caters for configuration, diagnostics and remediation functions of all connections in the access network as discussed in [i.20], a scenario in which management functions are implemented by the Multi-tenant Management System. In such a scenario the Knowledge Plane can have to rely only on the management and control mechanisms available in the multi-tenant management system and not available through an OSS owned by a Virtual Network Operator, to dynamically adapt the configuration of the network services and connections whenever it determines to do so. The multi-tenant management & control system can be made to run in a virtualized environment. The Knowledge Plane can run as multiple instances and as independent tenants for specific Virtual Network Operators operating in the shared access network. A means to enable the Knowledge Plane (integrated as part of a multi-tenant management and control system)to access all the infrastructure network elements (VNFs or PNFs) without any administrative constraints should be put in place, as the Knowledge Plane DEs can also dynamically policy the lower level GANA DEs instrumented in the network elements. The **Data Sources** for the Knowledge Plane are for example VNF's data, VNFManager, VIM, SDN controller, Service Orchestrators, Performance Management Systems, Data Collectors, Probes, Information shared through ONIX, etc., if such data sources can be available to the Knowledge Plane. The ONIX part of the Knowledge Plane should also be instantiated to serve as Real-Time Inventory for various types of information and should complement any databases that can be used.

- **Sub-Scenario (b):** Multiple Knowledge Plane instances, whereby a Virtual Network Operator (VNO) has a Knowledge Plane instance (**VNO Knowledge Plane**) associated and attached to the management and control systems (including the OSS) dedicated to the VNO, and the Physical Infrastructure Provider has a Knowledge Plane instance (**Physical Infrastructure Provider Knowledge Plane**) associated and attached to the management and control systems (including the OSS) dedicated to the Physical Infrastructure Provider. Such management and control systems can be implemented outside an Access Virtualization System as discussed in [i.20]. A means to enable the individual Knowledge Plane instances to access the infrastructure network elements (VNFs or PNFs) that should be under their control without any administrative constraints should be put in place, as Knowledge Plane DEs can also dynamically policy the lower level GANA DEs instrumented in the network elements. The **VNO Knowledge Plane** and **Physical Infrastructure Provider Knowledge Plane** can need to be federated such that they coordinate their operations if their collaborative behaviours can effect a global self-optimization of network resources. The ONIX part of the Knowledge Plane should also be instantiated to serve as Real-Time Inventory for various types of information and should complement any databases that can be used. The ONIX Information servers owned by the different players can also need to be federated to form a global ONIX system. The **Data Sources** for the Knowledge Plane are for example VNF's data, VNFManager, VIM, SDN controller, Service Orchestrators, OSS, Performance Management Systems, Data Collectors, Probes, Information shared through ONIX, etc., if such data sources can be available to the Knowledge Plane.

- **Scenario 3: SDAN to the Home**

  Knowledge Plane (KP) characterization: In having to management that is extended into the home network and is made to include end-user customer experience involving user access to OTT services as discussed in [i.20], the characterization of the Knowledge Plane can take similar nature to the KP in the scenario involving Multiple Operator SDAN. In such a scenario, the Knowledge Plane can be implemented as an integral part of a multi-tenant management & control system that serves the needs for all the operators involved (including the Virtual Network Operators) and caters for configuration, diagnostics and remediation functions of all connections in the access network as discussed in [i.20], a scenario in which management functions are implemented by the Multi-tenant Management System. In the case of extending management into the home network, probes instrumented in the home network should disseminate performance data collected across networking devices owned or controlled by multiple service providers as discussed in [i.20]. The Knowledge Plane DEs as an integral part of the multi-tenant management system can either produce recommendations that enable VNOs to control and optimally configure the access network, while at the same time the Knowledge Plane DEs, in a "closed loop" fashion autonomically apply the recommendations to realize self-optimization as autonomic objective. Data fusion that spans CPEs and Wi-Fi access points that may have been deployed by different service providers should enable the Knowledge Plane DEs (a process orchestrated and driven by the Fault-Management-DE) to perform Root Cause Analysis (fault correlation/diagnosis/localization) to resolve the faults (root causes) that commonly affect multiple end users serviced by the different access points. The ONIX part of the Knowledge Plane should also be instantiated to serve as Real-Time Inventory for various types of information and should complement any databases that can be used.

  The **Data Sources** for the Knowledge Plane are for example End-user management systems that gather data exported by monitoring probes/agents instrumented in the home network and OTT service data and export such data to the Knowledge Plane part of the multi-tenant management system, as well as VNF's data, VNF Manager, VIM, SDN controller, Service Orchestrators, OSS, Performance Management Systems, Data Collectors, Probes (e.g. passive probes) gathering network traffic data, etc., if such data sources can be available to the Knowledge Plane.

8 E2E Value of Federated Autonomics across Multiple BBF Network Segments

8.1 Introduction on Use Cases for E2E Business value of Autonomics/AMC

The main focus of clauses 6 and 7 is the instantiation of GANA model concepts (such as DEs) on each of the (physical and virtualized manifestations) main nodes of the BBF architecture. In contrast, this current clause looks at this instantiation from an end-to-end (e2e) perspective while seeking to show the value of E2E business value of autonomics. This means that the focus is placed on the cooperation and interaction among the instantiated GANA DEs in each of the (physical and virtualized) nodes of the BBF architecture.

The goal is to describe and elaborate on holistic use cases that can be used to demonstrate the relevance and importance of introducing autonomics both in terms of business value for network operators/service providers and in terms of improved experience for the end-user (customer). One such a use case is described in Table 11.

Table 11: Example Use Case on the value of autonomics for Network Operators in improving customer Quality of Experience (QoE)

Use case name	Proactive identification and resolution of customer's network experience incidents
Description/Storyline Use Case	Analytics and autonomic management and control are applied in this case in order to: a) understand the value autonomics brings in customer network experience, proactively and autonomically addressing the impact of incidents on services (i.e. autonomic service assurance) in a holistic manner and from different perspectives; b) plan remediation actions; and c) apply remediation actions, thus preventing the customer from contacting the call centre to complain-thanks to autonomic service assurance performed by GANA DEs. Apart from information about network capabilities and line characteristics, and current installation base of equipment/services, insights and predictions derive based on a customer network experience profile created from a multitude of different perspectives, including: • Location type e.g. home, work, etc. • Time of the day, week, month. • Type of service usage e.g. voice calls, email, browsing, video, etc. • Type of application e.g. YouTube™, etc. • Relevant posts on social media. Insights and predictions can be then used by GANA DEs to plan and execute remediation actions including: • Dynamic increase of bandwidth offered for specific service and application type and time. This applies for instance in cases that a high increase in Video or IPTV traffic is expected in certain locations at night and during the weekend. • Optimization and dynamic application of flexible maintenance profiles. • Software/Firmware updates and/or equipment upgrades. but also opportunities for: • Upselling to customers. For example, identifying frequent dropped calls happening while the customer is at home location or her enterprise can trigger the recommendation for a small cell or a license for a new product upsell.
Network Environment(s)	Broadband, fixed-access networks (the use case can be extended to cellular network in case of hybrid mode operation).
Problems	Operators are investing a lot in order to intensify their customer retention efforts for maintaining their market share and profitability. Nevertheless, resources are limited and should be properly targeted. The network incidents that that will be perceptible by the customer and therefore impact the customer experience, constitute a main frustration factor that creates the need for the customer to interact with an assisted channel. It is noted that the interaction with the call centre is very expensive. According to McKinsey™/IBM™ *"1M calls are received per month by a mid-size SP's call centre at an average cost of 10$ per call".* In addition, repeated deterioration in experience and subsequent complaints can potentially lead to churn. Accordingly, there is an imminent need to leverage (predictive) analytics and autonomic management and control in order to identify/predict incidents, which can that can be fixed proactively to prevent the customer from calling the call centre to complain.

Use case name	Proactive identification and resolution of customer's network experience incidents
Functions Impacted	Self-optimization, self-diagnosis, self-healing and other self-* features that autonomics bring in departing from manual management methods currently employed by human network administrators.
Systems Involved	CPE, Access Nodes, Aggregation nodes, BNG.
Indicators/Evaluation criteria/Metrics	**Indicators/Data:** • Network data (including layer 3 and above). • Customer Demographics. • Social Data. **Evaluation criteria/Metrics:** • Decrease or even nullify number of (repeated) contacts. • Decrease or even nullify complaints. • Increase net promoter score (NPS).
Players	• Customer. • Network operator/Service provider. • Equipment vendor. • Service Provider.
Beneficiaries, and the Benefits	• Customer experience is improved. • After-sales services costs are reduced as calls to centres and complaints are reduced or nullified, thus resulting in increased customer loyalty and lifetime value which in effect solidifies existing revenue streams. • New revenue streams can be opened for the SP through the derived proactive upsell/marketing opportunities.

8.2 Recommendations on how Autonomics Implementers can use the GANA instantiation for the BBF architectures to implement the Use Case(s)

Based on the GANA instantiation for autonomics (AMC) in BBF architectures provided in the various clauses of the present document and the exemplary use case in clause 8.1 and described in Table 11, this clause provides some recommendations to implementers of autonomics on how to deduce an approach to take in implementing a use case for E2E autonomics.

The outcome is Table 12, which aims at guiding implementers of autonomics on how to identify a particular part of the GANA instantiation that plays a role in a specific aspect captured by the example Use Case. More specifically, the table indicates the GANA FBs that play a role in each aspect of the Use Case such that implementers can be guided accordingly on how to implement this by using the recommended GANA instantiations in BBF architectures, as presented in the various clauses of the present document.

Table 12 can be seen as a checklist, which could be augmented by additional items that make sense for a given Use Case an implementer is considering. At the same time, it can happen, for a given Use Case, one or multiple mentioned items could be not relevant to the implementer's specific Use Case, hence they should be tagged "NA" (Not Applicable).

Table 12: Recommendations to implementers of autonomics for realizing the E2E QoE use case

	Element				
Aspects of use case	**Autonomic CPE**	**Autonomic AN**	**Autonomic BNG**	**Knowledge Plane (ONIX)**	**Knowledge Plane (DEs and MBTS)**
Monitoring of QoS-related data/information and faults and SLA violations	X DEs in the autonomic CPE are expected to provide the value of NE level and internal autonomics	X DEs in the autonomic AN are expected to provide the value of NE level and internal autonomics	X DEs in the autonomic BNG are expected to provide the value of NE level and internal autonomics		
Monitoring of the home Wi-Fi environment e.g. congestion, interference issues, etc.	X DEs in the autonomic CPE are expected to provide the value of NE level and internal autonomics				
Monitoring the customer experience w.r.t. Service Provider or OTT services at home	X DEs in the autonomic CPE are expected to provide the value of NE level and internal autonomics				X Depending on the network infrastructure involved in the service delivery for the customer services, there can be a possibility for Multi-Tenants Knowledge Planes and their Federation as discussed in clause 7.4.3 on Characterization of the GANA Knowledge Plane instantiated for SDAN
Collection of data coming from network (OSS), customer (BSS/CRM), Social media feeds and home environment				X	X The MBTS (if deployed) should play a role in Collection of data coming from network elements (NEs) and generating Knowledge presented to the KP DEs and storage into ONIX as history, while providing for the mediation services between KP DEs and NEs as expected of the MBTS

Element					
Aspects of use case	**Autonomic CPE**	**Autonomic AN**	**Autonomic BNG**	**Knowledge Plane (ONIX)**	**Knowledge Plane (DEs and MBTS)**
Context enriched diagnostics, Correlations and predictive analytics on data coming from multiple sources of data e.g.: • **model QoE with respect to network QoS, time/location context and service type** • **correlate repeated network issues with high probability of churn, etc.**					X (in reference to NET_LEVEL_QOS&Perf-Mgt_DE in clause 7.4.3 in collaboration with other NET_LEVEL_DEs (e.g. NET_LEVEL_MON_DE, NET_LEVEL_Fault-Management-DE, etc.) as can be required). Depending on the E2E network infrastructure used to deliver customer services, various E2E aspects of the GANA KPs and KP DEs should play a role in the broader picture for AMC, with the various DEs providing for Self-* operations w.r.t. Managed Entities (MEs) autonomically orchestrated or managed by their corresponding DEs. For example SDAN would imply the need to implement the GANA instantiation onto Software-Defined Access Network (SDAN) as described in clause 7.4
Derivation of recommendations regarding optimized network configurations e.g.: • **Dynamic bandwidth increase for specific service and application type and time** • **Optimization and dynamic application of flexible maintenance profiles** • **Software/Firmware updates and/or equipment upgrades**					X All the KP DEs are expected to collaborate in producing the recommendations based on the collective analytics and optimizations performed by the KP DEs collectively (in reference to clause 4.3 on Characterization of the GANA Knowledge Plane) Software/Firmware updates and/or equipment upgrades can be triggered by the KP DEs during the KP's operation

Element					
Aspects of use case	**Autonomic CPE**	**Autonomic AN**	**Autonomic BNG**	**Knowledge Plane (ONIX)**	**Knowledge Plane (DEs and MBTS)**
Derivation of marketing related recommendations and interfacing to campaign management systems					X All the KP DEs are expected to collaborate in producing the recommendations based on the collective analytics and optimizations performed by the KP DEs collectively (in reference to clause 4.3 on Characterization of the GANA Knowledge Plane)
Indicators/Data • **Network data (including layer 3 and above)** • **Customer Demographics** • **Social Data**				X The ONIX can be used to store information on Customer Demographics and Social Data, else such information can be stored in other systems the operator can be using	X Network data (including layer 3 and above) gathered from NEs and Data Collectors are presented to KP DEs (directly or through the MBTS that processes the data and presents in form of Knowledge to DEs). Data Collectors should process such data and present knowledge to the KP DEs
Context Information processing	X	X	X	X	X
Policy Control of lower Level DEs in the autonomic NEs (CPEs, Access Nodes, Aggregation nodes, BNGs)	X	X	X		X Knowledge Plane DEs perform Policy Control of lower Level DEs in the autonomic NEs as they take into consideration the various context information and apply Analytics to determine where policy changes and adaptive configuration of MEs need to be applied by DEs in the NEs

NOTE: Regarding the following *Evaluation criteria/Metrics* associated with the Use Case, it is expected that as the autonomic network (autonomic CPEs, Access Nodes, Aggregation nodes and BNGs) and the KP operate over time the human network operator should be able to assess the metrics by analysing Trouble Tickets and related statistics:

- Decrease or even nullify number of (repeated) contacts.
- Decrease or even nullify complaints.
- Increase Net Promoter Score (NPS).

8.3 E2E realization through the instantiation of the GANA into the NFV-based BBF

The use case in clause 8.1 is described to be addressed by GANA FBs across multiple network segments and domains (e.g. those outlined for the SDAN scenarios) in a federated fashion and by taking into account the virtualization framework recently specified in BBF TR 359 [i.8]. (For Mobile/Fixed Convergence scenarios please refer to clause 9). As already stated in clause 7.2, the Domain Management Coordination Function (DMCF), introduced in [i.8], plays an important role in providing the management functions needed to maintain the "desired state" of functions within a specified domain. For example, the DMCF for the NERG provides the management functions (e.g. retrieve device topology, configure firewall) necessary to maintain functions within the residential domain.

In the case of various BBF network domains, traffic is forwarded through different networks operated by different service providers. To implement autonomic networks, each segment GANA Knowledge Plane (KP) needs to peer to other GANA KP in order to dynamically change QoS profiles applied on network elements and use the most appropriate combination depending on network conditions. Figure 20 shows two BBF network segments, which are autonomically monitored by the "Monitoring-DE" instantiated in the GANA Knowledge Plane on each network segment. Based on this information and thanks to the communication interface between both GANA Knowledge Planes, QoS policies might be enforced on network equipment in a coordinated and efficient manner.

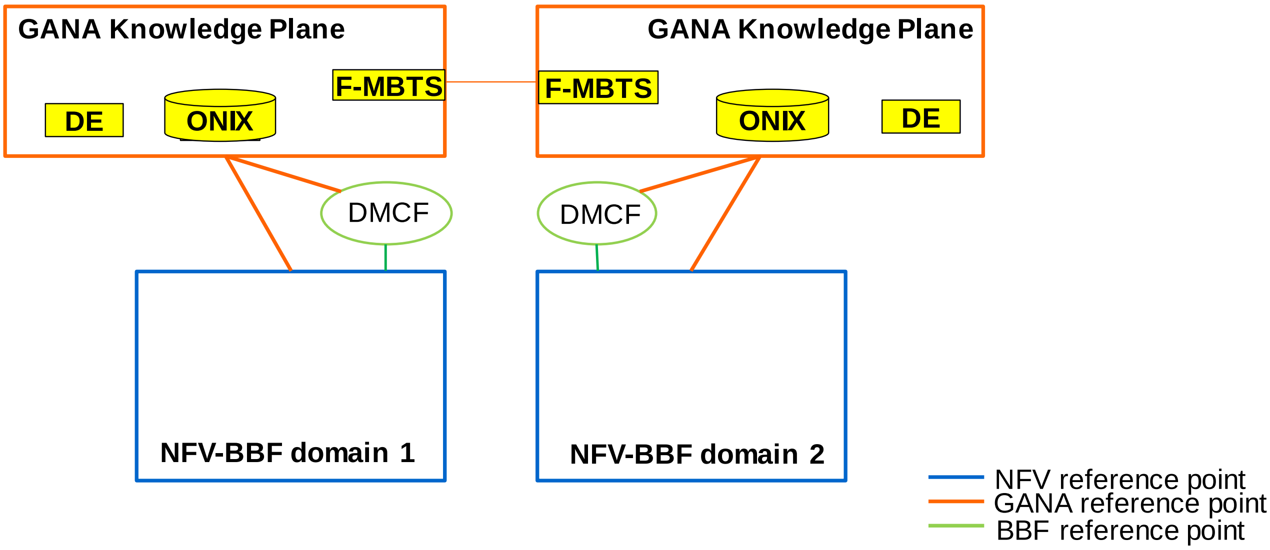


Figure 20: E2E instantiation of the GANA onto the various BBF network domains

9 Interworking and coordination between GANA-BBF and GANA-3GPP (Core Network) in terms of autonomic functions in the two domains

9.1 Introduction

The objective of this clause is to provide recommendations on the interworking between GANA-BBF and GANA-3GPP (Core Network) and between virtualized GANA-BBF and virtualized GANA-3GPP (Core Network) in terms of autonomic functions in the two domains. The study in this clause is in alignment with the work that has been already initiated and is ongoing in both 3GPP and BBF regarding the so called Fixed and Mobile Convergence (FMC) [i.43] and [i.44]. Whereas, such interworking and convergence between BBF and 3GPP domains has been discussed for quite some time now, this clause aims to elaborate architecture recommendation on such an interworking and coordination when both segments are instantiated with GANA autonomic DEs hence being "autonomics-aware". The concept is demonstrated through selected reference architectures and recommendations on the interworking are given based on a set of selected use cases. Finally, the present document is taking onto consideration both legacy (physical) network architectures but also virtualized ones.

9.2 Overview of BBF-3GPP interworking and reference architecture

As already stated in the introduction of this clause, there is already quite some work that has been done regarding interworking between BBF and 3GPP network domains under FMC. The goal of FMC is briefly, to deliver any service, anytime and anywhere and independently of the access technology, whereas at the same time utilizing available resources in the most efficient way for providing the optimum user experience.

In particular BBF TR 203 [i.36] and ETSI TS 123 139 [i.37] define a large set of different architectures to support different scenarios.

BBF TR 203 [i.36] summarizes the above different aspects and scenarios in the reference architecture in Figure 21 below, where interworking is being looked at from both the user plane and control plane perspectives. In particular, in this reference architecture the following points are in common for a various set of more specific architectures and scenarios:

- Interfaces for User Plane communication such as S2a, S2b or S2c taking into consideration an end-to-end approach for traffic forwarding (e.g. QoS consideration).
- Interfaces for Control Plane communications such as:
    - STa/SWa for Authentication, authorization and accounting.
    - S9a for policies management.

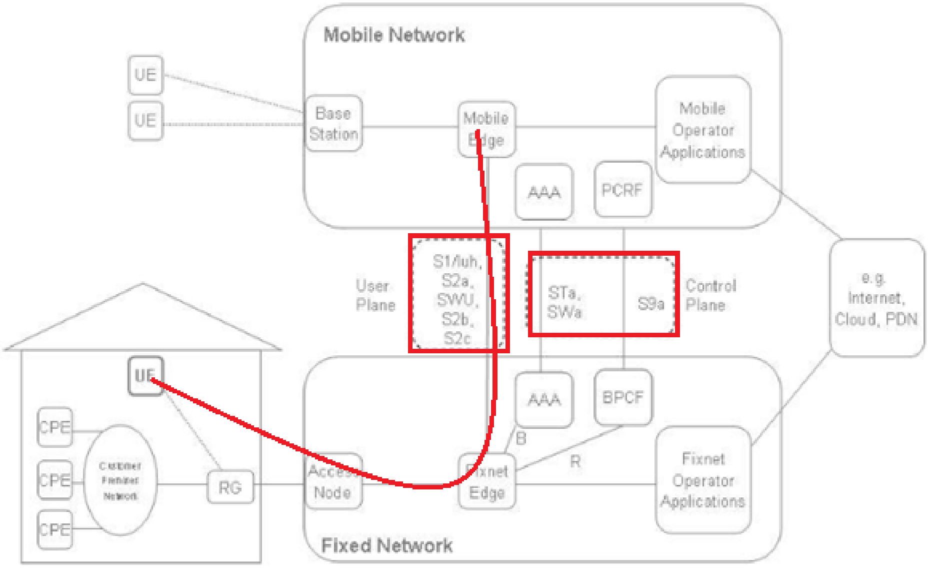


Figure 21: 3GPP Interworking Reference Architecture from BBF TR 203 [i.36]

On the other hand, and from the 3GPP perspective, 3GPP specified the EPC as one common core network for several heterogeneous accesses in Release 8 [i.38] and [i.39] and developed features for supporting non-3GPP accesses, including multi-access PDN connectivity (MAPCON) [i.38] and [i.39], IP flow mobility (IFOM), seamless WLAN offload [i.40], and non-seamless WLAN offload [i.39], in Release 10. Moreover, 3GPP Release 11 has specified the interworking architecture between a 3GPP system and a fixed broadband access network defined by BBF to provide IP connectivity to 3GPP user equipment (UE) connected to a fixed broadband access network [i.37].

By taking into account what has been already done so far, it seems that the main problem was associated with interworking and convergence of Policy control. Accordingly, the interworking architecture focuses mainly on how the different policy, QoS and charging systems of the 3GPP system and the fixed broadband access network can interwork and exchange information or at a next step, result in a convergent architecture with a common/federated mechanism for policy control and QoS, handling both the 3GPP and fixed broadband access networks.

For such policy and QoS interworking between a 3GPP system and a fixed broadband access network, two architecture models could be considered in general as follows:

- Interworking architecture using WLAN access.
- Interworking architecture using H(e)NB.

Another distinction among the architectures is done based on the types of traffic as follows:

- EPC-routed traffic: User plane traffic could be routed back to EPC; that is, the traffic which is routed via a P-GW in EPC as part of a PDN connection [i.37].
- Non-seamless WLAN offloaded traffic: The specific IP flows could be routed over WLAN access to the local wireline network without traversing the EPC, and it was defined as non-seamless WLAN offload (NSWO) in [i.39].

Moreover, the interworking architecture can support both the scenario of a single network operator deploying both 3GPP EPC and BBF network and the scenario of two different network operators deploying the 3GPP EPC and the BBF network, respectively. Finally, it can support the roaming scenarios between two 3GPP mobile operators, however in the present document, non-roaming architectures are only considered. Focusing now on interworking architecture using WLAN access and for EPC-routed traffic, the respective architecture model supports the following mobility management schemes based on 3GPP Release 10:

- Host-based mobility management (via S2c interface) for trusted access or untrusted access.
- Network-based mobility management for untrusted access (via S2b interface).

All in all, without loss of generality and for simplicity reasons, the interworking architecture in Figure 22 is summarizing various aspects above and is selected herewith as a reference architecture for demonstrating the interworking of GANA instantiated BBF and 3GPP domains. More specifically, the figure depicts the non-roaming interworking architecture using network-based mobility for an untrusted WLAN fixed broadband access network based on the S2b interface. As shown in the figure, important entities for the interworking besides the evolved packet data gateway (ePDG), are PCRF and broadband policy control function (BPCF), as well as interfaces for the interworking, which are either newly defined (e.g. S9a, Gxb*) or enhanced from existing 3GPP interfaces (e.g. Gx, S2b). Finally, this reference architecture is applicable when the 3GPP and Fixed Broadband access networks belongs to the same network operator or to different network operators.

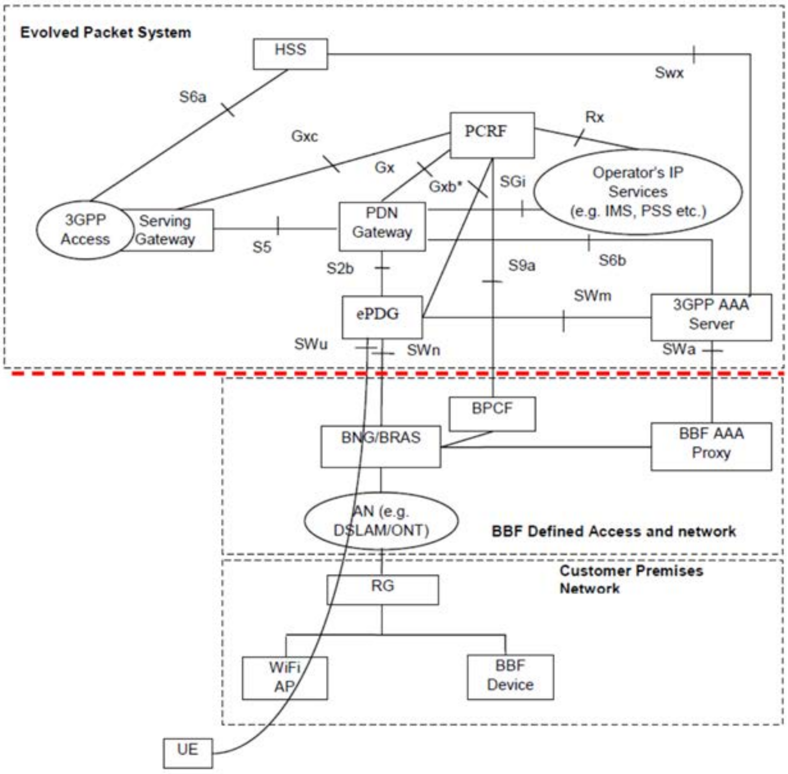


Figure 22: Non-Roaming Architecture for untrusted Fixed Broadband access network based on S2b [i.37]

9.3 Introducing autonomics into interworking BBF and 3GPP segments and identification of potential interactions

9.3.1 Overview

In essence, autonomics through the instantiation of GANA into the reference architectures can prove beneficial for the management in terms of:

- Automating inter-domain QoS policies exchanges between PCRF and BPCF and/or creating policies based on the acquired knowledge and awareness of the network.
- Automating configurations for accounting session based on service providers agreement (single session, two session, etc.) between AAA platforms.
- Improving end-to-end QoS for the User Plane by applying the best profiles according to network conditions over time.

The following clauses aim at providing more details but also recommendations on the interactions among GANA entities when instantiated in the two domains. The interworking of GANA autonomic elements is initially demonstrated in a generic case for end-to-end QoS preservation and then, through two use cases, directly inspired from the ones elaborated in ETSI TS 122 278 [i.41] and BBF TR 203 [i.36], namely:

- Application continuity between segments
- Dual WAN connectivity

9.3.2 Recommended interactions for End-to-End QoS

Customer experience can suffer from insufficient QoS configurations on network elements when traffic is forwarded through different networks operated by different service providers. Autonomics can solve this issue by implementing DEs into the GANA knowledge plane in order to dynamically change QoS profiles applied on network elements and use the most appropriate combination depending on network conditions.

As shown in Figure 23, network conditions are monitored by the "Monitoring-DE" instantiated in the Knowledge Plane on each service provider. "Monitoring-DE" collects piece of information from "Monitoring-ME" (not represented in Figure 23) implemented in network equipment. "Network Analytics" modules analyses collected information to give an overview of the network conditions at any time. Based on this information and supported by the communication interface between both Knowledge Planes, QoS policies are enforced on network equipment in a coordinated and efficient manner.

The type of data that can indicatively be considered as inputs from the 3GPP domain are:

- Radio Network utilization by information flows.
- User Equipment (UE) measurements.
- Average response time.
- Availability.
- Faults.
- Packet loss.
- Latency.
- Location information, coverage.
- Mobility parameters or patterns.
- Capacity utilization.
- Parameterization of common channels.
- QoS and flow characteristics.
- Throughput and connectivity parameters.
- Network security monitoring.
- Reference Signal Received Power (RSRP) and Reference Signal Received Quality (RSRQ) coming from the serving and neighbouring eNBs for UEs.

For the BBF domain, indicatively the potential metrics are (more detailed metrics can are addressed at BBF TR 304 [i.42]):

- Bandwidth consumption.
- Resource utilization by function or service type.
- Network security monitoring.

- Network flows and QoS.
- Rate, interface type and protocol.
- Throughput (mainly TCP).
- Network performance monitoring-delay, jitter, packet loss, packet ordering, and packet corruption in the network.
- Faults.
- Edge-to-edge network availability monitoring.

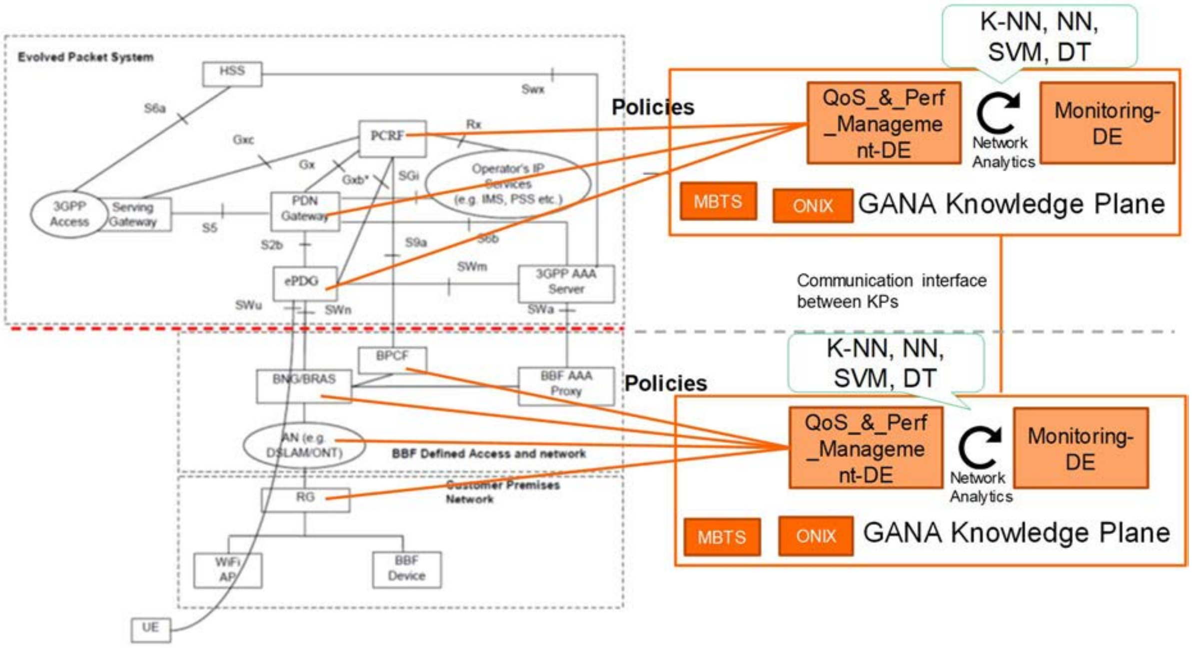


Figure 23: Policy exchanges between both domains and policies enforcement through Knowledge Plane

Note that "QoS_&_Perf_Management-DE" can also be named "QoS and QoE Management DE".

The aforementioned data types are used in order to feed the Network Analytics functions in the Knowledge planes, thus deriving the policies that are enforced on the Network domains (BBF and/or 3GPP). The main outcomes from the Network analytics support the classification of network status and service demands, enable the prediction of specific operational pattern appearances in the networks and provide Application aware configurations for the Network domains and users.

9.3.3 Recommendations for autonomic interworking between BBF and 3GPP segments through exemplary use cases

9.3.3.1 Application continuity between segments

The BBF and 3GPP interworking is highly dependent upon the policy exchange for the seamless application provision between the involved network segments. The policies enable the faster and synchronized triggering of segment components in order to accommodate the application continuity between the segments in a way transparent to the end user. The main entities involved in the interactions are the PCRF and BPCF for the policy exchange and the deployment of the relevant policies to the other networking components.

Table 13: Example Use Case on autonomic interworking between BBF and 3GPP segments

Use case name	Application continuity between segments
Description/Storyline Use Case	The children in the backseat of the car are watching an Internet TV show on their laptop using a 3GPP Radio Access Network connection to the Internet TV Provider while travelling home from the grandparent's house. Once home, the terminal detects indoor Wi-Fi coverage where the subscriber has a Wi-Fi Residential Gateway connected to the fixed broadband network. The network segments autonomically can select to switch the connection or the terminal can automatically select to switch the IP connection to the fixed broadband connection and enable the user to resume watching the same TV show on the same laptop, based on network level policies, possibly with a better quality picture as allowed by the available bandwidth, user-specific policy, network policy and QoS setting.
Network Environment(s)	3GPP - BBF segments interworking.
Problems	Interworking between BBF - 3GPP segments.
Functions Impacted	Self-configuration, Self-optimization.
Systems Involved	Mainly PCRF, BPCF, (implicitly, CPE, Access Nodes, Aggregation nodes, BNG, MME).

The GANA knowledge plane enriched with the ability to create policies based on the acquired knowledge and awareness of the network overview enables the policy fusion towards all network segments and their policy management functions. The GANA Knowledge Plane enables Network Analytics deriving policies for Application aware configurations for the Network domains and users. Data types that are considered for the specific use case are mainly (but not limited to) availability, performance, latency, bandwidth, QoS and flow characteristics. The GANA policy framework enables dynamic behaviours through the policy exchange, including providing policy capabilities that allow QoS, bandwidth, and access control for various application sessions that a roaming device can establish. The policy framework can fuse generic policies, e.g. session independent policies for the QoS and resource access between segments, but also provide session or call specific dynamic policies based on user and network policies and capabilities. In this case, the basic steps for the use case addressed above, would involve the interaction of GANA knowledge plane and policy framework exchange and PCRF, BPCF in order to establish both the generic session independent policies for the interworking between the BBF and 3GPP segments and in order to address the dynamic behaviours, more specific policies can be dynamically fused per call, per session, per user etc. In such cases, a potential protocol to be used would be DIAMETER, since it provides compatibility also with the S9a session establishment between PCRF and BPCF which will be used for the exchange between the peer nodes. The autonomic policies for the generic interworking rules between the two segments will apply initially and as soon as user specific profile and information is exchanged, then more dynamic and advanced policies are to be triggered for the dynamic accommodation of QoS and other user or network specific requirements and policies.

The generic policies for the interworking between the segments enable the initial establishment of the S9a session between the BPCF and PCRF. In this case, a unique client generated "session-id" is created to identify the particular session associated with the 3GPP UE. These sessions however run over the same S9a connection between two Diameter peer nodes given that further S9a sessions per 3GPP UE are between the same network domains, i.e. same realms between the Diameter nodes. The PCRF can trigger the BPCF to initiate S9a session establishment if it becomes aware (e.g. via tunnel authentication to the 3GPP network) that a 3GPP UE has attached via the BBF access to WLAN or when the UE perform an attachment to the H(e)NB, and the PCRF is able to find a corresponding BPCF. The BPCF should be capable of receiving the trigger information from the PCRF, which can include the IMSI, APN, in case of UE connected to the WLAN, the local UE IP address assigned to the 3GPP UE or the IP address locally assigned to the H(e)NB by the fixed broadband network. In SDN and NFV enabled environments, the policy framework concentrates on the policy integration between the controller(s) and the respective network functions PCRF, BPCF. In this case the SDN related policies become network policies and can be instantiated as dynamic policies for per-call, per-session, etc. targeting the requirements accommodation for QoS.

Figure 24 depicts GANA knowledge planes and policy interfaces enabling autonomic interworking between BBF and 3GPP segments.

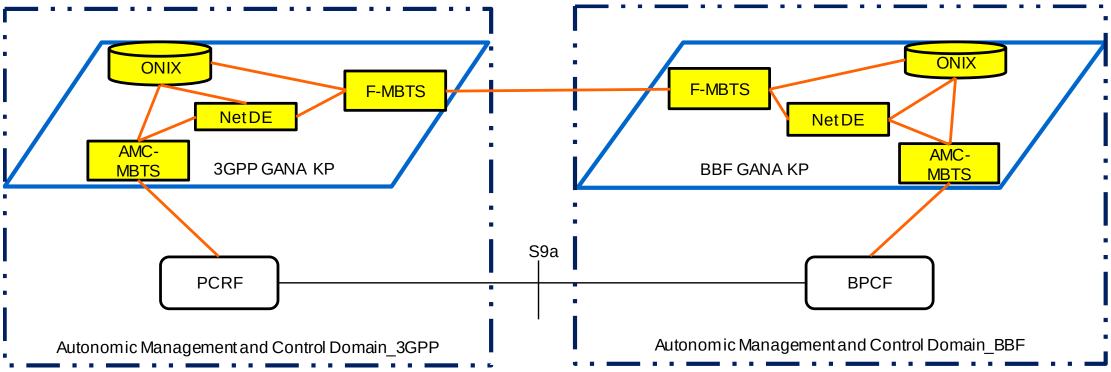


Figure 24: GANA knowledge planes and policies enabling autonomic interworking between BBF and 3GPP segments

The KP can be separated for the two network domains fixed and mobile as they could be owned by different providers. Furthermore information (operation/primitives) exchanged between 3GPP and BBF may need a transformation to be used in the fixed and in the mobile network as they do not use the same data model. The federation-MBTS can be used to translate the information and secure the information exchanged. The reference point between F-MBTS can be a direct link (point to point).

9.3.3.2 Dual WAN connectivity

The 3GPP network is expected to be used also for backup WAN connectivity in cases of fixed network failure. The BBF and 3GPP interworking can facilitate the connectivity continuity, related to fault or failure management and healing. In this context, the knowledge of a fixed network failure is important to be shared among the respective domains, in order to trigger the reservation of network resources in the 3GPP network and the policy exchange for the continuation of application provision between the involved network segments. In order to avoid major service disruption for the user, the knowledge plane is expected to provide a common substrate for the management of both domains. The main entities involved in the interactions are the GANA Knowledge Plane, the PCRF and BPCF for the failure identification, the planning of related reconfigurations on network elements for optimal resolution of the service continuity through the backup segment (3GPP), as well as policy exchange and the deployment of the relevant policies to the involved networking components. The GANA Knowledge Plane enables Network Analytics deriving policies for the classification of network status and service demands for the Network domains and users. Data types that are considered for the specific use case are mainly (but not limited to) fault, throughput and connectivity parameters, availability, User Equipment (UE) measurements, performance, latency, bandwidth, QoS and flow characteristics.

Table 14: Example Use Case on Knowledge based autonomic interworking between BBF and 3GPP segments for fault and failure management (Dual WAN connectivity)

Use case name	Application continuity between segments
Description/Storyline Use Case	A subscriber has an RG connected through the fixed broadband network. The RG also has an embedded 3G modem that provides a back-up WAN connection through the 3GPP mobile network, when the fixed broadband network is unavailable. The subscriber is using broadband services, such as IP telephony, IPTV and web access. When the fixed broadband network gets disconnected inadvertently, some of the ongoing communications are automatically switched to the backup WAN connection and through the 3GPP network: the voice conversation is not disturbed by this event and continues seamlessly; HD-TV is interrupted as the bandwidth of the mobile network does not support that service; Internet service is maintained, but with a reduced bandwidth. Similarly, when the fixed broadband network is re-established, communications ongoing through the 3GPP network switch are switched back seamlessly to the fixed broadband network, without perceptible interruption by the end-user.
Network Environment(s)	3GPP - BBF segments interworking.
Problems	Interworking between BBF - 3GPP segments.
Functions Impacted	Fault Management, Self-Healing, Self-configuration, Self-optimization.
Systems Involved	Mainly Knowledge Plane, PCRF, BPCF, (implicitly, CPE, Access Nodes, Base Station, Mobile Edge), AAA.

The GANA knowledge plane is expected to provide a common "fabric" for the knowledge exchange and monitoring between BBF-3GPP segments. The GANA Knowledge plane is expected to support the identification of fault and failures in the fixed network and plan the course of action for the triggering and configuration of autonomic network elements in order to optimally support the service continuity for the end user, when service is necessary to be backed up by the 3GPP segment. GANA knowledge plane enriched with the ability to create policies based on awareness of the network overview enables the fault identification and policy fusion towards all network segments and their policy management functions. The GANA policy framework enables dynamic fault management through planning of optimal reconfigurations of network segments in order to support the user connectivity continuity by the backup network segments and elements. The service is resumed through the 3GPP network components for the optimal support of the end user. Thus, the policy framework can fuse policies for resource access between segments, but also provide session or call specific dynamic policies based on user and network policies and capabilities. In this case, the basic steps for the use case addressed above, would involve the interaction of distributed GANA knowledge plane for the fault or failure identification between network components, as well as the policy framework exchange between PCRF, BPCF in order to establish the resource allocation for the backup connectivity between the BBF and 3GPP segments and the service and application continuity.

In order to address the service requirements, some policies are expected to be pre-installed in order to enable the fast reaction of the network elements to the fault/failure, while more specific policies (e.g. for routing) can be dynamically fused per call, per user, etc. The autonomic policies for fault and failure management rules between the two segments will apply initially and as soon as user specific profile and information is exchanged, then more dynamic and advanced policies are to be triggered for the dynamic accommodation of application and other user or network specific requirements. Finally, for authorization and authentication of a BBF user on a 3GPP access network, the 3GPP AAA infrastructure and BBF AAA infrastructure will exchange parameters using the STa or SWa interface as appropriate.

Figure 25 depicts GANA knowledge planes and policy interfaces enabling autonomic fault management and interworking between BBF and 3GPP segments for service continuity.

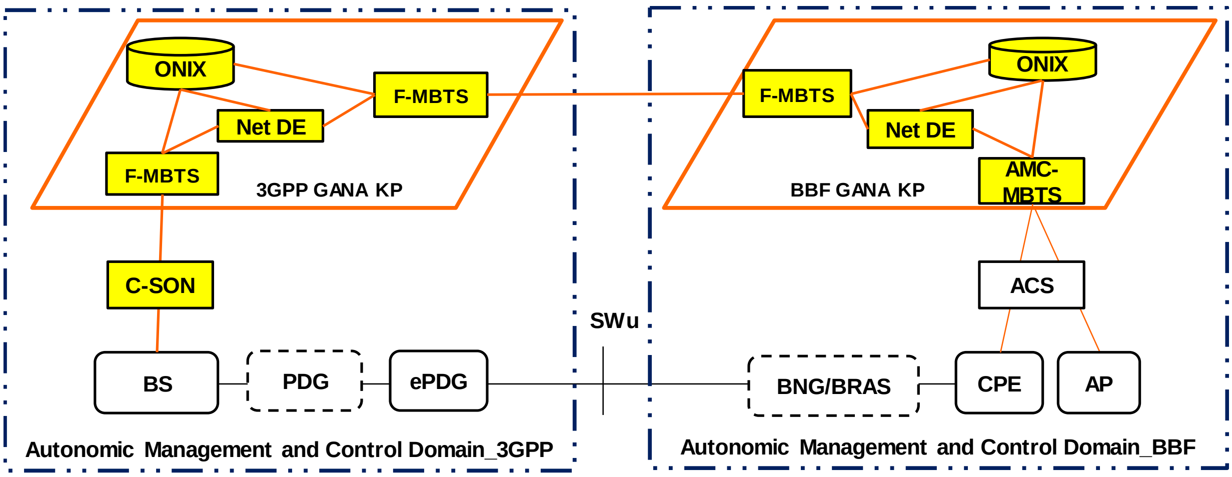


Figure 25: GANA knowledge planes and policies enabling autonomic fault management and interworking between BBF and 3GPP segments for service continuity

As in the previous case, two separate KPs are instantiated, yet in this case the 3GPP GANA KP retrieves information from the BS through the C-SON which self-manages the Radio access network. Information (operation/primitives) exchange between the mobile network and the fixed network can require dedicated reference points to ensure fast decision (connect the CPE to a BS in case of fixed network failure).

9.3.4 Interworking among virtualized BBF and 3GPP segments

In clause 7 of the present document, the BBF SDN enabled architecture and the BBF and ETSI NFV architectures were addressed in the context of instantiating the GANA model features into the respective virtualized component architectures. The proposed mappings in Figure 7, Figure 10 and Figure 11, are generic as to cover similar instantiation of GANA autonomics in the case of an underlying virtual EPC [i.5].

When it comes to the interworking between the two domains (BBF and 3GPP), both the 3GPP and BBF networks can manage only their own domain (virtualized or not virtualized) with separate MANO and GANA KPs. However, from an E2E decision making perspective across those two domains, there is a need for exchanging information crossing both GANA KPs K (3GPP GANA KP and BBF GANA KP).

With this respect, the 3GPP core network GANA KP can schedule the information exchange with the fixed network (BBF network) and the different domain of the mobile network or vice versa. This requires specifying a reference point between both GANA KPs.

The above are depicted in Figure 26.

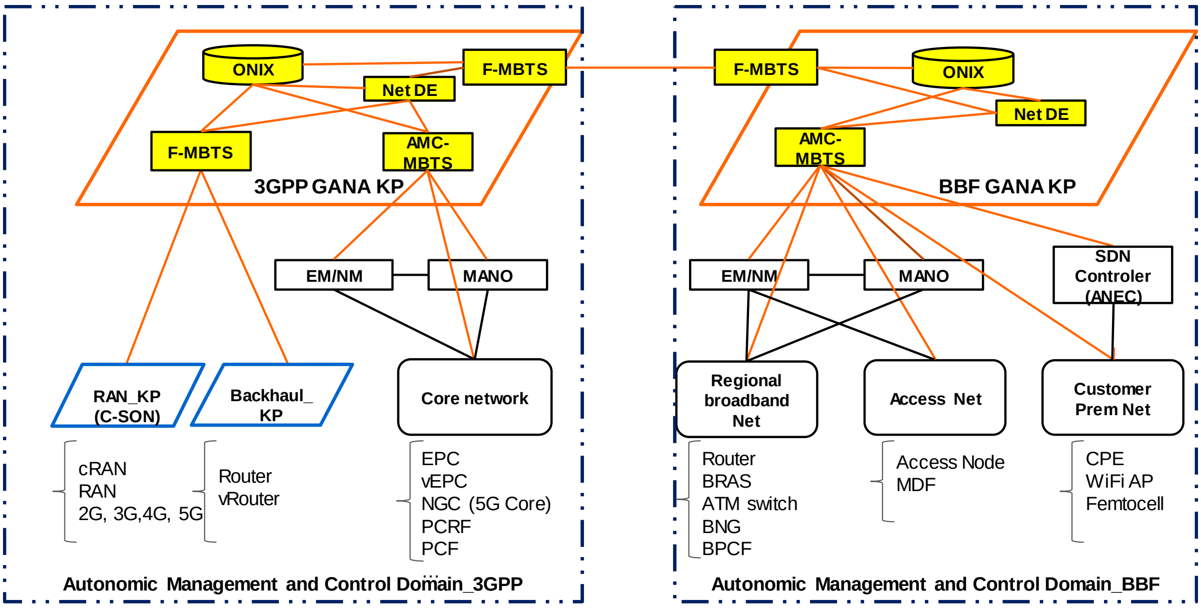


Figure 26: Proposed option for interworking between virtualized BBF and 3GPP Networks

Regarding 5G Fixed-Mobile Convergence, one could consider a single GANA-enabled MANO architecture but a specific study need to be carried out to conclude what would be the requirements to be derived from this use case.

10 Conclusions and Future work

The present document reports on the feasibility and recommendations for introducing autonomics in fixed broadband networks by elaborating several use cases and scenarios and eventually, by recommending the instantiation of various GANA DEs into the (both physical and virtualized) core elements and functions of the broadband architecture(s) specified by the BBF. It further elaborates and provides recommendations on the GANA instantiation in the case of interworking scenarios and architectures between BBF and 3GPP core network domains.

Furthermore, the following (non-exhaustive) list comprises an outlook of work items that could be launched to extend the present document regarding the introduction of autonomics in BBF architectures. Essentially this could include:

- Studying a framework for DE-to-DE coordination for conflict avoidance and stability: This would include definition of primitives and associated data model for DE coordinations, application of techniques such as Virtual Synchrony, etc.
- Adoption and extending of existing policy control frameworks for enabling dynamic policy generation and application by DEs in policy continuum.
- Setting up of GANA PoCs for AMC in BBF architectures that are based on the work of the present document.
- Derivation of concrete requirements for protocols and APIs for enabling GANA based Autonomics, cognitive Networking and self-management of networks and services in evolving and future networks.
- Extending the work in the present document to cover 5G related impacts such as Autonomic Management and Orchestration of Network Slices; and Autonomic Service Assurance for the Network Slices by Federated GANA Knowledge Planes in the context of Fixed 5G networks and Interworking with Mobile 5G Networks.
- Addressing the Requirements for Protocols and APIs for Enabling GANA based Autonomics, Cognitive Networking and Self-Management of Networks and Services in Evolving and Future Networks outlined in Annex B of GANA Specification document [i.30].

Annex A: The ONIX System and possible ways to implement ONIX

A.1 Possible Approach to Implementing ONIX and its protocols for ONIX Services

ONIX is characterized by:

- **ONIX Internal Protocols** for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques.
- **ONIX External Protocols** (e.g. DHCPv6++, an IPv6 based protocol that was prototyped in [i.31], [i.33], [i.34], [i.35], gRPC [i.32], or any other protocols that can be used for communicating information in formats that ONIX can be made to support) for supporting the following operations by ONIX users:
  1) Publish Information into ONIX.
  2) Subscribe to receive Information from ONIX, including "on-behalf" subscriptions.
  3) Query and Find Operation to retrieve Info from ONIX.

In terms of Information Servers as members of ONIX, the following types of servers can be distinguished:

- Information Server that stores Info purely in ONIX Native Format such as XML, YANG, and other types that could be supported as ONIX native formats for information communicated to ONIX users (consumers of the Information such as GANA Decision Elements (DEs) or Network Elements (NEs-Physical or Virtual)) or stored by ONIX users intending to store information into the ONIX.
- Traditional Relational Databases that can be made to support ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques, and can convert some data they store into ONIX native formats for information exchange with ONIX users.
- Other Types of Data Storage that can be made to support ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques, and can convert some data they store into ONIX native formats for information exchange with ONIX users.
- Shared Common Repository (R) for State Data (e.g. VNFs (Virtual Network Functions State Data) that is made to support ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques, and can convert some data they store into ONIX native formats for information exchange with ONIX users. Such a Shared Common Repository can still be directly accessible via a Native Data/Info Access Interface it should still expose. Such a Direct Data Access Interface exposed by the Server can support access methods such as LDAP, SPML, Diameter, API, or other methods.
- Some Information Servers that are members of ONIX and also exposing their Server-Native Interfaces for use by some "Non-ONIX Native" Data/Information Repository User. As such server-native Data/Info Access Interface can be exposed by e.g. a Repository or Database that is also a member of ONIX at the same time.

NOTE 1: Data/Information Servers ("N", "X", R") on the Figure A.1 support ONIX Internal Protocols for Federation of Information Servers (i.e. they can be made to operate as ONIX members) and can convert some data they store into ONIX native formats for information exchange with ONIX users.

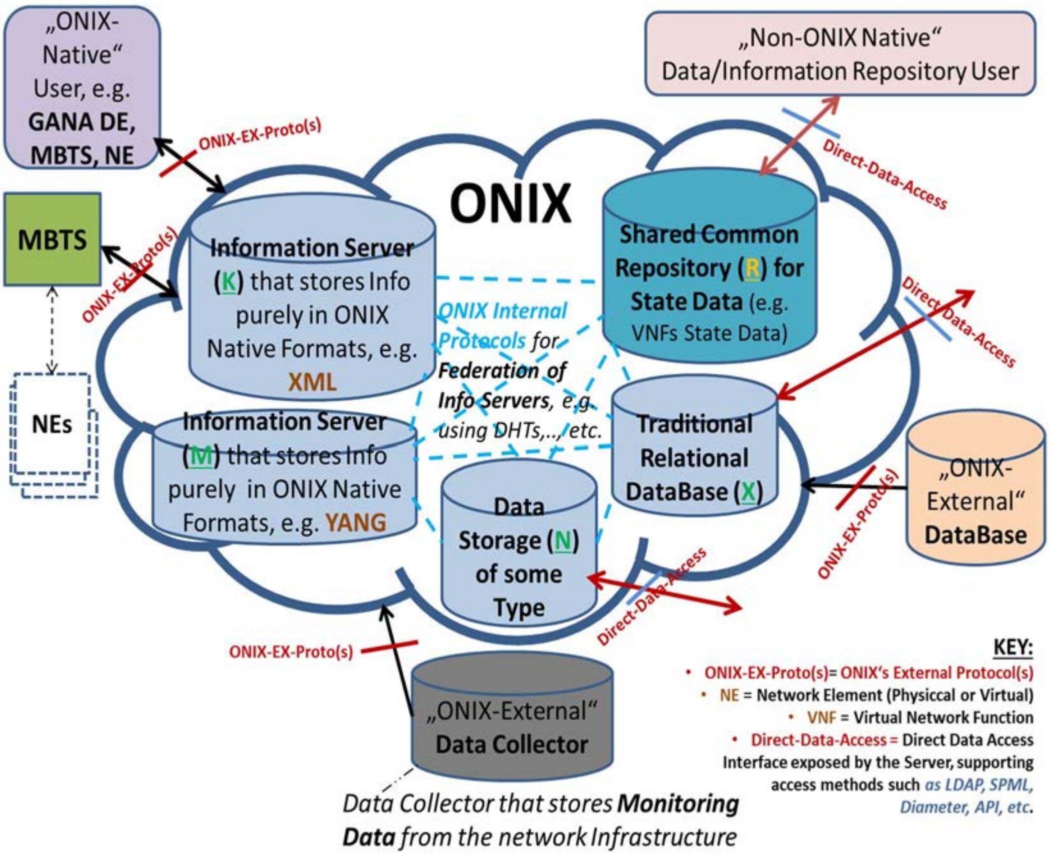


Figure A.1: ONIX Interfaces and Services, Internal and External Protocols [i.30]

Table A.1 provides illustrations of External Interfaces and Services of ONIX, External Protocols and Internal Protocols of ONIX. Figure A.2 provides an illustration of an example approach used in an ONIX implementation of some limited functionality (in reference to [i.31], [i.33], [i.34] and [i.35]).

Table A.1: ONIX Interfaces and Services, Internal and External Protocols

External Interfaces and Services of ONIX	External Protocols	Internal Protocols of ONIX
ONIX-EX-Proto(s) Interface enables "ONIX native" users such as **GANA DE, MBTS, or a GANA Node (NE)** to use the following services of ONIX: • Publish Information into ONIX • Subscribe to receive Information from ONIX • Query and Find Operation to retrieve Info from ONIX	Various external protocols can be supported by ONIX for providing such services, e.g. extended DHCPv6 (DHCPv6++ [i.31], [i.33], [i.34], [i.35]), gRPC [i.32], or any other protocols that can be used for communicating information in formats that ONIX can be made to support.	Various external protocols can be supported by ONIX for ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques.
ONIX-EX-Proto(s) Interface enables ONIX native users such as **"ONIX-External" Data Collector** that stores Monitoring Data from the network infrastructure to use the following services of ONIX: • Publish/Update Information into the ONIX via any accessible ONIX server (Cognitive Algorithms operate on raw data on the Data Collector and create Knowledge stored into ONIX and also streamed to DEs in the GANA Knowledge Plane)	Various external protocols can be supported by ONIX for providing such services, e.g. extended DHCPv6 (DHCPv6++ [i.31], [i.33], [i.34], [i.35]), gRPC [i.32], or any other protocols that can be used for communicating information in formats that ONIX can be made to support.	Various external protocols can be supported by ONIX for ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques.
ONIX-EX-Proto(s) Interface enables ONIX native users such as **"ONIX-External" DataBase** to use the following services of ONIX: • Publish/Update Information into the ONIX via any accessible ONIX server	Various external protocols can be supported by ONIX for providing such services, e.g. extended DHCPv6 (DHCPv6++ [i.31], [i.33], [i.34], [i.35]), gRPC [i.32], or any other protocols that can be used for communicating information in formats that ONIX can be made to support.	Various external protocols can be supported by ONIX for ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques.

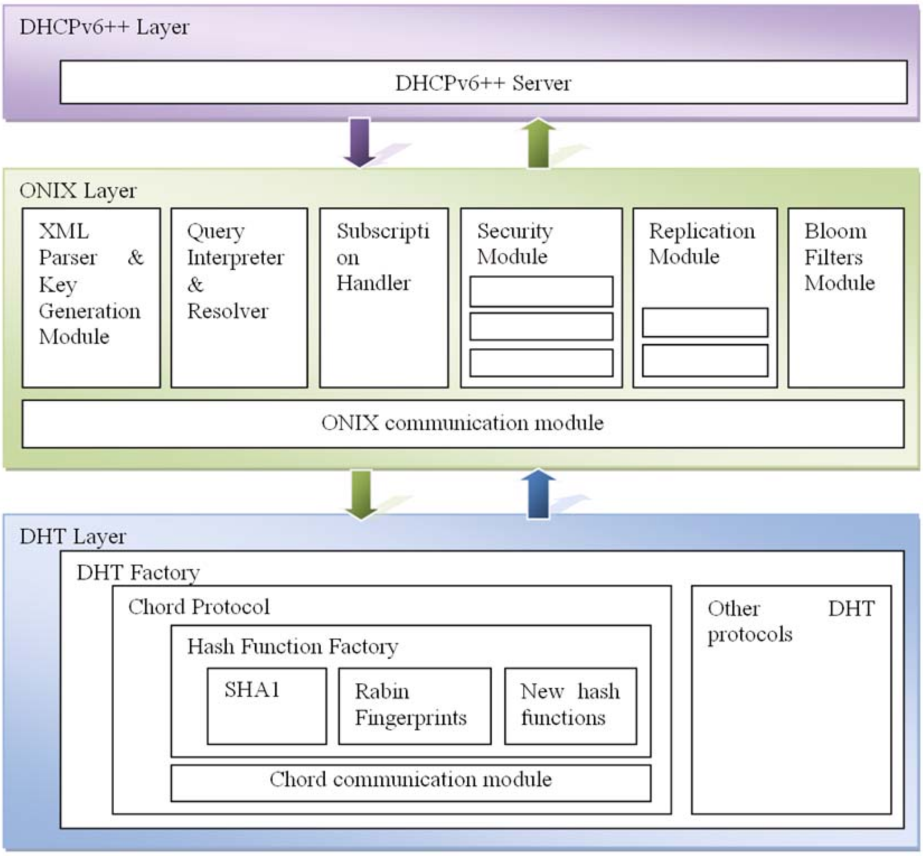


Figure A.2: An illustration of an example approach used in an ONIX implementation of some limited functionality (in reference to [i.31], [i.33], [i.34] and [i.35])

NOTE 2: There are other sources of resourceful concepts and insights in literature that may be considered in implementing ONIX capabilities such as context storage (and possibly processing as well) and brokerage, and metadata management for the various data models the ONIX servers may be designed to use in information stored on some ONIX servers and also for information exchanged between ONIX and its user entities. For example, Fi-WARE concepts and insights from [i.45] that relate to context storage, context brokering and metadata management for data models can be exploited in the design and implementation of the ONIX servers.

Annex B: A GANA Instantiation onto other SDAN Scenarios, but can only be applied if such SDAN scenarios are permissible by BBF standards (e.g. TR-384, TR-370, etc.)

NOTE 1: SDAN (Software-Defined Access Network) scenarios standardized by BBF are described in published BBF documents such as BBF TR-384 [i.53] and BBF TR-370 [i.26]. GANA instantiations for such SDAN scenarios are described in the core clauses of the present document, e.g. the integration of the GANA Knowledge Plane in the CloudCO architecture and environments described in BBF TR-384 [i.53]. This annex considers other SDAN scenarios that possibly may not be directly supported by BBF standards such as BBF TR-384 and BBF TR-370. Such other scenarios on SDAN include the ones described in [i.55]. Therefore, before implementing the GANA instantiation onto such other SDAN Scenarios described in this annex and have been discussed in BBF and in industry in general, the implementer should first ensure that these other SDAN scenarios are permissible by BBF Standards that touch on SDAN such as BBF TR-384 [i.53] and BBF TR-370 [i.26], before implementing the corresponding recommendations on the instantiation of GANA autonomics in such SDAN scenarios as described in this annex.

The other SDAN scenarios that have been discussed in BBF and in industry in general relate to implementation of SDAN by defining a set of control plane components that can be localized in the SDN controller or externalized into a physical access node. For example, some proposals in the industry had defined so-called Access Node Localized Control (ANLC) functions by which an SDN controller can delegate control functions to an SDAN network element, functions such as Spanning Tree Protocol (STP), Link Aggregation Control Protocol (LACP), Ethernet Ring Protection Switching (ERPS), Operations, Administration and Management (OAM), etc. The proposals also defined so-called Access Node Externalized Control (ANEC) functions, by which an SDN controller also has the option to run control protocols itself (for example, IGMP processing, DHCP relay, IEEE 802.1X [i.52] Authenticator, etc.). However, this SDAN approach is slightly different from the approach advocated for in the case of CloudCO environments described in BBF TR-384 [i.53], while BBF TR-370 [i.26] could possibly support this other approach involving implementation of SDAN by defining a set of control plane components that can be localized in the SDN controller or externalized into a physical access node.

NOTE 2: Readers and GANA autonomics implementers should ensure that there are BBF standards that involve SDAN related topics that support the SDAN scenarios described below, involving the implementation of SDAN by defining a set of control plane components that can be localized in the SDN controller or externalized into a physical access node. This should be done in oder to be compliant with BBF standards when implementing the instantiation of GANA autonomics for such SDAN scenarios as described below in this annex.

Based on such an approach of having some control functions delegated to an SDAN network element while some control functions are implemented in an SDN Controller, the implication of mapping of GANA DEs to SDAN (AN node) functions and Managed Entities (MEs) is such that the main autonomic capabilities can be split between the SDN controller and the SDAN Network Element as described in Table B.1 and the figures and descriptions that follow in this annex.

Table B.1: Separation of autonomic features and capabilities between SDAN Network Element and SDN Controller

Decision Element (DEs)	The AN Functions - Managed Entities (MEs)	SDAN Network Element	SDN Controller
NODE_LEVEL_AC_DE - Node-Level Auto-Configuration Decision-Element	Auto-configuration of Access Nodes Auto-discovery of Access Nodes and others nodes Bulk provisioning Ethernet interfaces PON interfaces (DBA configuration) xDSL ports (profiles configuration)	X	
NODE_LEVEL_R&S_DE - Node-Level Resilience & Survivability Decision-Element	Software upgrade Dual-Homing Link Aggregation RSTP/MSTP	X	
NODE_LEVEL_SEC_DE - Node-Level Security Decision-Element	ACL configuration Traffic filtering (broadcast, mac address filtering& flooding) Control-plane protection IEEE 802.1X [i.52] Authenticator	X	
NODE_LEVEL_FM_DE - Node-Level Fault-Management Decision-Element	Diagnostic tools Hardware faults detection and report	X	
FUNC_LEVEL_MON_DE - Function-Level Monitoring Decision-Element	OAM Synchronization	X	
FUNC_LEVEL_GCP_M_DE - Function-Level Generalized Control Plane-Management Decision-Element	DHCP relay PPPoE Relay IGMP snooping/ proxy		X
FUNC_LEVEL_QoS_M_DE - Function-Level Quality of Service-Management Decision-Element	Traffic classification Queue configuration (buffer allocation) MTU	X	
FUNC_LEVEL_DP&FWD_M_DE - Function-Level DataPlane&Forwarding-Management Decision-Element	Auto-sensing of protocol encapsulation VLANs handling VLAN forwarding (1:1 or 1:N) MPLS Adaptation Module Multicast forwarding	X	
FUNC_LEVEL_RT_M_DE - Function-Level Routing-Management Decision-Element	Routing protocols		X
FUNC_LEVEL_SM_DE - Function-Level Service-Management Decision-Element			

The mapping of the GANA DEs to SDAN can be done in two different ways for such SDAN scenarios:

- The first solution is depicted on Figure B.1 and shows the mapping of GANA DE to SDAN according to Table B.1. This approach can be seen as a first option for implementing GANA model into SDN-based architecture.

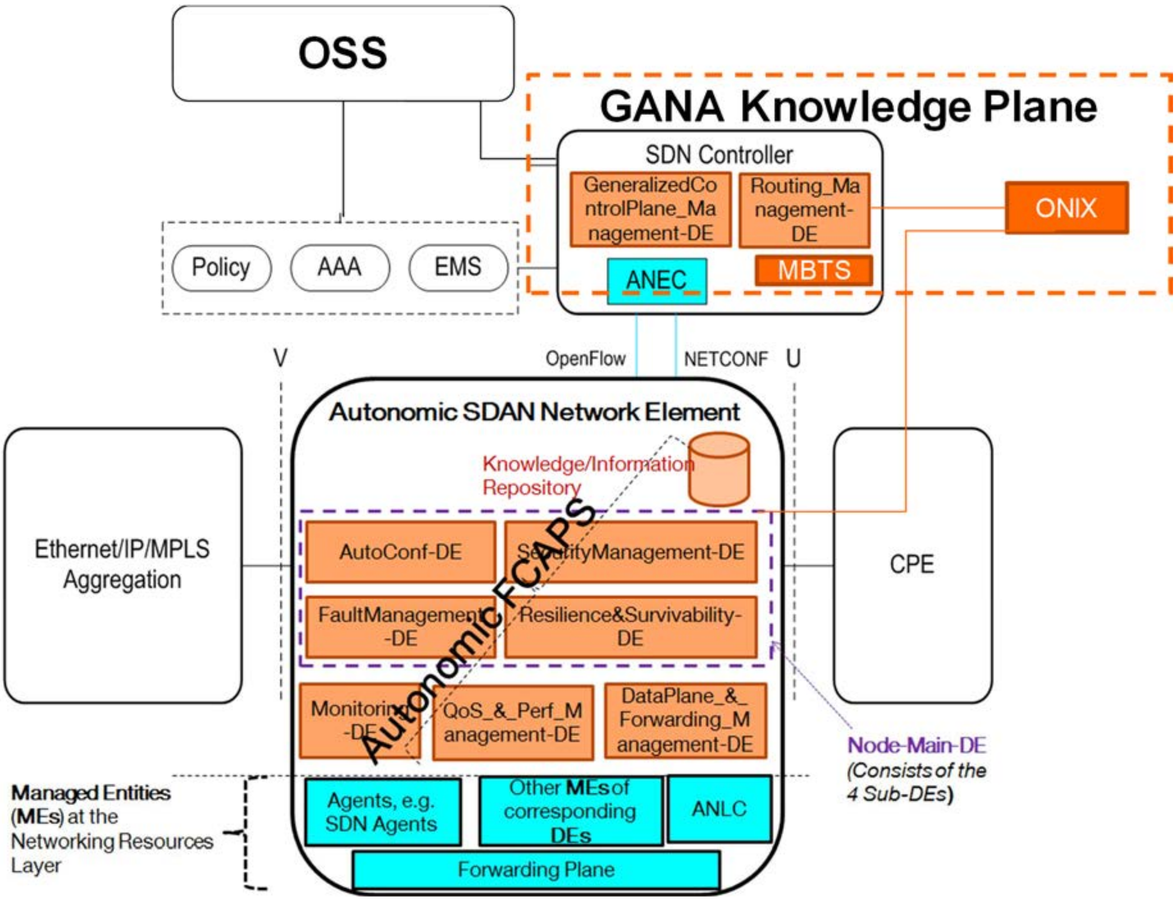


Figure B.1: GANA instantiation on SDN/NFV architecture for Virtual AN - Option 1

- The second option is depicted on Figure B.2 and shows the mapping of GANA "ANEC-related" DE on top of the SDN controller. This second approach introduces no impact on the SDN controller. "ANEC-related" DE are implemented in the knowledge plane and interact with the SDN controller through its northbound interface.

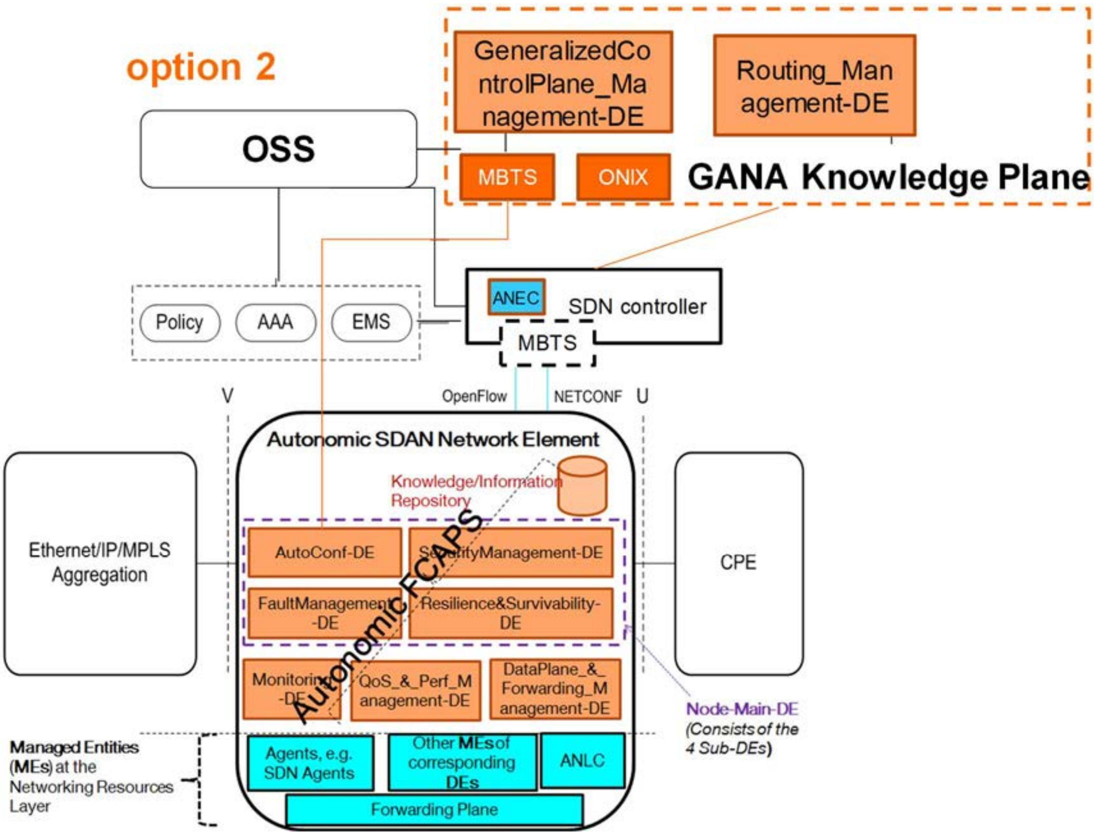


Figure B.2: GANA instantiation on SDN/NFV architecture for Virtual AN - Option 2

Dynamic (Autonomic) Management and Control aspects that can be addressed by the DataPlane_&_Forwarding_Management-DE in an SDAN element include dynamic management of OAM aspects as well as the following aspects:

- **Dynamic (Autonomic) Management of LACP** forwarding based on local and/or network events and at the same time in respect of the external governing policies enforced by a management and control system such as the SDN-Controller or the Knowledge Plane. The DE algorithm developer can use any Managed Objects (MOs) defined for the LACP to determine what could be dynamically (autonomically) configured/adjusted for LACP's operation to achieve a certain goal by virtue of the DE algorithm innovation. Such dynamic management performed by the DE can be based on various data sources (including local data sources within the SDAN network element). The MOs that the DE designer can consider in designing the DE can come from the corresponding MIBs (Management Information Bases) available for LACP.

- **Dynamic (Autonomic) Management of STP** based on local and/or network events and at the same time in respect of the external governing policies enforced by a management and control system such as the SDN-Controller or the Knowledge Plane. The DE algorithm developer can use any Managed Objects (MOs) defined for the STP to determine what could be dynamically (autonomically) configured/adjusted for STP's operation to achieve a certain goal by virtue of the DE algorithm innovation. Such dynamic management performed by the DE can be based on various data sources (including local data sources within the SDAN network element). The MOs that the DE designer can consider in designing the DE can come from the corresponding MIBs (Management Information Bases) available for STP.

- **Dynamic (Autonomic) Management of ERPS** based on local and/or network events and at the same time in respect of the external governing policies enforced by a management and control system such as the SDN-Controller or the Knowledge Plane. The DE algorithm developer can use any Managed Objects (MOs) defined for the ERPS to determine what could be dynamically (autonomically) configured/adjusted for ERPS's operation to achieve a certain goal by virtue of the DE algorithm innovation. Such dynamic management performed by the DE can be based on various data sources (including local data sources within the SDAN network element). The MOs that the DE designer can consider in designing the DE can come from the corresponding MIBs (Management Information Bases) available for ERPS.

Annex C: Bibliography

- ETSI TS 103 371: "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Proofs of Concept Framework".
- Krzysztof Cabaj, Krzysztof Szczypiorski and Sheila Becker: "Towards Self-defending Mechanisms Using Data Mining in the EFIPSANS Framework", Published in: N.-T. Nguyen et al. (Eds.): Advances in Multimedia and Network Information System Technologies: AISC 80, pp. 143-151.

Annex D: Change History

Date	Version	Information about changes
December 2016	0.0.1	First publication of the TR for TC NTECH #17
January 2018	1.1.0	This version V1.1.1 took into consideration the comments received during the discussions between ETSI TC NTECH AFI WG and BroadBand Forum (BBF) from the following meetings held under the liaison between ETSI NTECH AFI WG and BroadBand Forum (BBF): • ETSI TC NTECH AFI WG Presentation and discussions with BBF A&M: held 30th January 2017 as Virtual Meeting • Joint Session with BBF A&M and R&T WAs and ETSI TC NTECH AFI WG on Autonomic Networking, held 21st March 2017 during the BBF Q1 2017 Meeting in Chicago, USA
May 2018	1.1.0	This version was created after ETSI NTECH AFI WG made a presentation of this ETSI TR 103 473 to BBF during the BBF meeting in Athens on the 28th March 2018. Then following the guidance received from BBF thereafter, on using BBF published documents such as TR-384, in describing GANA instantiations onto Software Defined Access Network Scenarios, and dropping references to WT-358, which had not been published by BBF as it was meant to provide input to BBF TR-384 and other documents in BBF. Based on the guidance from BBF, the following modifications were performed to create this version: • Changes were made to clause 7.2. to illustrate the integration of GANA with CloudCO architecture based on extracts from BBF TR-384, and clause 7.2.4 was introduced. • Changes were also made to clause 7.4. to further illustrate the integration of GANA with CloudCO architecture, and then moving some aspects of "A GANA Instantiation onto other SDAN Scenarios that were discussed in BBF, but can only be applied if permissible by BBF standards such as TR-384, TR-370" to a newly introduced Annex B. Remarks (NOTEs) were added in Annex B to guide implementers of this ETSI TR 103 473 in ensuring that in implementing GANA instantiation onto the other SDAN scenarios described in Annex B they are aware of the need for compliancy with relevant BBF documents and requirements. • Reference [i.32] to the recently published ETSI GANA Technical Specification (ETSI TS 103 195-2) was updated. • Reference [i.55] to BBF TR-384: Cloud Central Office Reference Architectural Framework, was added. • Reference [i.56] on IEEE paper on "SDN Enablers in the ETSI AFI GANA Reference Model" was added. • Reference [i.57] on an IEEE Article on "Software-Defined Access Networks" was added.

History

Document history		
V1.1.1	November 2018	Publication
V1.1.2	December 2018	Publication