ETSI TR 103 858 V1.1.1 (2026-03)

TECHNICAL REPORT

Core Network and Interoperability Testing (INT); Autonomic/Autonomous IPv6 based 5G Networks: powered by ETSI GANA Multi-Layer Autonomics & Multi-Layer AI-Algorithms and IPv6 Capabilities

Reference
DTR/INT-009001

Keywords
5G, artificial intelligence, autonomic networking, cyber security, enhanced mobile broadband, IPv6, security, self-management

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

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.

Executive Summary

The main target of the present document is to serve as a Framework or Guide for Implementing Autonomic/Autonomous IPv6 based E2E 5G Networks, by leveraging the ETSI GANA Multi-Layer AI/ML and Multi-Layer Autonomic Management and Control Model and IPv6 Capabilities and its Extensions that enable to Build Autonomic Networks. ETSI GANA is an Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services standardized by ETSI in ETSI TS 103 195-2 [i.2]. Through the Framework, software modules (called Autonomic Functions) for enabling automated management, autonomic management (self-management) and self-adaptive control of the network, called GANA Decision-making-Elements (DEs), and their associated Algorithms (including analytics, optimization and AI/ML algorithms), can be innovated and implemented for the network. GANA DEs are meant to drive control-loops within Network Elements/Functions (NEs or NFs) of the 5G network infrastructure and/or drive control-loops at the higher level of abstraction for self-management functionality that is positioned within the outer Management and Control realm of a 5G Network Infrastructure - within a platform called the GANA Knowledge Plane (KP) Platform that uses complex AI algorithms to dynamically and adaptively (re)-configure the network and services using management and control systems such as OSS/BSS, SDN Controllers, Orchestrators, MANO stacks, etc. DE algorithms are not subject to standardization as they provide for the space for innovation and DE and Algorithm supplier differentiations. Examples of Autonomic Functions (i.e. GANA DEs) are: *QoS-management-DE, Security-management-DE, Mobility-management-DE, Fault-management-DE, Resilience & Survivability-DE, Service & Application management-DE, Forwarding-management-DE, Routing-management-DE, Monitoring-management-DE, Generalized Control Plane management-DE*.

The Framework presented in the present document prescribes how to utilize IPv6 Capabilities and emerging IPv6 Extensions in implementing GANA DEs powered Autonomic/Autonomous IPv6 based E2E 5G Network. Innovators obtain guidance on the types of GANA DEs that should be designed to auto-configure and dynamically (autonomically/adaptively) orchestrate and (re)-configure various Managed Entities (MEs), including IPv6 Protocols as MEs of the of 5G Network, as driven by Service or Slice provisioning, or adaptively to meet certain objectives. DEs also provide the means to intelligently adapt the network to various kinds of detected and predicted situations and challenges the autonomic 5G network may experience during its operation.

Introduction

Artificial Intelligence Models (AI Models) are enablers for advanced intelligence in the management and control operations now strongly required for the evolving and future networks such as 5G Networks. AI algorithms bring benefits to diverse aspects in development and deployment of AI exhibiting systems such as Autonomic (Closed-Loop) and Cognitive 5G networks and their associated Autonomic Management and Control systems. European Telecommunications Standards Institute (ETSI) Technical Committee (TC) INT/AFI Working Group (WG) has recently published the de-facto standard on the Generic Autonomic Networking Architecture (GANA) Reference Model - An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services in which AI plays a role in autonomic management and control of networks and services [i.2]. ETSI TS 103 195-2 [i.2] defines an Intelligent Management and Control Functional Block called GANA Knowledge Plane (KP) that is an integral part of Management and Control Systems for the network. GANA KP Platform host complex AI powered network analytics functions that are performed by interworking modules for autonomic (closed-loop) decision-making and execution called GANA Decision-making-Elements (DEs).

The KP DEs run as software in the Knowledge Plane (KP) Platform and drive **self-* operations such as self-adaptation, self-optimization, self-monitoring, self-protection and self-defense** objectives for the network and services by programmatically (re)-configuring Managed Entities (MEs) in the network infrastructure through various means possible. The means to program MEs include NorthBound Interfaces available at the Operations Support Systems (OSS), Service Orchestrator, Domain Orchestrator, Software Defined Networking (SDN) controller, Element Management System/Network Management System (EMS/NMS), Network Functions Virtualisation (NFV) Orchestrator, etc. KP DEs are powered by Artificial Intelligence (AI) algorithms such as Machine Learning (ML), Deep Learning (DL), computational intelligence, etc., such that they execute as AI models or components that embed AI Models [i.2], [i.3], [i.7], [i.6] and [i.11].

ETSI TC INT/ AFI WG has established that E2E Autonomic (Closed-Loop) Service and Security Assurance should be achievable through the Federation of GANA Knowledge Planes (KPs) Platforms that implement components for Autonomic Management and Control (AMC) intelligence for specific network segments and domains. The ETSI GANA Framework enables to define and standardize such a framework. Autonomics by the GANA Knowledge Plane (KP) for a particular network segment/domain is complemented by lower level autonomics introduced in Network Elements/Functions (NEs/NFs) of the particular network segment under the responsibility of the KP, such that the KP policy-controls the lower level autonomics introduced in NEs/NFs. The E2E federation of KPs for the various network segments/domains and their policy-controlling of lower levels autonomics in the NEs/NFs of their respective network segments enable to achieve the complementary multi-layer autonomics. The complementary multi-layer autonomics and the federations of KP Platforms should realize (achieve) Holistic Multi-Domain State Correlation and resources programming by the GANA KPs for the network segments/domains such as the Access, X-Haul (Fronthaul, Midhaul and Backhaul), and Core Networks, etc. While such an E2E Federation of KP Platforms for multiple network segments (as domains) has to be primarily considered within a single network operator administrative domain, the E2E Federation of KPs may be extended to even span multiple network operators' or enterprises' network administrative domains.

ETSI TC INT/AFI WG Specifications such as ETSI TR 103 404 [i.5], ETSI TR 103 495 [i.13], ETSI TR 103 473 [i.4], and ETSI TR 103 747 [i.63] provide the answer to the question of how to implement GANA-defined autonomic manager components (called autonomic functions, i.e. GANA DEs) that implement control-loops in physical Network Elements/Functions (NEs/NFs) and in Virtualised Network Functions (VNFs). This includes answers to how to complement the NE/NF Level autonomic manager components with autonomic manager components defined to operate in the realm outside of NEs/NFs (the realm of management and control systems for particular network architectures), i.e. in the realm called the GANA Knowledge Plane (KP).

ETSI TC INT/AFI WG is also running a Proof-Of-Concept (PoC) Program on **5G Network Slices Creation, Autonomic & Cognitive Management & End-to-End (E2E) Orchestration; with Closed-Loop (Autonomic) Service Assurance of 5G Slices**, as described in clause 10 of the present document.

1 Scope

The present document is a Framework (Guide) to Implementing Autonomic/Autonomous IPv6 based 5G Networks, by leveraging the ETSI GANA Multi-Layer AI / Multi-Layer Autonomic Management and Control Model and IPv6 Capabilities & Extensions that enable to Build Autonomic Networks. The Framework prescribes how to introduce software components called Autonomic Functions (ETSI GANA Decision-making-Elements (DEs)), e.g. Autonomic-QoS-Management-DE, Autonomic-Security-Management-DE, etc. in the 5G Architecture and its associated Management and Control Architecture. The DEs and their associated Algorithms (including analytics, optimization and AI algorithms) are meant to drive control-loops within Network Functions of the 5G network infrastructure and/or drive control-loops at the higher level of abstraction for self-management functionality that is positioned within the outer Management and Control realm of a 5G Network Infrastructure - within a platform called the GANA Knowledge Plane (KP) Platform. The Framework also serves to:

- prescribe how to leverage certain IPv6 Capabilities in enabling Autonomic Functions (called Decision-making-Elements (DEs) in the present document) of the Autonomic 5G network to auto-discover each other, auto-discover various context information, monitoring data, and to exchange DE-to-DE control messages among each other for their collaborative operations in the Self-Driving/Self-Management Operations of the 5G network(s);
- provide Guidance to Innovators of DEs and their associated Autonomics Algorithms, on the types of GANA DEs that should be designed to auto-configure and dynamically (autonomically) orchestrate and (re)-configure various IPv6 Protocols of the of 5G Network as driven by Service or Slice provisioning, or adaptively to meet certain objectives.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[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".

[i.2] 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".

[i.3] White Paper No.1 of the ETSI 5G PoC: "C-SON Evolution for 5G, Hybrid SON Mappings to the ETSI GANA Model, and achieving E2E Autonomic (Closed-Loop) Service Assurance for 5G Network Slices by Cross-Domain Federated GANA Knowledge Planes".

[i.4] ETSI TR 103 473 (V1.1.2): "Evolution of management towards Autonomic Future Internet (AFI); Autonomicity and Self-Management in the Broadband Forum (BBF) Architectures".

[i.5] ETSI TR 103 404: "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] White Paper No.3 of the ETSI 5G PoC: "Programmable Traffic Monitoring Fabrics that enable On-Demand Monitoring and Feeding of Knowledge into the ETSI GANA Knowledge Plane for Autonomic Service Assurance of 5G Network Slices; and Orchestrated Service Monitoring in NFV/Clouds".

[i.7] White Paper No.2 of the ETSI 5G PoC: "ONAP Mappings to the ETSI GANA Model; Using ONAP Components to Implement GANA Knowledge Planes and Advancing ONAP for Implementing ETSI GANA Standard's Requirements; and C-SON - ONAP Architecture".

[i.8] ETSI TS 129 520 (V16.6.0): "5G; 5G System; Network Data Analytics Services; Stage 3 (3GPP TS 29.520 version 16.6.0 Release 16)".

[i.9] ETSI TS 128 533 (V15.0.0): "5G; Management and orchestration; Architecture framework (3GPP TS 28.533 version 15.0.0 Release 15)".

[i.10] NGMN Alliance: "5G End-to-End Architecture Framework v3.0.8".

[i.11] White Paper No.4 of the ETSI 5G PoC: "ETSI GANA as Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI Models for Autonomic Management & Control (AMC) of Networks and Services; and Intent-Based Networking (IBN) via GANA Knowledge Planes (KPs)".

[i.12] ETSI GS AFI 002 (V1.1.1): "Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture (An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management)".

[i.13] ETSI TR 103 495: "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Autonomicity and Self-Management in Wireless Ad-hoc/Mesh Networks: Autonomicity-enabled Ad-hoc and Mesh Network Architectures".

[i.14] Ranganai Chaparadza, Michal Wodczak, Tayeb Ben Meriem, Paolo De Lutiis, Nikolay Tcholtchev, Laurent Ciavaglia: "Standardization of resilience & survivability, and autonomic fault-management, in evolving and future networks: An ongoing initiative recently launched in ETSI", In proceedings of 2013 9th International Conference on the Design of Reliable Communication Networks (DRCN 2013), ISBN 9781479900497, 4-7 March 2013, Budapest, Hungary.

[i.15] IETF RFC 9386: "IPv6 Deployment Status".

[i.16] Reliance Jio: "IPv6-only adoption challenges and standardization requirements", 2020.

[i.17] T-Mobile US: "Going IPv6-only", 2018.

[i.18] Carl A. Sunshine: "Source Routing In Computer Networks", ACM SIGCOMM Computer Communication Review Volume 7, Issue 1, January 1977, pp. 29–33.

[i.19] IETF RFC 8754: "IPv6 Segment Routing Header (SRH)", March 2020.

[i.20] IETF RFC 8986: "Segment Routing over IPv6 (SRv6) Network Programming", February 2021.

[i.21] ETSI GR IPE 001 (V1.1.1) (2021-08): "IPv6 Enhanced Innovation (IPE); Gap Analysis".

[i.22] ETSI TS 123 501 (V16.6.0) (2020-10): "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 16.6.0 Release 16)".

[i.23] IETF RFC 5120: "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", February 2008.

[i.24] IETF RFC 4915: "Multi-Topology (MT) Routing in OSPF", June 2007.

[i.25] IETF draft-ietf-teas-ietf-network-slices: "A Framework for IETF Network Slices", January 2023 (work in progress).

[i.26] IETF RFC 9350: "IGP Flexible Algorithm", February 2023.

[i.27] IETF RFC 9256: "Segment Routing Policy Architecture", July 2022.

[i.28] IETF RFC 5440: "Path Computation Element (PCE) Communication Protocol (PCEP)", March 2009.

[i.29] ETSI White Paper No. 16: "GANA - Generic Autonomic Networking Architecture".

[i.30] IETF RFC 9313: "Pros and Cons of IPv6 Transition Technologies for IPv4-as-a-Service (IPv4aaS)", October 2022.

[i.31] IETF RFC 6146: "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", April 2011.

[i.32] IETF RFC 6147: "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", April 2011.

[i.33] IETF RFC 6877: "464XLAT: Combination of Stateful and Stateless Translation", April 2013.

[i.34] IETF RFC 6333: "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", August 2011.

[i.35] ETSI TS 103 878: "Core Network and Interoperability Testing (INT); Network Interoperability Test Description for IPv6-only services over 5G".

[i.36] ETSI GR IP6 010: "IPv6-based SDN and NFV; Deployment of IPv6-based SDN and NFV".

[i.37] IETF RFC 9341: "Alternate-Marking Method", December 2022.

[i.38] IETF RFC 9342: "Clustered Alternate-Marking Method", December 2022.

[i.39] IETF RFC 6241: "Network Configuration Protocol (NETCONF)", June 2011.

[i.40] IETF RFC 7752: "North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP", March 2016.

[i.41] IETF RFC 8571: "IGP Traffic Engineering Performance Metric Extensions", March 2019.

[i.42] IETF draft-ietf-idr-segment-routing-te-policy: "Advertising Segment Routing Policies in BGP", July 2022 (work in progress).

[i.43] R. Chaparadza, S. Papavassiliou, S. Soulhi and J. Ding: "The Self-Managing Future Internet powered by the current IPv6 and extensions to IPv6 towards "IPv6++" — A viable roadmap Scenario for the Internet Evolution Path", 2010 IEEE™ Globecom Workshops, 2010, pp. 551-556, doi: 10.1109/GLOCOMW.2010.5700381.

[i.44] Chaparadza, R., Petre, R., Prakash, A., Németh, F., Kukliński, S., Starschenko, A. (2011): "IPv6 and Extended IPv6 (IPv6++) Features That Enable Autonomic Network Setup and Operation", In: Szabó, R., Zhu, H., Imre, S., Chaparadza, R. (eds) Access Networks. AccessNets 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 63. Springer, Berlin, Heidelberg.

[i.45] A. Starschenko, N. Tcholtchev, A. Prakash, I. Schieferdecker and R. Chaparadza: "Auto-configuration of OSPFv3 routing in fixed IPv6 networks", 2015 7th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2015, pp. 196-205, doi: 10.1109/ICUMT.2015.7382427.

[i.46] Ranganai Chaparadza, Tayeb Ben Meriem, Benoit Radier, Szymon Szott, Michal Wódczak, Arun Prakash, Jianguo Ding, Said Soulhi, Andrej Mihailovic: "Implementation Guide for the ETSI AFI GANA model: A Standardized Reference Model for Autonomic Networking, Cognitive Networking and Self-Management", 2013 IEEE™ Globecom Workshops (GC Wkshps), 2013, pp. 935-940, doi: 10.1109/GLOCOMW.2013.6825110.

[i.47] N. Tcholtchev, A. Prakash, I. Schieferdecker, R. Chaparadza and R. Petre: "Auto-Collaboration for optimal network resource utilization in fixed IPv6 networks", 2012 IEEE™ Globecom Workshops, 2012, pp. 807-812, doi: 10.1109/GLOCOMW.2012.6477679.

[i.48] Kaldanis, V., Benko, P., Asztalos, D., Simon, C., Chaparadza, R., Katsaros, G. (2011): "Methodology towards Integrating Scenarios and Testbeds for Demonstrating Autonomic/Self-managing Networks and Behaviors Required in Future Networks", In: Szabó, R., Zhu, H., Imre, S., Chaparadza, R. (eds) Access Networks. AccessNets 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 63. Springer, Berlin, Heidelberg.

[i.49] Prakash, A., Starschenko, A., Chaparadza, R. (2011): "Auto-discovery and Auto-configuration of Routers in an Autonomic Network", In: Szabó, R., Zhu, H., Imre, S., Chaparadza, R. (eds) Access Networks. AccessNets 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 63. Springer, Berlin, Heidelberg.

[i.50] Rétvári, G., Németh, F., Chaparadza, R., Szabó, R. (2009): "OSPF for Implementing Self-adaptive Routing in Autonomic Networks: A Case Study", In: Strassner, J.C., Ghamri-Doudane, Y.M. (eds) Modelling Autonomic Communications Environments. MACE 2009. Lecture Notes in Computer Science, vol. 5844. Springer, Berlin, Heidelberg.

[i.51] Zafeiropoulos, A., Liakopoulos, A., Davy, A., Chaparadza, R. (2010): "Monitoring within an Autonomic Network: A GANA Based Network Monitoring Framework", In: Dan, A., Gittler, F., Toumani, F. (eds) Service-Oriented Computing. ICSOC/ServiceWave 2009 Workshops. ServiceWave ICSOC 2009 2009. Lecture Notes in Computer Science, vol. 6275. Springer, Berlin, Heidelberg.

[i.52] Szymon Szott, Janusz Gozdecki, Katarzyna Kosek-Szott, Krzysztof Loziak, Marek Natkaniec, Michal Wagrowski, Ranganai Chaparadza: "Enabling autonomicity in wireless mesh networks with the ETSI AFI GANA reference model", International Journal of Network Management, First published: 01 August 2017.

[i.53] "Evolution of the current IPv6 towards IPv6++ (IPv6 with Autonomic Flavours", In: International Engineering Consortium (IEC) Annual Review of Communications, vol. 60 (December 2008).

[i.54] Georgios Aristomenopoulos, Timotheos Kastrinogiannis, Zhaojun Li & Symeon Papavassiliou: "An Autonomic QoS-centric Architecture for Integrated Heterogeneous Wireless Networks", Mobile Netw Appl 16, 490–504 (2011).

[i.55] G. Aristomenopoulos, T. Kastrinogiannis, Z. Li, M. Wilson, M. González Juan, A. Lozano-López Jose, Y. Li, V. Kaldanis, S. Papavassiliou: "Autonomic mobility and resource management over an integrated wireless environment — A GANA oriented architecture", 2010 IEEE™ Globecom Workshops, Miami, FL, USA, 2010, pp. 545-550, doi: 10.1109/GLOCOMW.2010.5700379.

[i.56] Z. Li: "An autonomic hierarchical mobility management framework for 3GPP heterogeneous networks", 2010 Future Network & Mobile Summit, Florence, Italy, 2010, pp. 1-8.

[i.57] A. Jaron, P. Pangalos, A. Mihailovic, A.H. Aghvami: "Proactive autonomic load uniformisation with mobility management for wireless Internet Protocol (IP) access networks", Source: Volume 1, Issue 4, December 2012, p. 229 - 238: doi: 10.1049/iet-net.2011.0009, Print ISSN 2047-4954, Online ISSN 2047-4962.

[i.58] A. Liakopoulos, A. Zafeiropoulos, C. Marinos, M. Grammatikou, N. Tcholtchev and P. Gouvas: "Applying distributed monitoring techniques in autonomic networks", 2010 IEEE™ Globecom Workshops, Miami, FL, USA, 2010, pp. 498-502, doi: 10.1109/GLOCOMW.2010.5700369.

[i.59] European Commission (EC) funded FP7: "Exposing the Features in IP version Six protocols that can be exploited/extended for the purposes of designing/building Autonomic Networks and Services".

[i.60] IETF draft-chaparadza-6man-igcp-00: "IETF Autonomic Networking Integrated Model and Approach (anima)".

[i.61] IETF draft-chaparadza-6man-igcp-00.txt: "ICMPv6 based Generic Control Protocol (IGCP)".

[i.62] European Commission funded -EFIPSANS-FP7-IP Project: Deliverable-D3.2: "Advanced Network Services in Autonomic IPv6 Networking: Performance Analysis and Evaluation", issued on 31.12.2009 (accessed November 2023).

[i.63] ETSI TR 103 747 (V1.1.1): "Core Network and Interoperability Testing (INT/WG AFI); Federated GANA Knowledge Planes (KPs) for Multi-Domain Autonomic Management & Control (AMC) of Slices in the NGMN® 5G End-to-End Architecture Framework".

[i.64] EANTC: "MPLS SDN Interoperability Test 2023", SRv6 test.

[i.65] ETSI GR IPE 005 (V1.1.1): "IPv6 Enhanced Innovation (IPE); 5G Transport over IPv6 and SRv6".

[i.66] ETSI TR 103 626: "Autonomic network engineering for the self-managing Future Internet (AFI); An Instantiation and Implementation of the Generic Autonomic Network Architecture (GANA) Model onto Heterogeneous Wireless Access Technologies using Cognitive Algorithms".

[i.67] ETSI White Paper No. 35: "IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward", First edition, August 2020.

[i.68] oneM2M TR-436: "Access & Home Network OAM Automation/Intelligence", Issue: 1 Issue Date: February 2021.

[i.69] IETF RFC 8992 (2021): "Autonomic IPv6 Edge Prefix Management in Large-Scale Networks".

[i.70] IETF RFC 8990: "GeneRic Autonomic Signalling Protocol (GRASP)".

[i.71] Recommendation ITU-T Y.3324: "Requirements and architectural framework for autonomic management and control of IMT-2020 networks".

[i.72] IETF RFC 7596: "Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture".

[i.73] IETF RFC 7599: "Mapping of Address and Port using Translation (MAP-T)".

[i.74] IETF RFC 7597: "Mapping of Address and Port with Encapsulation (MAP-E)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
5G SA	5G StandAlone
AcN	Autonomic Network
AFI	Autonomic Future Internet
AFTR	Address Family Transition Router
AGG	AGgregation Gateway
AI	Artificial Intelligence
AMC	Autonomic Management & Control
AMF	Access and Mobility Management Function
AN	Autonomous Network

ANIMA	Autonomic Networking Integrated Model and Approach
API	Application Programming Interfaces
APN	Application - aware Networking
APN6	Application - aware IPv6 Networking
AS	Autonomous System
ASN	Autonomous System Number
ATS	Abstract Test Suite
BBF	BroadBand Forum
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BGP-LS	Border Gateway Protocol Link-State
CAPEX	CAPital EXpenditure
CLAT	Client-side NAT
CLI	Command Line Interface
CPE	Customer Premises Equipment
CSG1	Communication Systems Group
C-SON	Centralized Self Organizing Network
DC	Data Centre
DE	Decision making Element
DL	DownLink
DNS	Domain Name System
DS-lite	Dual Stack lite
D-SON	Distributed - Self Organizing Network
E2E	End-to-End
EC	European Community
ECMP	Equal-Cost Multi-Path
EMS	Element Management System
EPC	Evolved Packet Core
FBB	Fixed BroaBand
FlexE	Flexible Ethernet
FP7	Seventh Framework Programme
FW	FireWall
GANA	Generic Autonomic Network Architecture
GRASP	GeneRic Autonomic Signalling Protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technology
IFIT	In-situ Flow Information Telemetry
IGCP	ICMPv6 based Generic Control Protocol
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IoT	Internet of Thing
IP	Internet Protocol
IPE	IPv6 Enhanced innovation
IS-IS	Intermediate System-to-Intermediate System
ISP	Internet Service Provider
KP	Knowledge Plane
KP DE	Knowledge Plane Decision-making Element
KPI	Key Performance Indicator
MANO	Management and Orchestration
MAP-E	Mapping of Address and Port with Encapsulation
MAPE-K	Monitor-Analyse-Plan-Execute over a shared Knowledge
MAP-T	Mapping of Address and Port using Translation
MBB	Mobile BoradBand
MBTS	Model-Based Translation Service
MDAS	Management Data Analytics Service
ME	Managed Entity
MEC	Mobile Edge Computing
ML	Machine Learning
mMTC	massive Machine Type Communications
MPLS	MultiProtocol Label Switching

NAT	Network Address Translation
NB	NorthBound
NE	Network Element
NF	Network Function
NFV	Network Function Virtualisation
NGMN	Next Generation Mobile Networks
NSSF	Network Slice Selection Function
NWDAF	NetWork Data Analytics Function
NWDAS	NetWork Data Analytic Service
OAM	Operations Administration and Maintenance
ODA	Open Digital Architecture
ONIX	Overlay Network for Information eXchange
OPEX	OPerating EXpenses
O-RAN	Open RAN
OSe	Operating System embedded
OSPF	Open Shortest Path First
OSS	Operations Support Systems
PE	Provider Edge
PLAT	Provider-side NAT
PoC	Proof of Concept
Pre-AGG	Pre-Aggregation Gateway
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RAN	Radio Access Network
RIC	RAN Intelligent Controllers
RR	Route Reflectors
SBA	Service Based Architecture
SDN	Software Defined Networks
SDO	Standards Development Organizations
SDWAN	Software-Defined Wide Area Network
SEG	Secure Gateway
SID	Segment Identifier
SLA	Service Level Agreement
SMF	Session Management Function
SNMP	Simple Network Management Protocol
SON	Self Organizing Networks
SPAN	Switched Port Analyser
SPF	Shortest Path First
SR-BE	Segment Routing Best Effort
SRH	Segment Routing Header
SR-PCE	Segment Routing - Path Computation Engine
SR-TE	Segment Routing - Traffic Engineering
TAP	Test Access Points
TE	Traffic Engineering
TLV	Type-Length-Value
TWAMP	Two-Way Active Measurement Protocol
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra Reliable and Low Latency Communications
VNF	Virtual Network Function
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
WG	Working Group
YANG	Yet Another Next Generation

4 Principles for Autonomic Networking and Autonomic Management & Control (AMC), and Enablers

This clause refers to clause 4 of ETSI TR 103 747 [i.63].

The Generic Autonomic Networking Architecture (GANA) Reference Model serves as a standardized architectural framework for autonomic networking, cognitive networking, and self-management of networks and services. It defines a hierarchy of Functional Blocks (FBs) that implements a control-loop as the core driver of the self-management, their reference points, and messaging protocols, supporting both micro-level (within network elements) and macro-level (network-wide) autonomic control loops.

Central to GANA is the Knowledge Plane (KP), which orchestrates intelligent management and control through key components such as network-level Decision-making Elements (DEs), the ONIX overlay for distributed information exchange, and the Model-Based Translation Service (MBTS) for protocol-agnostic communication between DEs and network elements. GANA's hybrid approach allows implementers flexibility in deploying autonomic logic either centrally (macro-autonomics) or in a distributed manner (micro-autonomics), and is compatible with hybrid Self-Organizing Networks (SON) models.

GANA DEs are organized hierarchically to enable scalable and coordinated autonomic management. Higher-level DEs, often situated within the Knowledge Plane (KP), exercise supervisory control over lower-level DEs and Managed Entities (MEs) by implementing intent-driven, closed control loops.

Specifically, a higher-level DE analyses aggregated network-wide data and determines the appropriate intent or configurations. It then communicates directives, intent/policies, or configuration parameters to subordinate DEs, which are instantiated within specific network elements or functions. These lower-level DEs, in turn, execute fast, localized control loops—directly managing the behavior and state of their respective MEs based on the guidance received from the higher-level DE.

This hierarchical control structure ensures that overarching network objectives are maintained, while allowing for rapid, context-aware adjustments at the local level. The approach enables seamless coordination between macro-level (network-wide) and micro-level (element-specific) autonomics, promoting both global optimization and local agility in network management.

GANA facilitates integration with diverse management and control systems as depicted in Figure 1 with NorthBound (NB) Application Programming Interfaces (API) (e.g. SDN controllers, OSS/BSS, NFV MANO), leveraging standardized APIs to enable end-to-end orchestration and analytics. GANA also addresses the coordination and collaboration among autonomic functions, the handling of intent-based networking, and the design principles necessary for the stability and synchronization of control loops, positioning itself as a holistic and unifying framework for autonomic management and control.

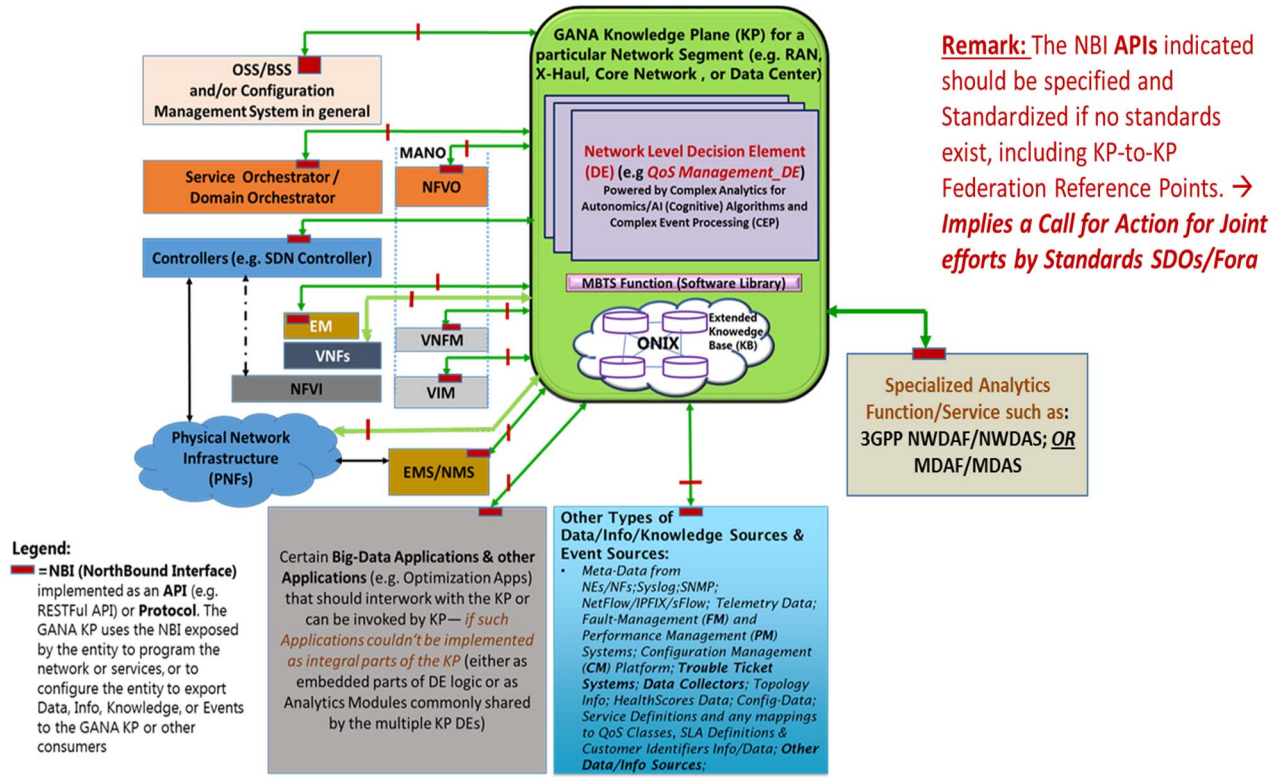


Figure 1: GANA Knowledge Plane (KP) interfaces with multiple management and control systems, as well as integrates with various event, data, and knowledge sources, thereby enabling selective and dynamic network programmability

5 Use Cases for AI/ML and Autonomics in E2E IPv6 based 5G Networks in general; and Mappings to GANA DEs that help implement particular Use Case

5.1 Autonomic Management and Control (AMC) of Network Slices

ETSI TR 103 747 [i.63] and clause 6.6 of the present document discuss Autonomic Orchestration and Service and Security Assurance of E2E 5G Network Slices. Autonomic orchestration and use of SRv6 can be performed by a GANA Knowledge Plane (KP) for the Transport Network to dynamically create transport network slices based on SRv6 and perform service and security assurance of the transport network slices. Clause 6.6 also provides insights on autonomics with use of SRv6.

5.2 Auto-Discovery and Auto-Configuration (Self-Configuration) Use Case

This is an Autonomics Use Case by which GANA NODE_LEVEL_AC_DE provides logic, algorithms to ensure plug and play mechanisms of GANA Node. Provide auto discovery mechanisms and auto configuration mechanisms. The NODE_LEVEL_AC_DE may self-adapt the GANA Node according to GANA Profile derived from the KP's Network Level_AC_DE and orchestrate the different DEs within the GANA Node and in collaboration with other DEs outside the GANA node. The Use Case also includes the aspect by which GANA NETWORK_LEVEL_AC_DE provides logic, algorithm(s) to ensure plug and play mechanisms of GANA Network. Provide auto discovery, bootstrapping mechanisms and auto configuration mechanisms. The NETWORK_LEVEL_AC_DE may self-adapt the GANA Network according to GANA profile defined by an administrator domain and orchestrate the different DEs within the GANA network and in collaboration with other administrative domains.

NOTE 1: ETSI TS 103 195-2 [i.2] provides more details of these two DEs, guidance on how to design their associated Control-Loops, and how they complement and interwork with other when both are implemented for the targeted network architecture and its associated management and control architecture.

NOTE 2: There already exists in literature some research and implementation and validation work published on such autonomics use case, some of which are based on the GANA framework and IPv6. For example, readers may find work in [i.44], [i.49], [i.45], [i.48], [i.49], [i.1] and [i.62] very useful in this regard.

5.3 Autonomic Mobility Management and Control Use Case

This is an Autonomics Use Case by which GANA FUNC_LEVEL_MOM_DE provides logic, algorithm(s) to manage mobility related MEs hosted by NE, for example, MEs that help drive handover or handoff of devices/nodes between different networks and technologies and also ensure service continuity of applications flows. The Use Case also includes the aspect by which the GANA NET_LEVEL_MOM_DE provides logic and algorithms to ensure handover between access networks, network element with service continuity.

NOTE 1: ETSI TS 103 195-2 [i.2] provides more details of these two DEs, guidance on how to design their associated Control-Loops, and how they complement and interwork with other when both are implemented for the targeted network architecture and its associated management and control architecture.

NOTE 2: There already exists in literature some research and implementation and validation work published on such autonomics use case, some of which are based on the GANA framework and IPv6 (e.g. IP Level Mobility Management with PMIPv6, etc.). For example, readers may find work in [i.48], [i.52], [i.55], [i.56], [i.57], [i.1] and [i.62] very useful in this regard.

5.4 Autonomic Routing Management and Control Use Case

This is an Autonomics Use Case by which the GANA FUNC_LEVEL_RM_DE provides logic, algorithms to ensure the optimal and resilient routing of packets in the network in order to optimize the network utilization. The Use Case also includes the aspect by which the GANA NET_LEVEL_RM_DE provides logic, algorithms to ensure optimized routing of packets and flows in the network and in respect of network operator policies and in order to optimize the network's traffic routing objectives and behaviours.

NOTE 1: ETSI TS 103 195-2 [i.2] provides more details of these two DEs, guidance on how to design their associated Control-Loops, and how they complement and interwork with other when both are implemented for the targeted network architecture and its associated management and control architecture.

NOTE 2: Figure A.3 presents an illustration of the interworking and complementarity between the two DEs (more details on this are described in ETSI White Paper No.16 [i.1]).

NOTE 3: There already exists in literature some research and implementation and validation work published on such autonomics use case, some of which are based on the GANA framework and IPv6. For example, readers may find work in [i.1], [i.50], [i.48] and [i.62] very useful in this regard.

5.5 Autonomic Forwarding Management Use Case

This is an Autonomics Use Case by which GANA FUNC_LEVEL_FWD_DE provides logic, algorithm that autonomically manages the forwarding protocols and mechanisms of the node in order to optimize the forwarding behaviour of the node so as to meet certain objectives. The Use Case also includes the aspect by which GANA NET_LEVEL_FWD_DE provides logic, algorithms to ensure optimized forwarding of traffic flows in the network and in respect of network operator policies and in order to optimize the network's traffic engineering and forwarding objectives and behaviours.

NOTE 1: ETSI TS 103 195-2 [i.2] provides more details of these two DEs, guidance on how to design their associated Control-Loops, and how they complement and interwork with other when both are implemented for the targeted network architecture and its associated management and control architecture.

NOTE 2: There already exists in literature some research and implementation and validation work published on such autonomics use case, some of which are based on the GANA framework and IPv6. For example, readers may find work in [i.1], [i.46], [i.45], [i.48] and [i.62] very useful in this regard.

5.6 Autonomic QoS and QoE Management and Control Use Case

This is an Autonomics Use Case by which GANA FUNC_LEVEL_QoS_M_DE provides logic, algorithms to ensure QoS for services and improve QoE of services within the GANA node and other nodes through the collaboration of their FUNC_LEVEL_QoS_M_DEs. The Use Case also includes the aspect by which GANA NET_LEVEL_QoS_M_DE provides logic and algorithms to ensure QoS of services and also improve Quality of Experience (QoE) for services.

NOTE 1: ETSI TS 103 195-2 [i.2] provides more details of these two DEs, guidance on how to design their associated Control-Loops, and how they complement and interwork with other when both are implemented for the targeted network architecture and its associated management and control architecture.

In elaboration of the GANA autonomics by the GANA NET_LEVEL_QoS_M_DE, Autonomic Management Software **(**the GANA Quality of Service (QoS)-Management DE or a Combined Quality of Service (QoS)-and-Quality of Experience (QoE) Management DE) autonomatically configures resources associated with specific connectivity paths or Network Slices within the network segment the GANA KP is responsible for, such that Traffic Flows (e.g. IP Flows) carried over the paths experience KPIs (e.g. delay, throughput, bandwidth, etc.) that fulfil Service Level Agreements (SLAs) for those flows. The Autonomic Management Software (GANA KP Autonomic Performance-Management DE) also computes various paths within the network segment that should fulfil certain SLAs and is able to adaptively switch traffic flows onto another working path(s) in the event of detected or predicted failures/errors/faults on the primary path(s). Autonomic Management Software (GANA KP Autonomic Performance-Management DE) also continuously monitors and measures network and service performance Key Performance Indicators (KPIs), i.e. any performance degradations, and dynamically allocate resources in its network segment that help to achieve certain KPI targets for traffic flows in particular.

NOTE 2: There already exists in literature some research and implementation and validation work published on such autonomics use case, some of which are based on the GANA framework and IPv6. For example, readers may find work in [i.1], [i.54], [i.47], [i.46], [i.48], [i.52] and [i.62] very useful in this regard.

5.7 Autonomic Monitoring Management and Control Use Case

This is an Autonomics Use Case by which GANA 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. The FUNC_LEVEL_MON_DE's logic should include an algorithm to retrieve information (subscribe for information) and process the information indicative about the operations of the GANA node in order to infer and adaptively enforce the monitoring behaviour and monitoring-data flow of the GANA node that is needed by DEs within the node. The Use Case also includes the aspect by which GANA 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. The NET_LEVEL_MON_DE's logic should include an algorithm to retrieve information (subscribe for information) and process the information indicative about the operations of the Knowledge Plane DEs in order to infer and adaptively enforce the monitoring behaviour and monitoring-data flow (or knowledge flow) from NEs, Data Collectors and Probes as may be needed by Knowledge Plane DEs during their operations.

NOTE 1: ETSI TS 103 195-2 [i.2] provides more details of these two DEs, guidance on how to design their associated Control-Loops, and how they complement and interwork with other when both are implemented for the targeted network architecture and its associated management and control architecture.

NOTE 2: There already exists in literature some research and implementation and validation work published on such autonomics use case, some of which are based on the GANA framework and IPv6. For example, readers may find work in [i.1], [i.51], [i.58], [i.46], [i.48] and [i.62] very useful in this regard.

5.8 Autonomic Security Management and Control Use Case

This is an Autonomics Use Case by which GANA NODE_LEVEL_SEC_M_DE is used to manage any security issues in the Node. NODE_LEVEL_SEC_M_DE may also be used to secure and authenticate interactions between DEs and MEs within the same domain or to secure interaction with other MEs and DEs within different domain. The Use Case also includes the aspect by which GANA NET_LEVEL_SEC_M_DE is used to manage any security issues in the network. NET_LEVEL_SEC_M_DE may also be used to secure interactions between DEs and MEs within the same domain or to secure interaction with other MEs and DEs within different domain.

5.9 Autonomic Fault Management Use Case

This is an Autonomics Use Case by which GANA NODE_LEVEL_FM_DE is for autonomic fault management within the GANA Node by employing appropriate Fault Detection Mechanisms, Fault Isolation/Localization/Diagnosis Mechanisms, and Fault Removal Mechanisms that enable to repair the node's components and the node as a whole. NODE_LEVEL_FM_DEs of various GANA nodes may collaborate in achieving distributed autonomic fault-management that requires the collaboration of various nodes. The Node-Level-Fault Management-DE (NODE_LEVEL_FM_DE) interworks with the Node-Level-Resilience & Survivability-DE (NODE_LEVEL_R&S_DE) as described in [i.14] and in ETSI GS AFI 002 [i.12]. The Use Case also includes the aspect by which GANA NET_LEVEL_FM_DE is for autonomic fault management that require to be orchestrated at the network level by logically centralized algorithms of the NET_LEVEL_FM_DE-by employing appropriate Fault Detection Mechanisms, Fault Isolation/Localization/Diagnosis Mechanisms, and Fault Removal Mechanisms that enable to repair network services and/or functionality of a network node. The Network-Level-Fault Management-DE (NODE_LEVEL_FM_DE) interworks with the Network-Level-Resilience_&_Survivability-DE (NODE_LEVEL_R&S_DE) as described in [i.14] and in ETSI GS AFI 002 [i.12].

This is an Autonomics Use Case by which Autonomic Management Software (GANA Autonomic Fault-Management DE) automatically detect faults/errors/failures and perform fault-diagnosis and self-repair to sustain a high degree of availability, reliability and acceptable service delivery to end-users.

5.10 Autonomic Resilience & Survivability Management Use Case

This is an Autonomics Use Case by which GANA NODE_LEVEL_RS_DE provides logic, algorithms to ensure the resilience and survivability of the node(system) and the network (of some scope) in collaboration with other peer NODE_LEVEL_RS_DEs in other GANA nodes. The Node-Level-Resilience &Survivability-DE (NODE_LEVEL_R&S_DE) interworks with the Node-Level-Fault Management-DE (NODE_LEVEL_FM_DE) as described in [i.14] and in ETSI GS AFI 002 [i.12]. The Use Case also includes the aspect by which GANA NET_LEVEL_R&S_DE provides logic and algorithms to ensure the resilience and survivability of the network systems (network nodes/functions) as described in [i.14] and in ETSI GS AFI 002 [i.12].

5.11 Autonomic Performance Management Use Case

This is an Autonomics Use Case by which Autonomic Management Software **(**GANA Autonomic Performance-Management DE) monitors and measures network and service performance Key Performance Indicators (KPIs), i.e. any performance degradations, and dynamically allocate resources in the network that help to achieve certain KPI targets.

NOTE: There already exists in literature some research and implementation and validation work published on such autonomics use case, some of which are based on the GANA framework and IPv6. For example, readers may find work in [i.48] and [i.1] very useful in this regard.

6 IPv6-Only based E2E 5G Networks: E2E Aspects of IPv6 in 5G and Reference Architecture Scenarios for Consideration; Implications on GANA Autonomics

6.1 Background of SRv6 technology and the motivation in the context of Network Automation

This clause aims at showing how to utilize IPv6 capabilities and emerging IPv6 Extensions (e.g. Segment Routing version 6 "SRv6") in the big picture of an "Autonomic-based AI and Programmable 5G Network". Hence, the way it transforms the current complex "5G IP Bearer Network" into a simplified "E2E Programmable Bearer Network" under the paradigm of "Network as a Computer". This clause highlights the Business and Technical benefits SRv6 technology brings in this space. Then, it succinctly presents the SRv6 fundamentals along with the standardization journey and readiness/maturity level and its adoption by Services Providers, Public Sector as well as Products & Solutions Suppliers.

Segment Routing version 6 (SRv6) is a protocol defined by the Internet Engineering Task Force (IETF) that aims at simplifying the operations in a packet network. It is a key enabler of next-generation packet networks to effectively support advanced transport services as demanded by 5G, IoT, and Cloud applications.

SRv6 is based on two foundational technologies:

1) the Internet Protocol version 6 (IPv6); and

2) the Source Routing paradigm.

IPv6 received renewed interest in the past few years [i.15]. National Authorities and Regulators have issued policies to further incentivize the use of IPv6 and prepare the stage for IPv4 sunsetting. Some Service Providers have even moved to IPv6-only networks [i.16], [i.17].

Source Routing is an internet routing technique, originally proposed by Carl A. Sunshine [i.18], in which the packet source, typically the network ingress router, specifies the complete path the packet takes across the network. In doing that, no routing decision (states) needs to be taken at the intermediate nodes, thus simplifying the overall packet processing.

SRv6 leverages on two key technical capabilities to provide business benefits:

1) Simplification of Network Management and reduction of OPEX. SRv6 operations require a reduced protocol stack if compared to current IP/MPLS networks. As a result, simplified network operations are achieved, bringing to lower Operational Expenditure (OPEX) for Service Providers.

2) Increase of Quality of Experience (QoE). SRv6 enables both network programmability and network slicing, increasing QoE and allowing resource-based traffic steering. Such a capability fulfils the 5G and Cloud requirements for better control and usage over the Transport Network resources, indispensable for advanced applications as in the case of massive Machine Type Communications (mMTC), Ultra-Reliable Low-Latency Communications (URLLC) and Edge Cloud services.

From ETSI side [i.21], SRv6 is characterized by the following 5 key Technical Benefits: simplified network protocols, cloud-network convergence, compatibility with existing networks, enhanced inter-AS connectivity, and agile service provisioning.

6.2 Value of IPv6 in 5G network, and consideration of GANA Multi-Layer Autonomics in the picture

In this clause a set of selected architectural scenarios on IPv6 in 5G Networks are presented, and then insights on the impact of introducing GANA Autonomics into the Architectures and the interplay of some key aspects in the architectures with GANA autonomics are provided.

NOTE 1: Insights on how the GANA Knowledge Plane (KP) Platform integrates with other management and control systems (such as SDN controllers and NFV MANO, OSS/BSS and Service Orchestrators, etc.) and the network are provided in clause 4.

5G SA Core architecture enables to select for each 5G connection the application located in the best datacentre type (edge, regional, core) and the best path to deliver appropriate QoE for each Service. At the same time, it wants to have the lower impact possible in resource utilization and related power consumption to fulfil the service need, avoiding network over-dimensioning and relative costs.

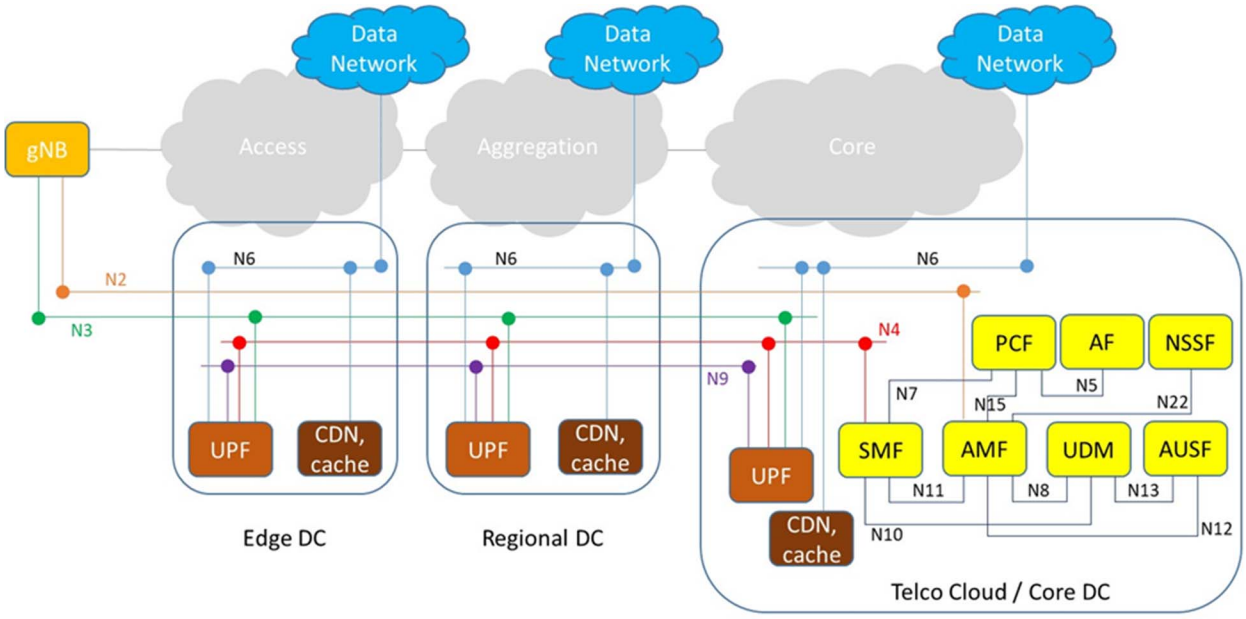


Figure 1a: 5G core reference architecture (ETSI TS 123 501 [i.22]) with functional distribution in a 3-levels DCs structure (Courtesy of ETSI GR IPE 005 [i.65])

In this scenario, the transport network plays a relevant role. IPv6 and SRv6, together with multiple other state of the art technologies, enable to fulfil those functionalities at best. Old technologies like IPv4, present a specific limitation that does not allow to exploit 5G SA core functionalities. Private IPv4 has to be reused multiple times within the operator network, and vertical access islands need to be created in order to avoid address overlap. This limits the possibility of freely using any UPF within the network. The location of the application is not freely selectable.

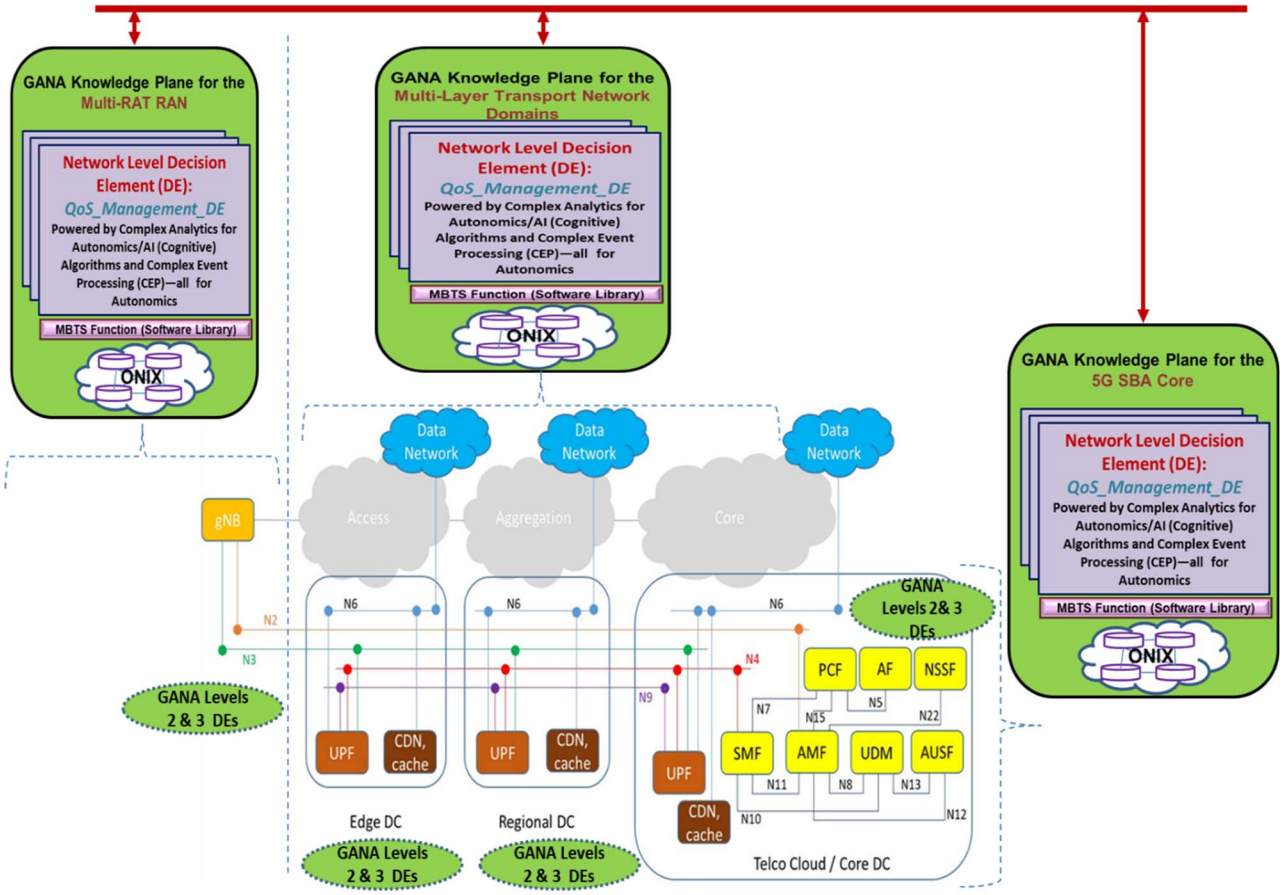


Figure 2: GANA instantiation onto specific network segments, including GANA instantiation onto the 5G core reference architecture (ETSI TS 123 501 [i.22]) with functional distribution in a 3-levels DCs structure

NOTE 2: Considerations for NWDAF/MDAF (NWDAS/MDAS) should be taken into consideration regarding the integration of these functions/services with the GANA KP Platform as described earlier in clause 4.3 of the present document (particularly in Figure 1 on "integration of the GANA Knowledge Plane (KP) with various management and control systems through which the Knowledge Plane can selectively program the network; and KP integration with Event Sources, Data Sources and Info/Knowledge Sources").

6.3 Slicing in packet networks

6.3.1 Network Slicing high level architecture

Network slicing is one of the biggest differentiators of 5G compared to previous generations of mobile services. Network slicing brings increased network resource utilization efficiency and deployment flexibility. It also provides a higher quality of experience in servicing the differentiated requirements of customers and applications.

From the network's perspective, the concept of slicing is discussed in [i.25]. There, "network slicing" is analysed within the context of IETF. [i.25] introduces the term "IETF Network Slice", which specifies a slice is implemented over the technologies identified by the IETF (e.g. MPLS, SR, SRv6, etc.), its characteristics and system components.

3GPP defined network slicing as a critical 5G Core (5GC) feature in [i.22]. A network slice is viewed as a logical end-to-end network that can be dynamically created, modified or deleted. A User Equipment (UE) may access to multiple slices over the same Access Network (AN). This latter is typically the 3GPP Radio Access Network (RAN), but it can also be a non-3GPP Access Network where the terminal may use any non-3GPP access to reach the 5GC, for example, via a secured IPSec/Internet Key Exchange (IKE) tunnel over a Wi-Fi® network.

E2E slice spanning various network segments (e.g. Access, Transport, Core) leverage on the above definitions from IETF and 3GPP. Each slice may serve a particular service type, set of applications or group of customers, each with an agreed upon Service Level Agreement (SLA).

The Access and Mobility Management Function (AMF) instance serving the UE is common (or logically belongs) to all the Network Slice instances that are serving the UE. Other network functions, such as the Session Management Function (SMF) or the User Plan Function (UPF), may be specific to each Network Slice. This is represented in Figure 3, which shows two different slices (both Red and Green).

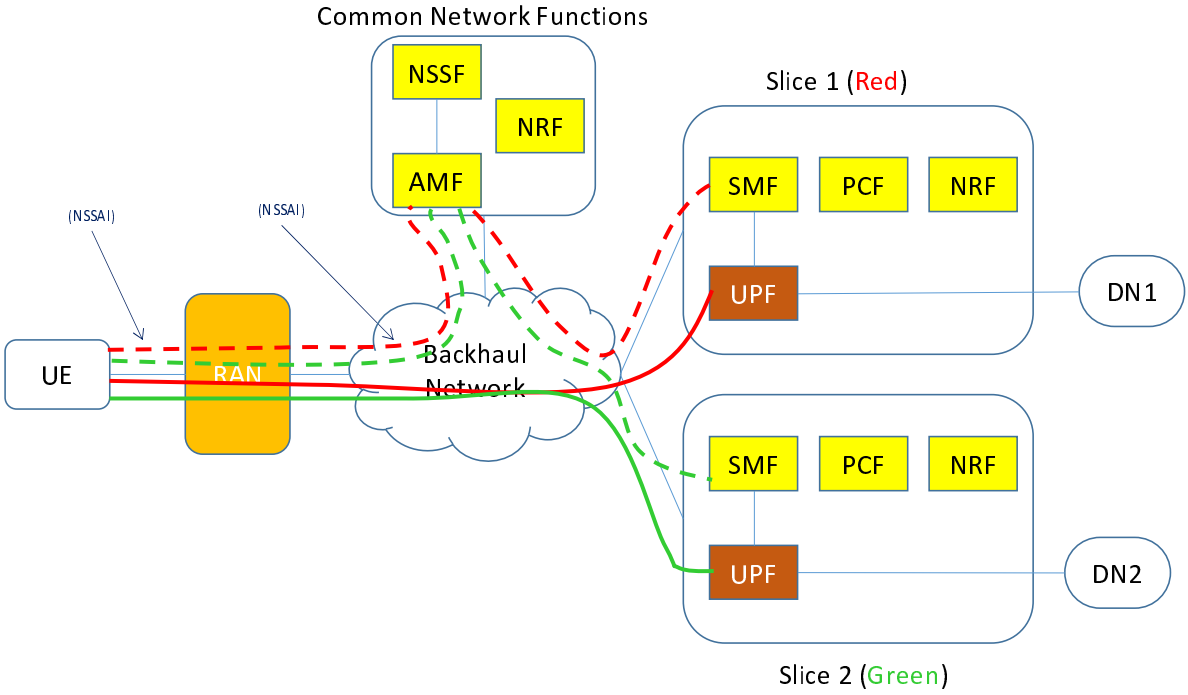


Figure 3: Network slicing high-level architecture (SRv6 in the backhaul network) (Courtesy of ETSI GR IPE 005 [i.65])

The network slice instance selection is triggered as part of the registration procedure by the first AMF that receives the registration request from the UE. The AMF retrieves the slices allowed by the user subscription and interacts with the Network Slice Selection Function (NSSF) to select the appropriate Network Slice instance.

In the IPv6-based 5G transport network, SRv6 programmability is essential to support 5G network slicing. The IPv6 data plane still uses both IGP (Interior Gateway Protocol) and BGP (Border Gateway Protocol) protocols to carry the routing and reachability information of the network nodes. The only extension requested is the support of multi-topology in [i.23] and [i.24]. In addition, SRv6 network programming [i.19] enables network slicing support through fine-grained packet handling and steering.

6.3.2 SRv6 based network slicing

SRv6 is the more suitable protocol to underpin Network Slicing in 5G network. Possibility to define connection flow spanning the whole network provide benefits in service creation and monitoring. Traffic Engineering policies can be prescribed to network slice instances and implemented in different sections of the network. SRv6, spanning the whole network, simplify the network in term of number of protocols used and interworking functions, as well as straight-forwarding the service lifecycle. It enables easy creation, modification and monitoring of each connection flow. It underpins properly the management system automation of the whole service lifecycle.

Different SRv6 SIDs are allocated per node, each associated with a slice. Every Segment Identifier (SID) is also related to specific network resources. This way, a node receives as many SIDs as the slices it is part of.

The physical network is decomposed in a virtual link with specific QoS. Each of those virtual links can be assigned to one or multiple slices. Flexible Ethernet (Flex-E) protocol could be used for this scope, to dedicate proper bandwidth and priority to each slide according to the needed SLA of the associated 5G Slice.

For each of those Flex-E links, a specific SID is associated, with the possibility for routing protocol to select the proper Flex-E link according to the needed QoS.

Each SID has a locator dedicated to a specific slice, as shown in Figure 4.

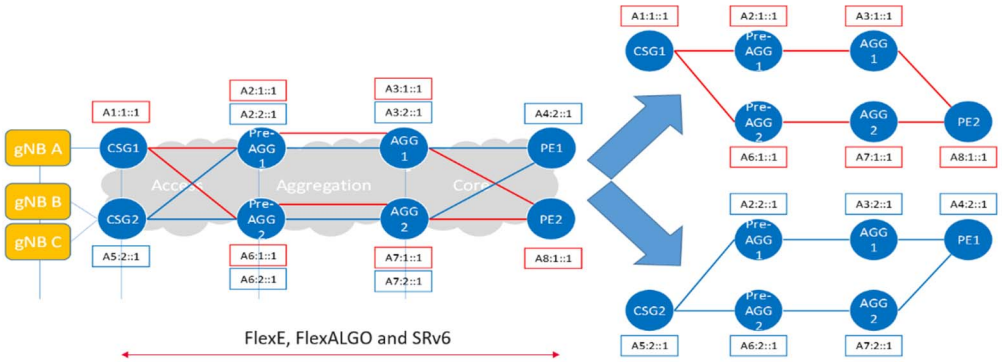


Figure 4: Network slicing based on FlexE, FlexALGO and SRv6 locators

The identification of a network slice is guaranteed by a specific locator assigned to a node. The example above shows that Communication Systems Group (CSG)-1 belongs to the "Red" slice. A loopback address in the form of A1:1::1 is then associated with CSG1. A1:1 is the locator of the node (the first part, A1), while the slice is identified by the following 1 (the third and fourth bytes of the address in the example). The transport network will result to be composed of several Flex-E links with different QoS.

The node **pre-Aggregation** Gateway(Pre-AGG)-1 support forwarding for two slices. This way is associated with two loopback addresses: a first one A2:1::1 is for the "Red" slice and a second one A2:2::1 for the "Blue" slice. Once again, A2 is the locator of Pre-AGG-1, while the following number is the slice identifier.

SR paths are normally configured based on the metrics provided by IGP protocols. In such a case, SR Best Effort (SR-BE) is considered, as paths are built upon the Shortest Path First (SPF) mechanisms. The path to a destination is thus calculated by minimizing the topological cost, normally associated with the link cost.

To address the lack of flexibility imposed by SPF, Flexible Algorithm (Flex-Algo) technology is introduced. A Flex-Algo allows an IGP to calculate constraint-based network paths, implementing Traffic Engineering (TE) capabilities in an easier and more flexible manner.

Flex-Algo technology IETF RFC 9350 [i.26] provides some technical advantages, such as:

- NEs involved in the same Flex-Algo natively form an independent logical topology. Also, constraints of the IGP path algorithm can be defined to further exclude some links in the logical topology.
- The types of metrics used in the IGP path algorithm can be defined. In addition to the link cost value, SPF algorithm can calculate the shortest path to the destination based on the link delay and TE metric values.

This way Flex-Algo can meet the requirements of different services, including high-bandwidth and low-delay services. Flex-Algo can be natively used on SR networks and is compatible with "Equal-Cost Multi-Path" (ECMP) load balancing and Topology Independent-Loop Free Alternate" backup paths in these networks.

[i.26] specifies a set of extensions to Intermediate System-to-Intermediate System (IS-IS), "Open Shortest Path First" version 2 OSPFv2, and OSPF version3 that enable a router to advertise through Type-Length-Values TLVs the key characteristics of a Flex-Algo.

Often, flexible algorithms are seen as the enabler of advanced applications, such as network slicing, in carrier's networks. While this is generally true, flexible algorithms may find utilization also in enterprises and utilities. The differentiated handling of applications, based on their diversified SLAs, may require having multiple logical topologies also in the context of a factory, campus or purpose-built network. Grid networks, as an example, may take benefit of diversified topologies each carrying an application which is characterized by low latency or strict availability.

SRv6 SIDs inherit the slice identification from Locator. The resulting virtual topology is shown on the right. The two slices have dedicated topology and associated behaviour as represented in Figure 4. One of the slices may be tuned for policies that enable low-latency transport or higher capacity or other metrics/parameters for an optimized transport that best serves a service's requirements.

To achieve this step, the control plane or the network controller (or a combination of the two) has to distribute the information about the network resources associated with a slice. This information distribution is based on the multi-topology concept, already supported by the IGP protocols. This is capable of propagating routing information associated to multiple virtual topologies enabled over the same physical network [i.23] and [i.24].

In order for SRv6-TE to take into consideration link characteristics such as latency and other TE constraints, a flexible routing algorithm (or flex-algo) has to be enabled on the control plane. Flex-Algo (0) to Flex-Algo (127) are reserved by the Internet Assigned Numbers Authority (IANA) as standard algorithms. Flex-Algos from 128 onwards are instead used for customizable path computation (e.g. with the lowest latency).

The specific computation may be propagated through either IGP control protocols or policies issued by an SDN controller. This latter may represent a better option as it has a centralized knowledge of the whole network. Assuming an SDN controller is employed, this will build a TE database of the network and, based on the service requirements, assign SIDs, in the form of locator:function, to all the nodes involved.

The structuring of a SID into the locator:function form is the second, indispensable pre-requirement to enable network programming and support TE mechanisms. The SRv6 SID function is the identifier of a "behaviour" defined locally to the locator (node). More formally, it takes the name of SRv6 Endpoint behaviour.

6.3.3 SR-based network programming

Network programming combines Segment Routing functions, both topological and service, to achieve a networking objective that goes beyond mere packet routing. The concept of network programming comes from computer programming. In computer programming, human beings can translate their intentions into a series of instructions that computers can understand, computers execute the instructions to realize the human intent. Correspondingly, network programming translates intent into a series of forwarding instructions that network devices can understand, the network executes the instructions to realize the intent.

SRv6 network programming [i.20] defines a base set of SRv6 endpoint behaviours. A network program is built from Segment IDs (SIDs), that are 128 bit opaque identifiers for a local endpoint behaviour. In other words, a SID represents a local action or policy at a node, such as forwarding a packet via an adjacency, or decapsulating and forwarding an inner packet via a Virtual Routing and Forwarding (VRF) table toward its destination. SRv6 SIDs are treated as IPv6 addresses by the network when they are in the IPv6 header destination address field. The network simply forwards packets destined to SIDs toward the node implementing the SID.

The 128bit SRv6 SID consists of three parts:

3) Locator, encoded in the most significant bits of the SID:

    a) The uppermost bits of a locator is called the Block, this is the block of the IPv6 address space SIDs are assigned from.

    b) The remaining bits of the locator identify the Node the SID is located on.

4) Function, encoded in the next most significant bits of the SID, identifies the local behaviour, and any local semantics for that behaviour, to be executed at the node.

5) Optional arguments, encoded in the next most significant bits of the SID, identify arguments to the function. The semantics and format of argument bits are defined by the endpoint behaviour specification.

SR policies [i.27] define an instantiated network program as a segment list. SR policies contain multiple candidate paths between an SR source and endpoint. Traffic is steered into an SR policy to apply a network program to it, such as traffic engineering i.e. to forward traffic via a low latency path, a disjoint path, a service function chain, or any network program represented as a list of SIDs.

Through policies it is possible to define differentiated handling for traffic flows, i.e. Traffic Engineering (TE). As an example, one policy between two endpoints may specify a low-latency path (e.g. to serve a time-bound mission critical application), another policy between the same two endpoints may specify a high-capacity path (e.g. to carry best-effort traffic).

SR Traffic Engineering (SR-TE) applies to both carrier and enterprise networks. The enablement of SR-TE in the backbones provide a sort of unification of the protocols used. SR-TE based on IPv6 may become the common underlay to enable multi-domain connectivity to transport all services, no matter whether they are legacy or new innovative applications.

SR-TE can be combined with SDN, for example, through SR Path Computation Engine (SR-PCE) [i.28]. SR-PCE provides scalable multi-domain, engineered path computation capabilities, and enables communication from a centralized SDN controller to the headend node at the ingress of a SR-TE domain and in charge of steering a traffic flows across it.

This may be applicable in those cases where automatic tunnel configuration is requested, to simplify the operational processes and reduce state in networks.

It is worth mentioning that the SRv6 network programming based on SID, Locator, Function and SR-TE Policies is complementing the GANA-based Programmable Network [i.29].

6.3.4 Application-aware Networking

There are proposals in the IETF for APplication-Aware Networking (APN), for which a working group is being considered.

One of the key objectives of APN is for the network to provide fine-grain SLA guarantees instead of coarse-grain traffic operations. Among various applications being carried and running in the network, some applications have much more demanding performance requirements such as low network latency and high bandwidth. In order to achieve better Quality of Experience (QoE), the network needs to be able to provide fine granularity and even application-level SLA guarantee. MPLS dataplane is rarely used at the packet origin (i.e. Branch Office) and therefore it is not possible to assume the MPLS encapsulation is available end-to-end in the traffic flow journey. So IPv6/SRv6 dataplane provides a better option for APN due to its flexibility, address space and further developments of SRv6 [i.19] and [i.20].

When APN applies to the IPv6/SRv6 dataplane, it is referred as "APplication-aware IPv6 Networking (APN6)". APN6 conveys information into the network infrastructure about the characteristics of the application associated with a traffic flow (including application identification and network performance requirements), using IPv6/SRv6 encapsulation allowing the network to quickly adapt and perform the necessary network resource adjustments to maintain SLA performance guarantees, and hence better serve application fine-grained service requirements. APN6 may fit well with the Software-Defined Wide Area Network (SDWAN) architecture.

6.3.5 SRv6 and SDWAN

With the adoption of the public cloud reliable and efficient data interconnection is critical. The solution to build a high performance Wide Area network (WAN) is given by Segment Routing over IPv6 (SRv6 and SDWAN technologies

SRv6 brings several key benefits. First, it connects enterprise sites and clouds by programming end-to-end paths at ingress nodes via source routing. It accomplishes this by leveraging routing protocols (OSPF or IS-IS) to distribute segment identifiers and utilizes them in the IPv6 destination address of the IPv6 header, as well as in the Segment Routing Header (SRH) extension header (see clause 6.3.2.).

SDWAN will make network entities plug-and-play, allowing branches to be connected to the cloud in one hop and achieve network connectivity immediately. SDWAN can employ intelligent traffic steering and make full use of multiple link resources such as 5G and private lines, by choosing the optimal link to transmit traffic of key applications, and forward different types of traffic along different paths.

The combination of SDWAN with an SRv6 underlay can provide significantly more path choices for the SDWAN to steer traffic on.

6.4 IPv6-only in 5G SA user plane based on 464XLAT/NAT64+DNS64

IPv6-only in 5G SA user plane based on limited IPv4 connectivity across an IPv6-only network (464XLAT) combined with Network Address Translation IPv6 addresses into IPv4 addresses (NAT64) and a Domain Name System (DNS) service that returns AAAA records (AAAA records to specify the IPv6 address of the server that contains Uniform Resource Locator site) with these synthetic IPv6 addresses for IPv4-only destinations(DNS64).

This clause discusses the possible IPv6-only transition solutions, and the process of selecting one of them to fit the need.

[i.15] reports the most common transition solutions for IPv6-only service delivery, 464XLAT, Dual Stack Lite is an architecture that allows IPv4 services to be provided in an IPv6 network (DS-lite), Lightweight IPv4 over IPv6 (lw4o6) An Extension to the Dual-Stack Lite Architecture (IETF RFC 7596 [i.72]), that MAP-T (IETF RFC 7599 [i.73]) translates the IPv4 header to the IPv6 header (and vice versa), MAP-E (IETF RFC 7597 [i.74]) encapsulates the entire IPv4 packet into the IPv6 packet.

For Mobile BroadBand (MBB), the IPv6 hosts (e.g. the Apps on the UE) behind the IPv6-only Customer-Premises Equipment (CPE) (i.e. the User Equipment (UE) itself) can natively access IPv6 websites or services. However, in order to access IPv4 websites, NAT64 and DNS64 are needed. NAT64 [i.31] is needed to accomplish the translation. DNS64 [i.32] is likely needed too, assuming DNS queries are required, see Figure 16. Note that Figure 5 shows how an IPv6-only host accesses an IPv4 website.

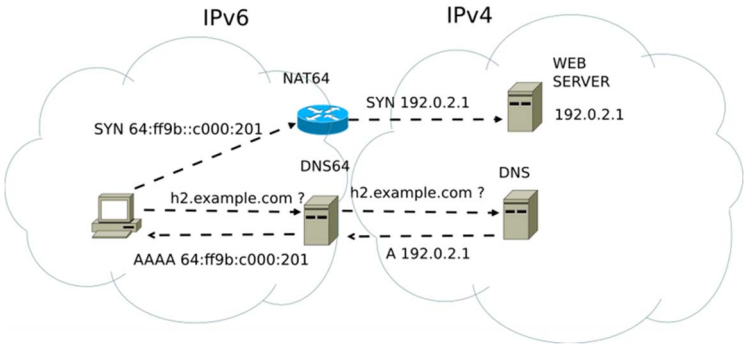


Figure 5: NAT64+DNS64: how they work (source: Wiki)

But "*NAT64+DNS64 is not sufficient for all scenarios. For example, when an IPv6-only UE is serving as a hotspot, some tethering devices may only support IPv4. To support such IPv4 hosts behind an IPv6-only CPE, 464XLAT [i.33] is a suitable choice, because 464XLAT consists of a "Client-side NAT46" (CLAT) at the CPE and a "Provider side NAT64" (PLAT), see Figure 6. PLAT is identical to the one described in the first case, while CLAT at the CPE can translate the IPv4 traffic from the IPv4 hosts into IPv6 traffic. So with 464XLAT, this second scenario effectively becomes the first scenario. On the provider side, NAT64 is the only NAT, and both IPv4 and IPv6 hosts behind the IPv6-only CPE will work, for any kind of website.*"

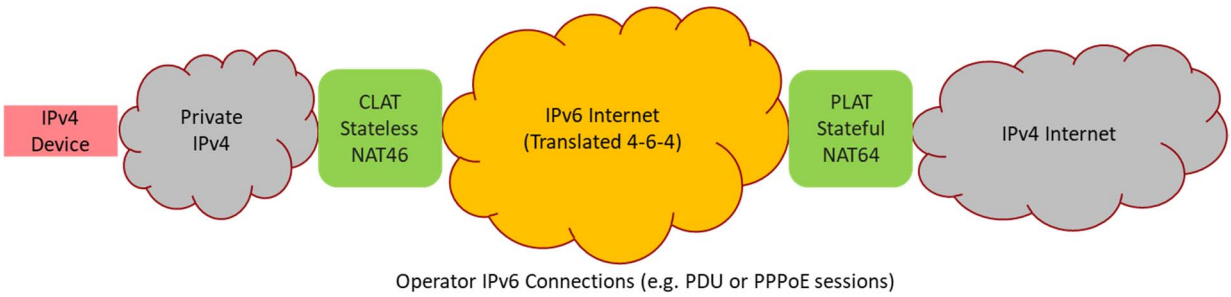


Figure 6: Overview of the 464XLAT (IPv4 as a service on top of IPv6 network)

"*Note that most of the mobile UE Operating System Embedded (Ose) support the client part of 464XLAT (provider part of 464XLAT is not relevant to mobile OSes). Furthermore, according to [i.30], mobile OSes generally do not support other IPv6-only transition solutions. Consequently, 464XLAT can be considered to be effectively the only IPv6-only solution for MBB.*

For FBB and enterprises, if the CPEs support 464XLAT, in particular CLAT, then it is the recommended IPv6-only solution. In this way, MBB, FBB and enterprises can apply the same solution, and NAT64 will be the only NAT. This can simplify network operations and management and reduce OPEX.

If the operators' CPEs do not support 464XLAT, then the DS-Lite IPv6 transition solution is a viable alternative. It is important to mention that many existing fixed IPv6-only deployments use DS-Lite, possibly due to the fact that DS-Lite was the first IPv6-only transition solution that was published, indeed DS-Lite [i.34] was published in Aug. 2011, while 464XLAT [i.33] was published in April 2013. Figure 18 provides an overview of the DS-Lite architecture. The IPv6 traffic will be transported natively; IPv4 traffic will be tunnelled from Basic Bridging Broadband (B4) to Address Family Transition Router (AFTR), where traffic will be decapsulated and NATted. The solution is comparable to 464XLAT in terms of technical merit, but it is different from the IPv6-only solution used for MBB. This could mean that operators will need to deploy two different NATs, NAT64 for MBB and NAT44 for FBB." [i.67]

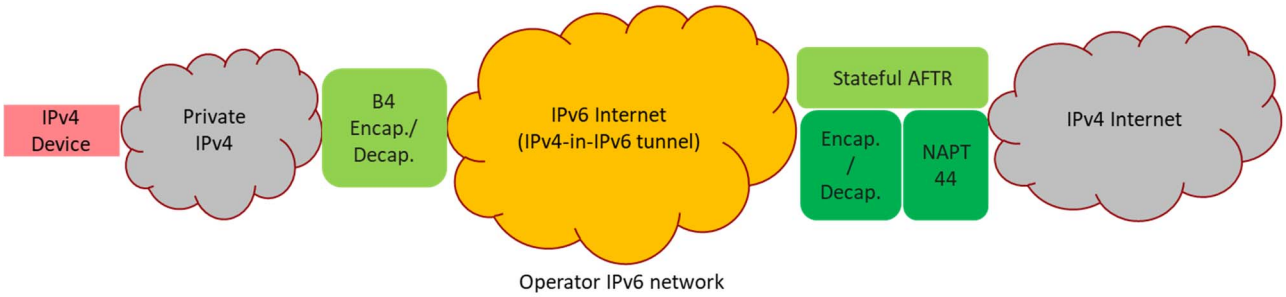


Figure 7: Overview of DS-Lite architecture (IPv4 tunnel in IPv6 network)

Based on the above discussion Dual-Stack is recommended as the IPv6 transition solution for IPv6 introduction in the early-stage, and 464XLAT / DS-Lite for the IPv6-only service delivery.

Note that MAP-T translates the IPv4 header to the IPv6 header (and vice versa), MAP-E encapsulates the entire IPv4 packet into the IPv6 packet . Theyhave clear technical merit for the Fixed BroadBand (FBB) scenario

[i.35] defines the Test Purpose, the Test Descriptions and the Abstract Test Suite (ATS) for IPv6-only services over 5G.

6.5 Network Automation and SDN

In the new world of networking, Network Functions Virtualisation (NFV) and Software-Defined Networking (SDN) are new paradigms in the move towards open software and network hardware. While NFV aims to virtualize network functions and deploy them into general-purpose hardware, SDN makes networks programmable by separating the control and data planes. NFV and SDN are complementary technologies capable of providing one network solution.

NOTE: Insights on how the GANA Knowledge Plane (KP) Platform integrates with other management and control systems (such as SDN controllers and NFV MANO, OSS/BSS and Service Orchestrators, etc.) and the network are provided in clause 4.

In this context, every network can benefit from the centralized model of NFV/SDN, rather than staying with networks that operate on the decentralized model of the Internet. In particular, the use of NFV/SDN can help to achieve levels of performance, resource optimization, and user responsiveness that are unthinkable in decentralized networks.

There are some considerations about the moving of a network to use SDN.

SDN can lower operating costs (OPEX) because most of the operating costs in a network are in network management. SDN provides new ways to centralize, automate and therefore simplify network management. Many tasks are made easier, such as changing switch/router configurations, adding new nodes to the network, detecting network issues, resolving these issues and maintaining security. The SDN automation also facilitates insight into the network and this is key for reducing the cost of network management. SDN does not impact substantially on capital expendure costs (CAPEX), indeed networking equipment are reliable, secure, high performing, power-efficient, and more, so the cost of building the equipment is not changing.

Moving to SDN allows faster introduction of new capabilities into the network. The intelligence is out of the switches/routers and into the controller/orchestrator. This means that the network functionality can be enabled through software and installed faster in the network. Hence, SDN relies on stable communication between network nodes and the controller. Ensuring the reliability of this critical communication path is very important.

SDN can improve network security, indeed security depends on blocking malicious users and malicious traffic. The SDN controller helps to ensure rapid and automated detection and to block malicious traffic within the network.

In addition, SDN can provide a better experience for the end users of the network. As new devices and services become available, users want to adopt them as soon as possible. So in the network it is required a high level of flexibility and the network infrastructure should be dynamic and responsive. SDN can automatically adapt to dynamic changes and enhance the user experience.

As described in [i.36], SDN also helps with the IPv6 transition; in particular the SDN Controller can guide IPv4 / IPv6 traffic to the appropriate network function (or virtual network function) automatically, the NFV allows the Internet Service Provider (ISP) to deploy virtual IPv4 / IPv6 network function in the same infrastructure.

Thanks to SRv6 SDN controller interactions, ISP can grant the SLA e2e even in the customer premises network, cloud network and service lan consistently.

6.6 IPv6/SRv6 Operations Administration and Maintenance (OAM) tools and Automation (mapping with GANA)

Thanks to the extensibility of the IPv6 protocol, new methodologies for telemetry and performance measurements can be used. In-situ Flow Information Telemetry (IFIT) denotes a family of flow-oriented on-path telemetry techniques which can provide high-precision flow insight and real-time network issue notification (e.g. jitter, latency, packet loss).

Alternate Marking, defined in [i.37] and [i.38], enables a flexible approach to network management that can be combined with SDWAN. As said, SDWAN allows connecting remote branch offices to data centres and building higher-performance WANs. This helps ensure that application performance meets Service Level Agreements (SLAs). The Alternate Marking methodology [i.37] and in particular its application to multipoint flows can also help the path selection for the WAN connection based on per-cluster and per-flow performance measurement and analytics as described in [i.38].

These new emerging techniques for telemetry and performance measurements are bringing out a new paradigm to allow Closed Loop Automation. It means that the relation between the Controller and the network is now bidirectional and the telemetry information can help the controller to decide accordingly. Since SDN Automation is now evolving and Yet Another Next Generation (YANG); a data modeling language; is now everywhere as a configuration language for networking, this approach is also known as Model Driven.

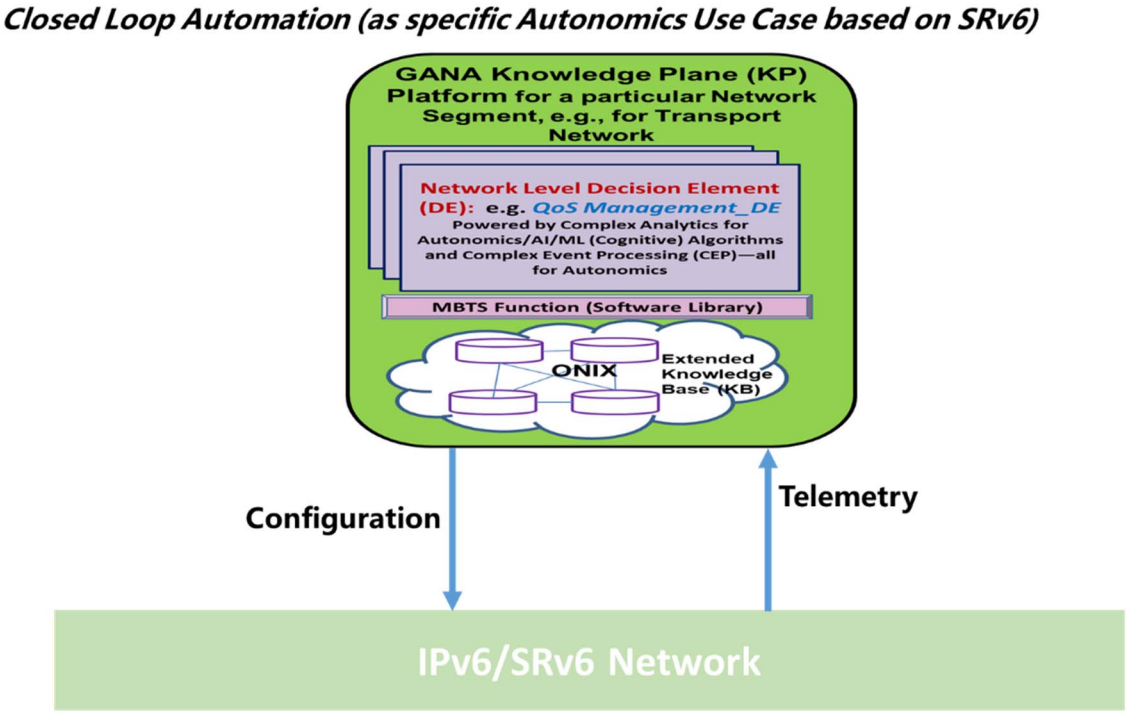


Figure 8: Closed loop automation for IPv6/SRv6 Network

NOTE: While Telemetry should be fed to the GANA KP Platform, it is important to note that the GANA framework also provides for principles by GANA DEs introduced to run within Network Elements/Functions (NEs/NFs) as GANA Nodes help limit the types and volume of telemetry data exported by the NEs/NFs to the KP Platform's DEs or Data Lake as the lower level DEs can perform certain delegated decisions based on observations (views) accessible by the DEs at that low level while the lower level DEs then export only some reports to the GANA KP Platform level's Network Level DEs. NEs/NFs within embedded DEs should still be configured to export certain types and volume of monitoring data to an external Data Lake and/or to the GANA KP Platform responsible for the NE/NF. These aspects on need and benefits to limiting the types and volume of monitoring data that may be exported by NEs/NFs are covered in ETSI TS 103 195-2 [i.2] dissertation on autonomics in multi-layer transport networks]. Applications, IP Flows, or Services that utilize the network or network slices should be made to provide (directly or indirectly) end-to-end requirements (e.g. acceptable end to end latency, throughput, jitter, security requirements, etc. as part of SLA) to GANA KP Platforms of the End-to-End so that the KPs act to assure the service offered by the network to fulfil the requires, including collaboratively working together to achieve E2E service assurance and E2E security assurance as required by the SLAs.

The Network orchestrator will need to manage the network at multiple layers:

- Flex-E configuration needs to be maintained and eventually reconfigured according to foreseen traffic volumes for the different categories of QoS.
- Assignment of Flex-E link and nodes to each Hard Slice (as both primary and backup link to be used only in case of failure) has to be dynamically managed.
- SRv6 connections have to be established in real-time, determining the proper Hard Slice to be used and the SR path to reach the destination according to the information received by the 5G SA core network.
- Service Function Chain can be realized, including in the SR path application information accordingly.
- In the event of a fault, activation of backup and quick convergence of the overall transport network needs to be granted.

The network design discussed so far moved from the assumption of running a traditional, distributed control plane where each router contributes to the exchange of reachability information through a mix of IGP protocols and BGP.

The approach currently adopted by many operators worldwide is to enable network automation through the SDN capability introduced in clause 5.6. In this context, an SDN system becomes the network controller, centralizing the control of the network and becoming the unified point from where policies and configurations are delivered to the network nodes.

A way to represent the role in SDN in the centralization of the network control processes is shown in Figure 9.

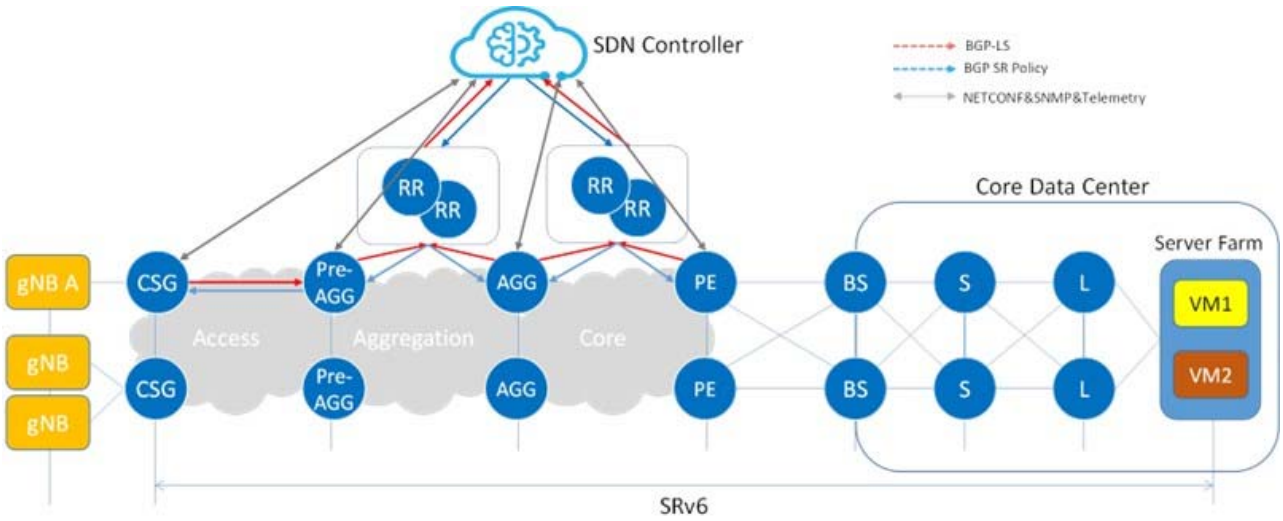


Figure 9: SDN role in an IPv6/SRv6 network

The SDN controller acts as the centralized repository of the configurations of all nodes, retrieved by several mechanisms or protocols, such as Netconf [i.39], Command Line Interface (CLI), Simple Network Management Protocol (SNMP), and others.

The SDN controller joins the network control plane, collecting the routing information distributed by the routers in the network. This information includes the IGP and BGP reachability and allows the SDN controller to construct the network topology. In addition to the routing information, the SDN controller also collects the status of the network components (e.g. a router's behaviour or the status of an interface) and the degree of utilization of the network resources. This may be achieved using different technologies (e.g. telemetry protocols, exchange of management data, configuration scripts). A way often found in live networks is BGP Link-State (BGP-LS) [i.40] and [i.41].

BGP-LS has been designed to derive from IGP protocols both the current state of the network connections and the associated TE information and share them with external components. Here an SDN controller finds its perfect fit: as highlighted in Figure 9, the SDN controller receives the BGP-LS updates from the Route Reflectors (RR), which in turn receive them from the other network nodes.

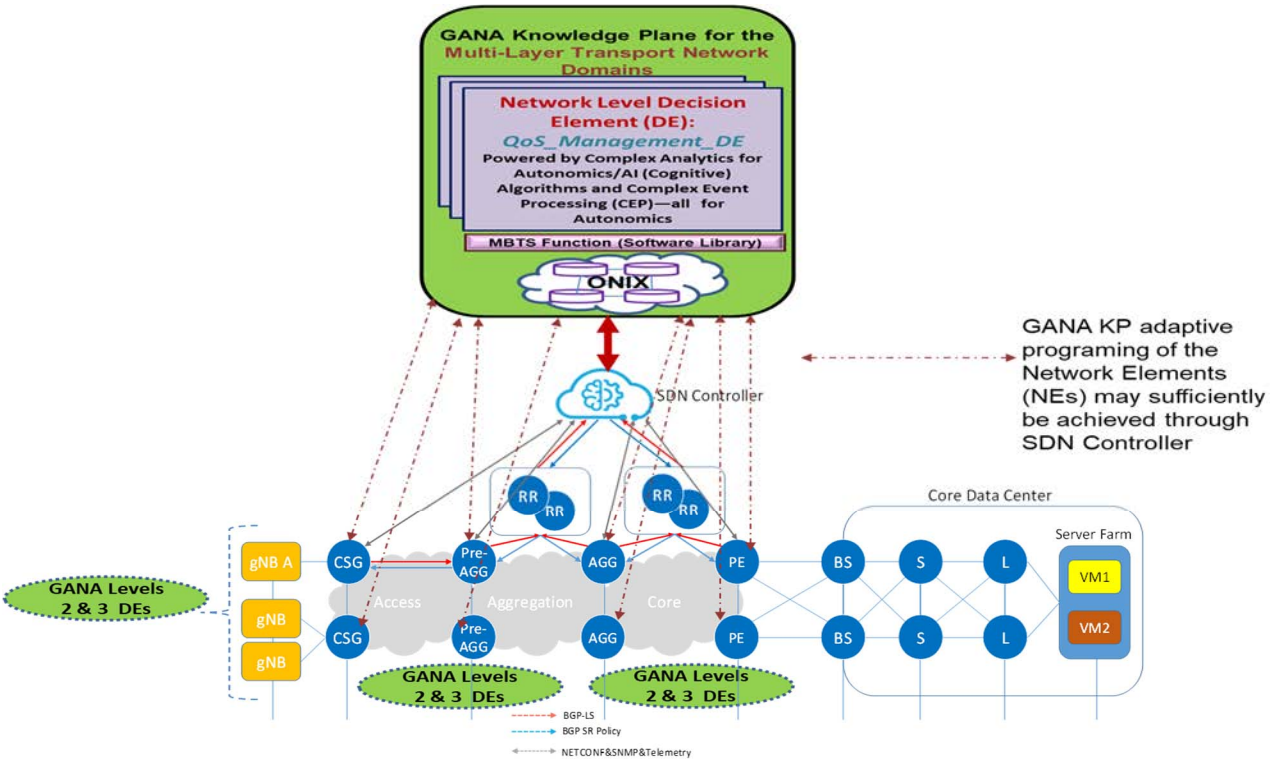
As shown, Pre-AGG, AGG, and Provider Edge (PE) devices collect IGP topology, bandwidth, link delay and report such information to RRs by BGP-LS. RRs report it to the SDN controller.

Once SDN knows the full network topology, including awareness of the network resources, it can take control over the entire network, implementing functions such as:

- Assigning the addresses to each node
- Delivering the SRv6 SIDs and locators
- Computing the SR policies identified by <Head-end, colour, End-point>
- Assigning the relevant resources to a network slice

Several mechanisms are also available for an SDN Controller to push the path information down to the network nodes. A way to propagate BGP SRv6 policies (sometimes abbreviated with BGP SR, as shown in Figure 10 is through [i.42].

An SDN controller uses BGP SRv6 to advertise an SR forwarding policy towards a headend node. The SR forwarding policy may include one or more candidate paths, each consisting of more segment lists. The SRv6 forwarding policy is used to describe the path of the IP packets from Source to Destination nodes across the network.



NOTE: Multi-Layer aspect in transport networks usually implies IP and Optical Level.

Figure 10: GANA Knowledge Plane (KP) Platform integration with SDN Controllers of Multi-Layer Transport Domains

6.7 Other ETSI IPE Reference Architecture Scenarios for consideration

In this clause a set of selected architectural scenarios on IPv6 in 5G Networks are presented, with the aim to add insights on the impact of introducing GANA Autonomics into the Architectures and the interplay of some key aspects in the architectures with GANA autonomics.

NOTE 1: Insights on how the GANA Knowledge Plane (KP) Platform integrates with other management and control systems (such as SDN controllers and NFV MANO, OSS/BSS and Service Orchestrators, etc.) and the network are provided in clause 4.

Figure 11 presents a 5G security architecture scenario presented in ETSI GR IPE 005 [i.65]. The impact of introducing GANA Autonomics into this architecture scenario is as follows:

- The Access part would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the Access network;
- The Transport network part would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the transport network;
- The Security Gateway (SEG) would have GANA Level-3 Security Management-DE instantiated into it to make it autonomic (control-loop based intelligent) in the way it operates;
- The Firewall (FW) would have GANA Level-3 Security Management-DE instantiated into it to make it autonomic (control-loop based intelligent) in the way it operates; the core network would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some NEs/NFs of the core network.

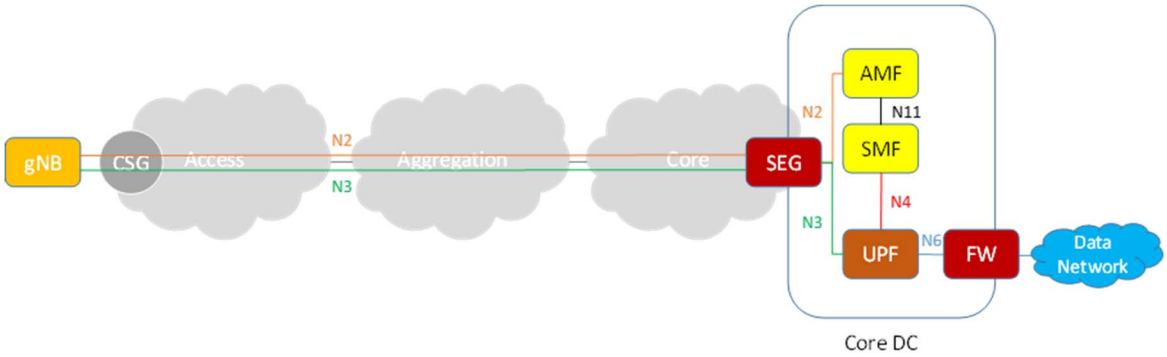


Figure 11: 5G security architecture (Courtesy of ETSI GR IPE 005 [i.65])

Figure 12 presents Typical architecture of a mobile transport network architecture described in ETSI GR IPE 005 [i.65]. The impact of introducing GANA Autonomics into this architecture scenario is as follows:

- The transport network would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the transport network;
- The Radio Access network part would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the Radio Access network.

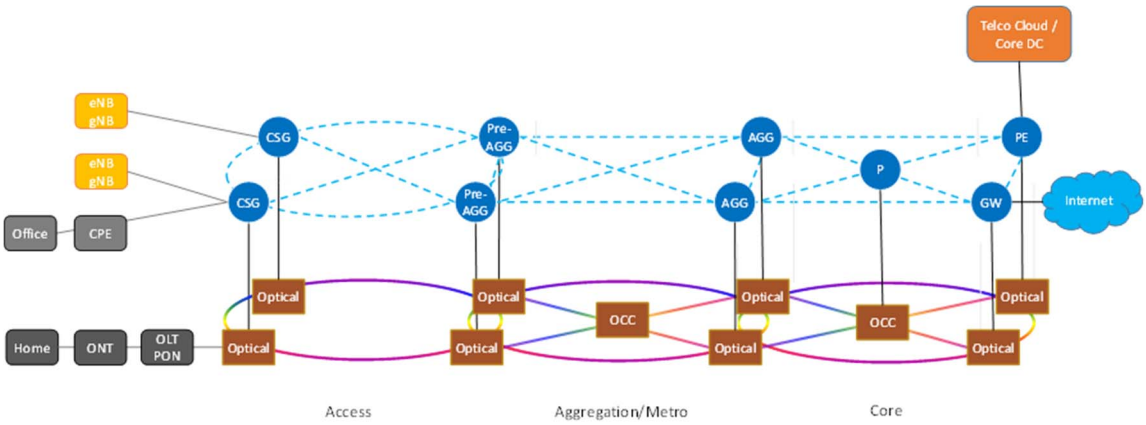


Figure 12: Typical architecture of a mobile transport network architecture (Courtesy of ETSI GR IPE 005 [i.65])

Figure 13 presents High-level architecture of a packet-based (layer-3) mobile transport network described in ETSI GR IPE 005 [i.65]. The impact of introducing GANA Autonomics into this architecture scenario is as follows:

- The transport network would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the transport network;
- Instantiation of GANA onto a Telco-Cloud environment follows approach described in ETSI TR 103 473 [i.4];
- The Radio Access network part would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the Radio Access network.

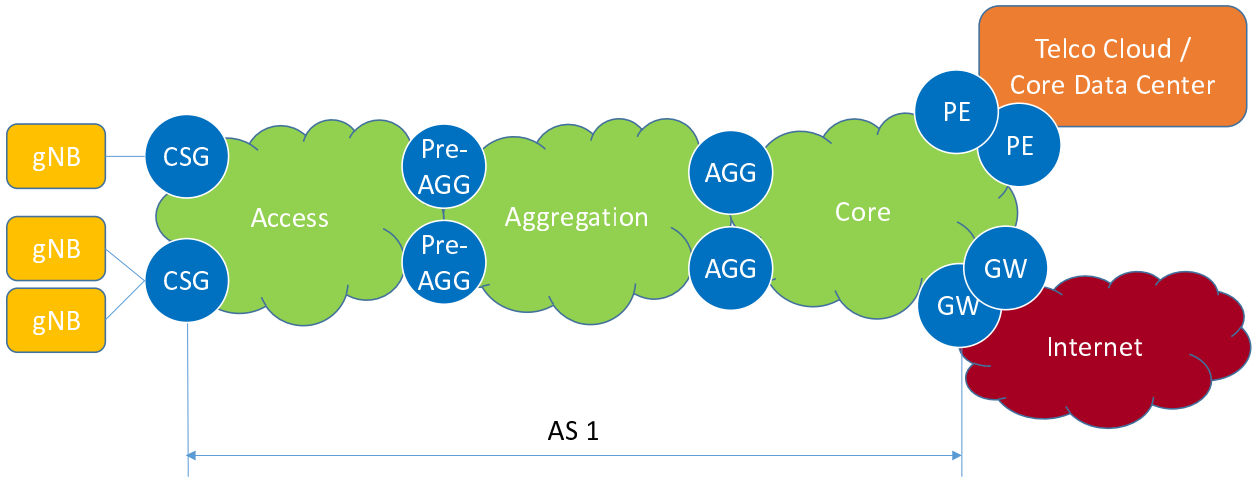


Figure 13: High-level architecture of a packet-based (layer-3) mobile transport network (Courtesy of ETSI GR IPE 005 [i.65])

Figure 14 presents Multiple Autonomous System Numbers (ASN) in a mobile transport network scenario described in ETSI GR IPE 005 [i.65]. The impact of introducing GANA Autonomics into this architecture scenario is as follows:

- The transport network would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the transport network;
- Instantiation of GANA onto a Telco-Cloud environment follows approach described in ETSI TR 103 473 [i.4];
- The Radio Access network part would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the Radio Access network.

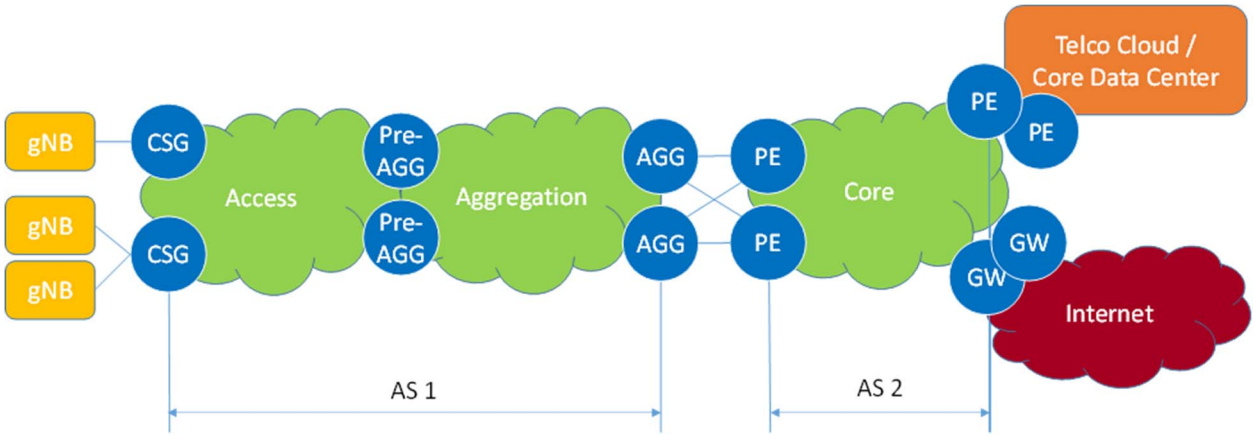


Figure 14: Multiple ASNs in a mobile transport network (Courtesy of ETSI GR IPE 005 [i.65])

Figure 15 presents a Routing architecture scenario described in ETSI GR IPE 005 [i.65]. The impact of introducing GANA Autonomics into this architecture scenario is as follows:

- The transport network would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the transport network;
- Instantiation of GANA onto a Data Centre (DC) physical network infrastructure follows the approach described in ETSI TR 103 404 [i.5] and if the DC is a virtualized one then the instantiation of GANA onto such virtualized DC network follows approach described in ETSI TR 103 473 [i.4];
- The Radio Access network part would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the Radio Access network.

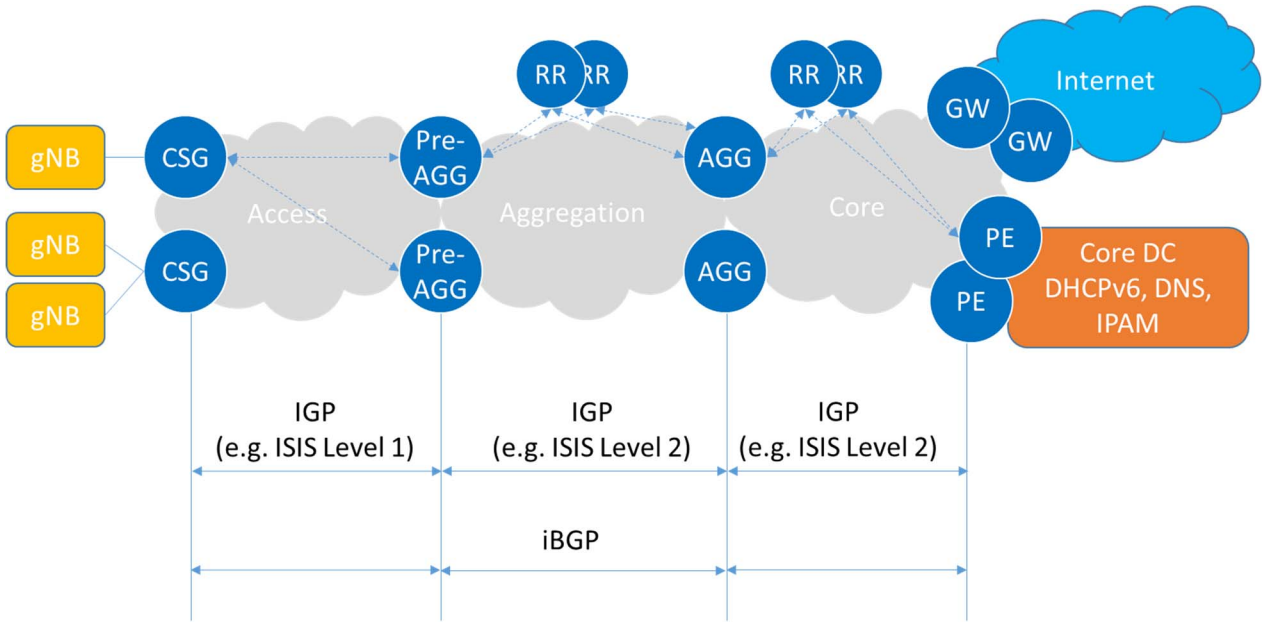


Figure 15: Routing architecture
(Courtesy of ETSI GR IPE 005 [i.65])

Figure 16 presents an End-to-end view, including RAN and Core DC described in ETSI GR IPE 005 [i.65]. The impact of introducing GANA Autonomics into this architecture scenario is as follows:

- The transport network would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the transport network;
- Instantiation of GANA onto a Data Centre (DC) physical network infrastructure follows the approach described in ETSI TR 103 404 [i.5] and if the DC is a virtualized one then the instantiation of GANA onto such virtualized DC network follows approach described in ETSI TR 103 473 [i.4];
- The Radio Access network part would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the Radio Access network.

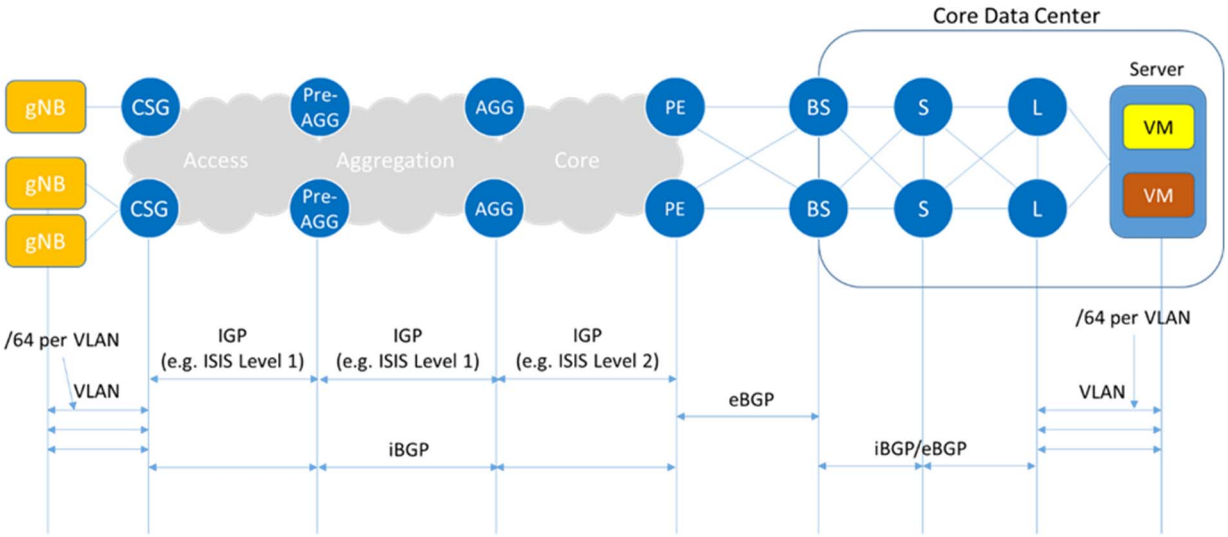


Figure 16: End-to-end view, including RAN and Core DC
(Courtesy of ETSI GR IPE 005 [i.65])

Figure 17 presents End-to-end transport of 5G services described in ETSI GR IPE 005 [i.65]. The impact of introducing GANA Autonomics into this architecture scenario is as follows:

- The transport network would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the transport network;
- Instantiation of GANA onto a Data Centre (DC) physical network infrastructure follows the approach described in ETSI TR 103 404 [i.5] and if the DC is a virtualized one then the instantiation of GANA onto such virtualized DC network follows approach described in ETSI TR 103 473 [i.4];
- The Radio Access network part would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the Radio Access network.

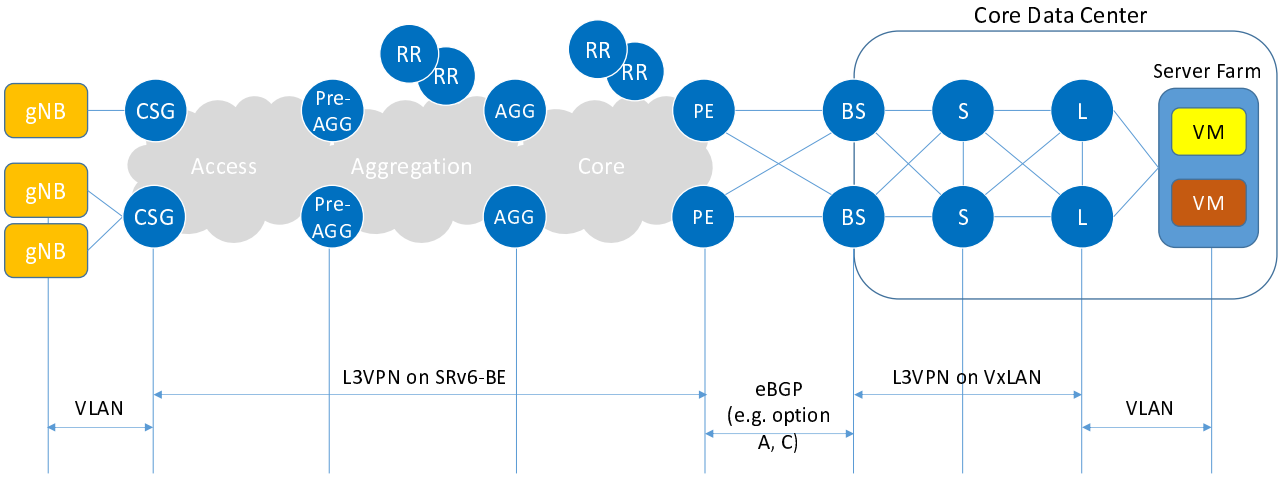


Figure 17: End-to-end transport of 5G services (Courtesy of ETSI GR IPE 005 [i.65])

Figure 18 presents VRF-based Service Infrastructure described ETSI GR IPE 005 [i.65]. The impact of introducing GANA Autonomics into this architecture scenario is as follows:

- The transport network would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the transport network;
- Instantiation of GANA onto a Data Centre (DC) physical network infrastructure follows the approach described in ETSI TR 103 404 [i.5] and if the DC is a virtualized one then the instantiation of GANA onto such virtualized DC network follows approach described in ETSI TR 103 473 [i.4];
- The Radio Access network part would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the Radio Access network.

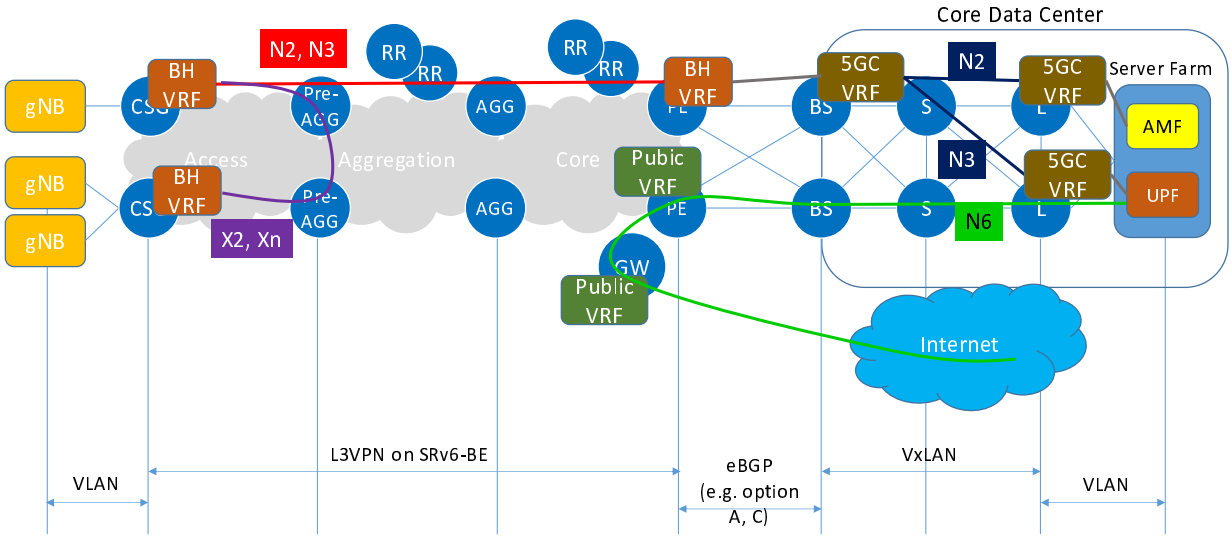


Figure 18: VRF-based Service Infrastructure (Courtesy of ETSI GR IPE 005 [i.65])

Figure 19 presents Network OAM protocols considered in ETSI GR IPE 005 [i.65]. The impact of introducing GANA Autonomics into this architecture scenario is as follows:

- There are GANA DEs that are responsible for autonomically managing and orchestrating OAM protocols (in particular the Monitoring-DE can be implemented to manage and orchestrate protocols such as Bidirectional Forwarding Detection (BFD), Two-Way Active Measurement Protocol (TWAMP), and Internet Control Message Protocol (ICMP) based monitoring tools/mechanisms);
- The transport network would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the transport network;
- Instantiation of GANA onto a Data Centre (DC) physical network infrastructure follows the approach described in ETSI TR 103 404 [i.5] and if the DC is a virtualized one then the instantiation of GANA onto such virtualized DC network follows approach described in ETSI TR 103 473 [i.4];
- The Radio Access network part would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the Radio Access network.

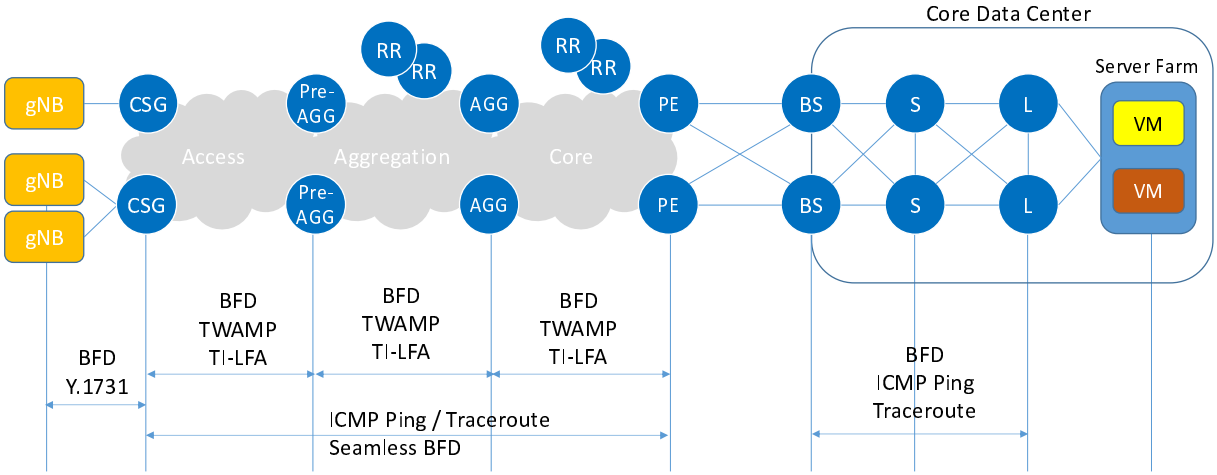


Figure 19: Network OAM protocols (Courtesy of ETSI GR IPE 005 [i.65])

Figure 20 presents the Evolution of the IPv6-based 5G transport architecture described in ETSI GR IPE 005 [i.65]. The impact of introducing GANA Autonomics into this architecture scenario is as follows:

- There are GANA DEs that are responsible for autonomically managing and orchestrating forwarding related protocols such as SRv6 (in particular the Forwarding-DE can be implemented to manage and orchestrate protocols SRv6 the other forwarding protocols;
- The transport network would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the transport network;
- Instantiation of GANA onto a Data Centre (DC) physical network infrastructure follows the approach described in ETSI TR 103 404 [i.5] and if the DC is a virtualized one then the instantiation of GANA onto such virtualized DC network follows approach described in ETSI TR 103 473 [i.4];
- The Radio Access network part would have a GANA KP associated with it instantiated and with possibility to have GANA levels 2 and 3 DEs introduced into some (possibly all) NEs/NFs of the Radio Access network.

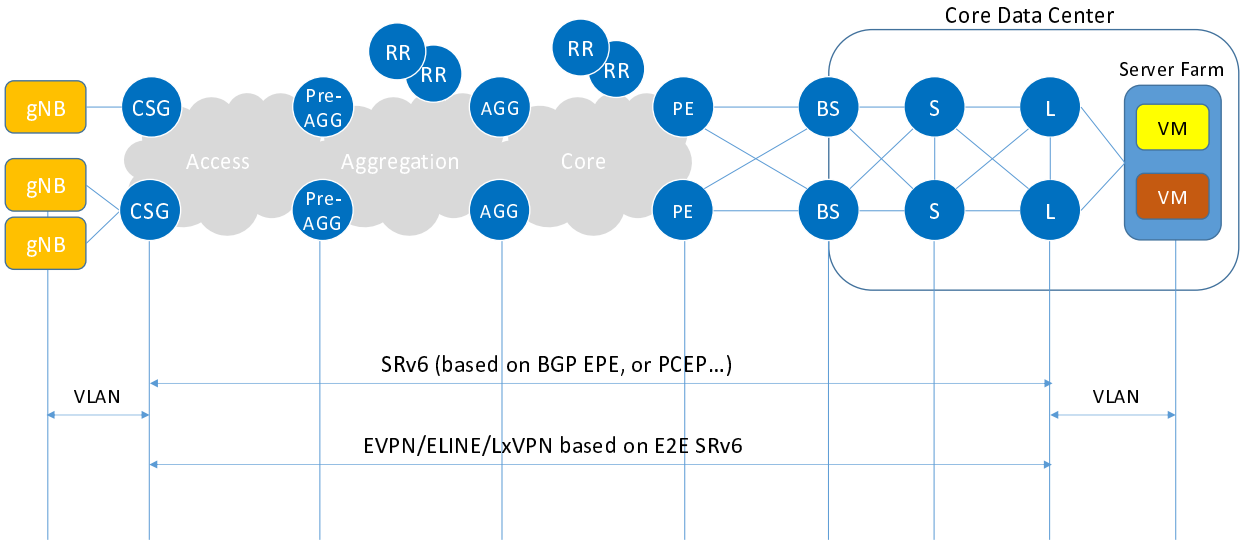


Figure 20: Evolution of the IPv6-based 5G transport architecture (Courtesy of ETSI GR IPE 005 [i.65])

NOTE 2: For further study: Reference Architecture Scenarios that consider "IPv4 as a Service" in the IPv6-Only based 5G & Beyond Networks.

7 GANA Autonomic Management & Control (AMC) for IPv6 Protocols; IPv6 Capabilities that enable to Design & Build Autonomic 5G Networks and Services

7.1 Overview on GANA Autonomic Management & Control (AMC) of IPv6 Protocols in E2E 5G Networks, with consideration for Use Cases of AI/ML in the AMC

Figure 21 presents an expanded view of the GANA node structure, the Decision Plane and Control Plane views and example assignments of DEs to some protocols, stacks and mechanisms as Managed Entities (MEs), that can be applied for a case of a GANA Node running IPv6 Protocols as Managed Entities (MEs).

NOTE: More details on this can be found in ETSI GS AFI 002 [i.12].

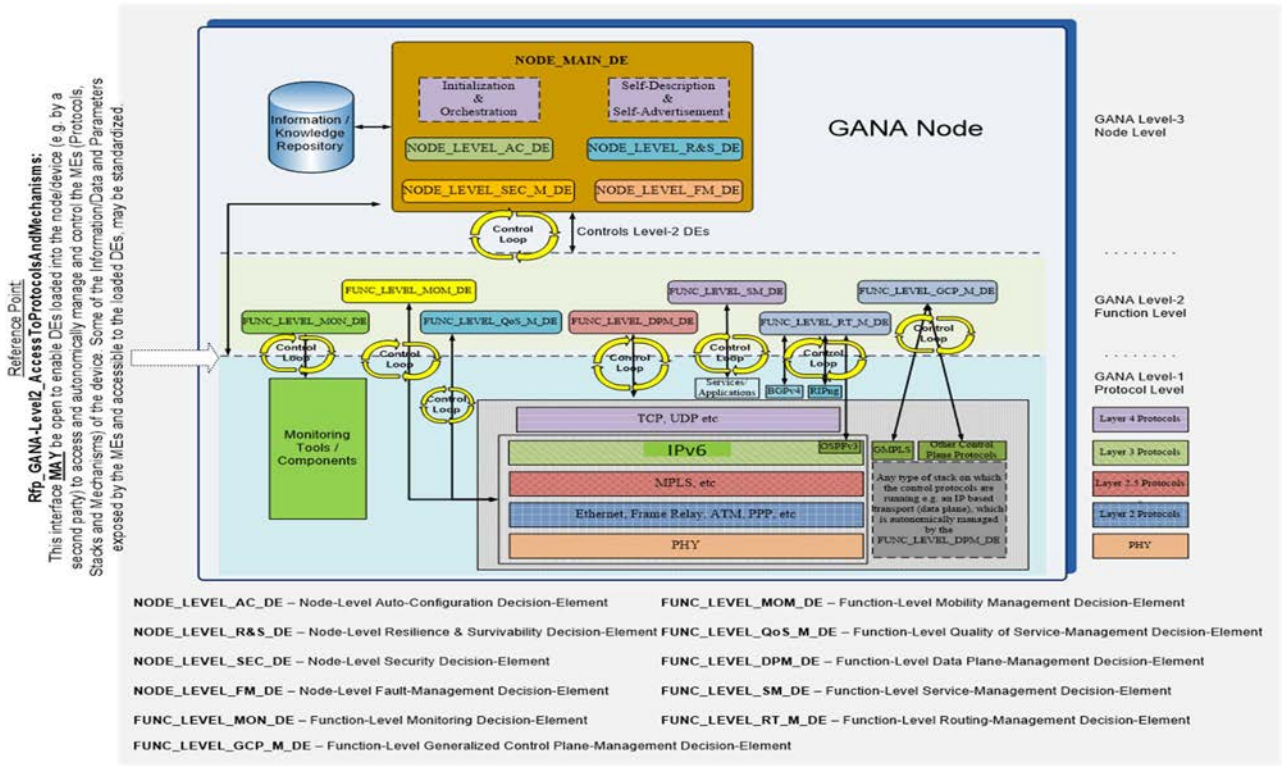


Figure 21: Expanded view of the GANA node structure, the Decision Plane and Control Plane views and example assignments of DEs to some protocols, stacks and mechanisms as Managed Entities (MEs)

Figure 22 presents the interworking of Automated Management and Autonomic Management through the GANA Operations Procedures, and this framework described in ETSI TS 103 195-2 [i.2] on how the Autonomated Management Framework with Profiles is expected to work should be considered when deploying GANA autonomics onto the IPv6 based 5G network too.

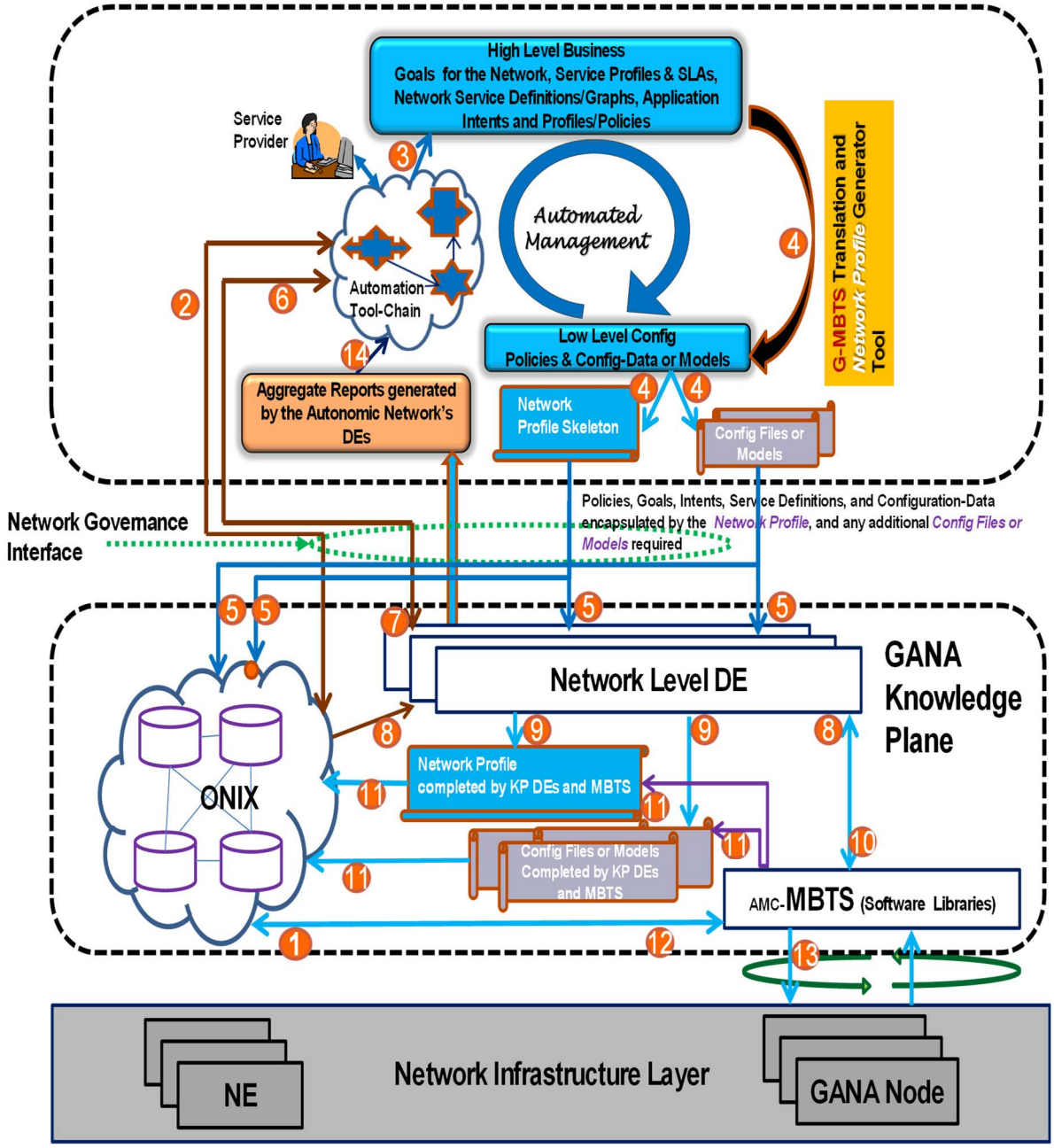


Figure 22: The Interworking of Automated Management and Autonomic Management through the GANA Operations Procedures

7.2 IPv6 Capabilities that enable to Design and Build Autonomic 5G Networks and Services

IPv6 Capabilities that enable to Design and Build Autonomic 5G Networks and Services have been started by the Seventh framework programme (FP7) of the European Community (EC) for research and technological development and demonstration activities [i.2] and IETF work such as work on ANIMA Protocols [i.60].

Research Projects like the European Commission (EC) funded FP7 Project EFIPSANS [i.59] carried out research on IPv6 capabilities that enable to design and build autonomic networks and services. **EFIPSANS stands for: Exposing the Features in IP version Six (IPv6) Protocols that can be exploited/extended for the purposes of designing/building Autonomic Networks and Services**. The EC funded FP7 EFIPSANS carried out the following study and produced results of relevance to the subject. EFIPSANS Project's main results covered the following aspects:

1) EFIPSANS Project examined and documented a number of the "existing" core IPv6 Features exploitable for autonomic networking (advanced Self-Managing Network Features) [i.43], [i.44], [i.53] and [i.62].

2) EFIPSANS Project came up with some proposals on Extensions to IPv6 (IPv6++) that may be developed along the path to the Self-Managing Networks of the future [i.43], [i.44], [i.48] and [i.62].

EFIPSANS Project findings are that IPv6 offers a lot of rich communication features and extensible communication possibilities beyond what is available in IPv4**.** The following **features in IPv6** can be considered as **enablers for designing large-scale networks** in which the basic attributes of scalability and some automated discovery and auto-configuration are required as enablers for more advanced autonomic/self-managing network behaviours:

- Neighbour Discovery (ND);
- auto-Configuration;
- support for dynamic network re-numbering;
- improved routing mechanisms;
- improved Quality of Service (QoS) handling;
- improved transport efficiency;
- improved security;
- flexibility for protocol extensions;
- advanced addressing schemes and route aggregation;
- true End-to-End communication;
- concepts for realizing "locator/identifier split";
- Bootstrapping Mechanisms, etc.

In EC funded EFIPSANS Project, some ideas on Extensions to IPv6 emerged and were developed:

- As **draft IPv6 Extension Headers** (new IPv6 protocols that complement existing IPv6 protocols);
- **Newly added protocol Options** in the Extension Headers that support the notion of Options;
- **Extensions to the "management interfaces" of some protocols** for ensuring enriched access to the protocols and autonomic management and control of the protocols by associated Decision-Making-Elements (DEs), and network architectural extensions such as cross-layering, etc.
- Examples of IPv6 protocol Extensions for self-managing networks innovated by EFIPSANS Project [i.59] include the following:
  - ICMPv6++ [i.61] for advanced control information exchange for use in DE-to-DE communications;
  - ND++ [i.43], [i.44] for advanced Auto-Discovery;
  - DHCPv6++ [i.43], [i.44] for advanced Auto-Discovery and Auto-Configuration as a protocol for providing ONIX Services;
  - PMIPv6++ [i.56]: This was not an extension to the protocol itself but to configurable and controllable parameters on the management interface of the protocol that DE can use in autonomic management and control of the PMIPv6 protocol;
  - IPv6 Extension Header for carrying advanced QoS Options, Other types of Newly added Options, some recommendations for Extensions to protocols like OSPFv3, and some newly suggested Extension Headers, etc.

Examples of protocols put forward in IETF and are of relevance to consider for GANA autonomics in IPv6 based networks:

1) Autonomic IPv6 Edge Prefix Management in Large-Scale Networks, IETF RFC 8992 [i.69].
2) GeneRic Autonomic Signalling Protocol (GRASP), IETF RFC 8990 [i.70].

3) ICMPv6 based Generic Control Protocol (IGCP) [i.61] is meant to be used in DE-to-DE coordinations.

4) There may be other IPv6 protocols or new extensions in IETF made as RFC Drafts proposals that need to be studied.

8 Framework for Implementing Autonomic/Autonomous IPv6 based 5G Networks, powered by GANA Multi-Layer AI/ML & Multi-Layer AMC and IPv6 Capabilities

8.1 Overview about the Framework defined by the present document

The following is a summary of what constitutes the Framework defined by the present document. This summary helps provide insights on the Framework's key aspects for considerations by implementers of GANA Multi-Layer AI/ML & Multi-Layer AMC in IPv6 based 5G Networks. The Framework consists of the following key aspects summarized below:

Aspects described in the earlier clauses of the present document:

- Principles for Autonomic/Autonomous Networking (AcN/AN) and Autonomic Management & Control (AMC), and Enablers.
- Implementing the GANA Framework for Multi-Layer Autonomics and Multi-Layer AI/ML in IPv6 based network (e.g. an E2E 5G Network). Examples of DEs for consideration include QoS-management-DE, Security-management-DE, Mobility-management-DE, Fault-management-DE, Resilience & Survivability-DE, Service & Application management-DE, Forwarding-management-DE, Routing-management-DE, Monitoring-management-DE, Generalized Control Plane management-DE.
- Integration of the GANA Knowledge Plane (KP) with various management and control systems through which the Knowledge Plane can selectively program the network, and KP integration with Event Sources, Data Sources and Info/Knowledge Sources.
- Federated AMC by GANA KP Platforms and also Federation of low level Autonomics.
- Use Cases for AI/ML and Autonomics in E2E IPv6 based 5G Networks in general; and Mappings to GANA DEs that help implement particular Use Case.
- IPv6-Only based E2E 5G Networks: E2E Aspects of IPv6 in 5G and Reference Architecture Scenarios for Consideration; Implications on GANA Autonomics.
- GANA Autonomic Management & Control (AMC) for IPv6 Protocols; IPv6 Capabilities that enable to Design & Build Autonomic 5G Networks and Services.

Aspects described in the subsequent clauses of the present document:

- GANA Multi-Layer Autonomics & AI/ML in IPv6-Only based 5G E2E Reference Architecture Scenarios, with Consideration of the Example Autonomics Use Cases.
- DEs to MEs Mappings, and Autonomic Management & Control of IPv6 Protocols by GANA DEs.
- GANA for Access Network (Fixed Access, RAN, Other Access Networks).
- GANA Autonomics for Multi Layer Transport SDN Architecture.
- GANA for 5G Service Based Architecture (SBA).
- GANA Autonomics for MEC Architecture.

- Federation of the GANA KPs for RAN, MEC, Transport Network, Core Network, and IP Multimedia Subsystem (IMS) Layer.

8.2 GANA Multi-Layer Autonomics & AI/ML in IPv6-Only based 5G E2E Reference Architecture Scenarios, with Consideration of the Example Autonomics Use Cases

8.2.1 DEs to MEs Mappings, and Autonomic Management & Control of IPv6 Protocols by GANA DEs

Table 1 below provides a guidance on DE-to-ME Mappings Table concerning which DE is responsible for autonomic management and control of specific types of Managed Entities (MEs). Following the GANA implementation guide this means in an IPv6 network, the MEs that are IPv6 specific and those that are not IPv6 specific should be assigned to specific DEs (in a 1-ME to 1-DE relationship) using Table 1 as a guide before designing and implementing the DEs in the GANA Knowledge Plane Level and in certain NEs/NFs. For example, the Routing Management DE's MEs are routing protocols and mechanisms as illustrated on Figure A.3 3. Each DE should employ AI/ML Algorithms in the autonomic management and control of its MEs (including IPv6 Protocols accordingly) using their Managed Objects and management methods that a DE can employ, while the DE performs the autonomic management and control of its MEs in reaction to detected or predicted situations, changes in network optimization or adaptation objectives, and in collaboration with other DEs as may be necessary.

Table 1: Generic Table for the Mapping of DEs to their associated Types of Managed Entities (MEs)

Network-Level DEs	Node-Level DEs	Function-Level DEs	Protocols and Mechanisms as Managed-Entities (MEs)	Examples of protocols and Mechanisms that are mapped as MEs
	GANA NODE			
NET_LEVEL_SEC_M_DE	NODE_LEVEL_SEC_M_DE		**Security Protocols, Algorithms and Mechanisms**	Certificates/Passwords Algorithms, Hash Algorithms, Encryption Algorithms, Access Control Mechanisms, Trust Mechanisms, Denial of Service (DoS) Detection/Prevention algorithms/mechanisms, Signature based intrusion detection mechanisms, etc.
NET_LEVEL_FM_DE	NODE_LEVEL_FM_DE		Fault Detection Mechanisms, Fault Isolation/Localization/Diagnosis Mechanisms, Fault Removal Mechanisms	Active Probing mechanisms, Bi-Directional Forwarding Detection (BFD protocol) for link failure detection, Self-test/diagnose functions, rebooting, reloading, automated module replacement mechanisms, etc.
NET_LEVEL_RS_DE	NODE_LEVEL_RS_DE		Proactive and Reactive Resilience Mechanisms, Survivability Strategies and Algorithms, Restoration and Protection Mechanisms	Node Resilience mechanisms, and Network Resilience mechanisms, etc.
	NODE_LEVEL_AC_DE		Neighbour Discovery Protocols/Mechanisms and Network Discovery Mechanisms	Neighbour Discovery Protocol (NDP), Secure Neighbour Discovery Protocol (SEND), etc.
NET_LEVEL_RM_DE	NODE_MAIN_DE	FUNC_LEVEL_RM_DE	Routing Protocols and Mechanisms	OSPF, BGP, RIP, ISIS, etc.
NET_LEVEL_FWD_M_DE		FUNC_LEVEL_FWD_M_DE	Layer-3 Forwarding Protocols and Mechanisms, Layer-2.5-Fowarding, Layer-2-Fowarding, Layer-3-Switching, Layer-2-Switching, etc.	IPv4/IPv6 Forwarding Engine, Multi-Protocol Label Switching (MPLS), etc.
NET_LEVEL_QoS_M_DE		FUNC_LEVEL_QoS_M_DE	QoS Protocols and Mechanisms	Packet classifier, Packet Marker, Queue Management, Queue Scheduler, RSVP, etc.
NET_LEVEL_MOM_DE		FUNC_LEVEL_MOM_DE	Mobility Management Protocols and Mechanisms	Mobility Support in Internet Protocol Version 6 (MIPv6), Datagram Congestion Control Protocol, Mobile Stream Control Transmission Protocol, Site Multi-homing by IPv6 Intermediation, Proxy-Mobile-IP, Mobility-Management User-Equipment Managed-Entity, Measurement-Report-Function Managed-Entity, Candidate-Access-Router-Discovery mechanism, Fast Handover Scheme, Policy Control and Charging Rules Function mechanism, etc.
NET_LEVEL_MON_DE		FUNC_LEVEL_MON_DE	Monitoring Protocols, Mechanisms and Tools	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.
		FUNC_LEVEL_SM_DE	Services and Applications	Orchestration of services, service-discovery, interpretation of service and application requirements at run-time and requesting the network layer to behave in a service/application-aware manner, realizing a control-loop over the services/applications as its Managed Entities (MEs), collaboration with other DEs of responsible of autonomic management of the network layer protocols in order to realize collaborative self-adaptation on both the service-layer and the network-layer.

NOTE: There are other DEs that may have not been included in the Table 3 and implementers should take them into account based on their descriptions provided in the present document. Such DEs include Network-Level-Generalized Control Plane-Management-DE (NET-LEVEL-GCP_M_DE), Function-Level-Generalized Control Plane-Management-DE (FUNC-LEVEL-GCP_M_DE), Network Level End-to-End "end-user oriented" Service and Applications Management (NET_LEVEL_E2E_Service_M).

NOTE 1: More details in ETSI TS 103 195-2 [i.2].

NOTE 2: **Autonomic management and control of IPv6 protocols**, stacks and mechanisms as so-called Managed Entities (MEs) at GANA's lowest level/layer, is based on the **assignment of specific IPv6 protocols and mechanisms to specific Decision Elements (DEs)** that autonomically manage and regulate/control the behaviour of the different MEs.

8.2.2 GANA for Access Network (Fixed Access, RAN, Other Access Networks)

Figure 23 presents GANA for the RAN as represented by C-SON and D-SON for traditional RAN, and by a combination of RAN Intelligent Controllers (RIC) and rApps/xApps and dApps in the case of the Open RAN (O-RAN) Alliance Architecture, with consideration that the GANA KPs for each network segment should be federated for E2E Federated Autonomic Management and Control (AMC).

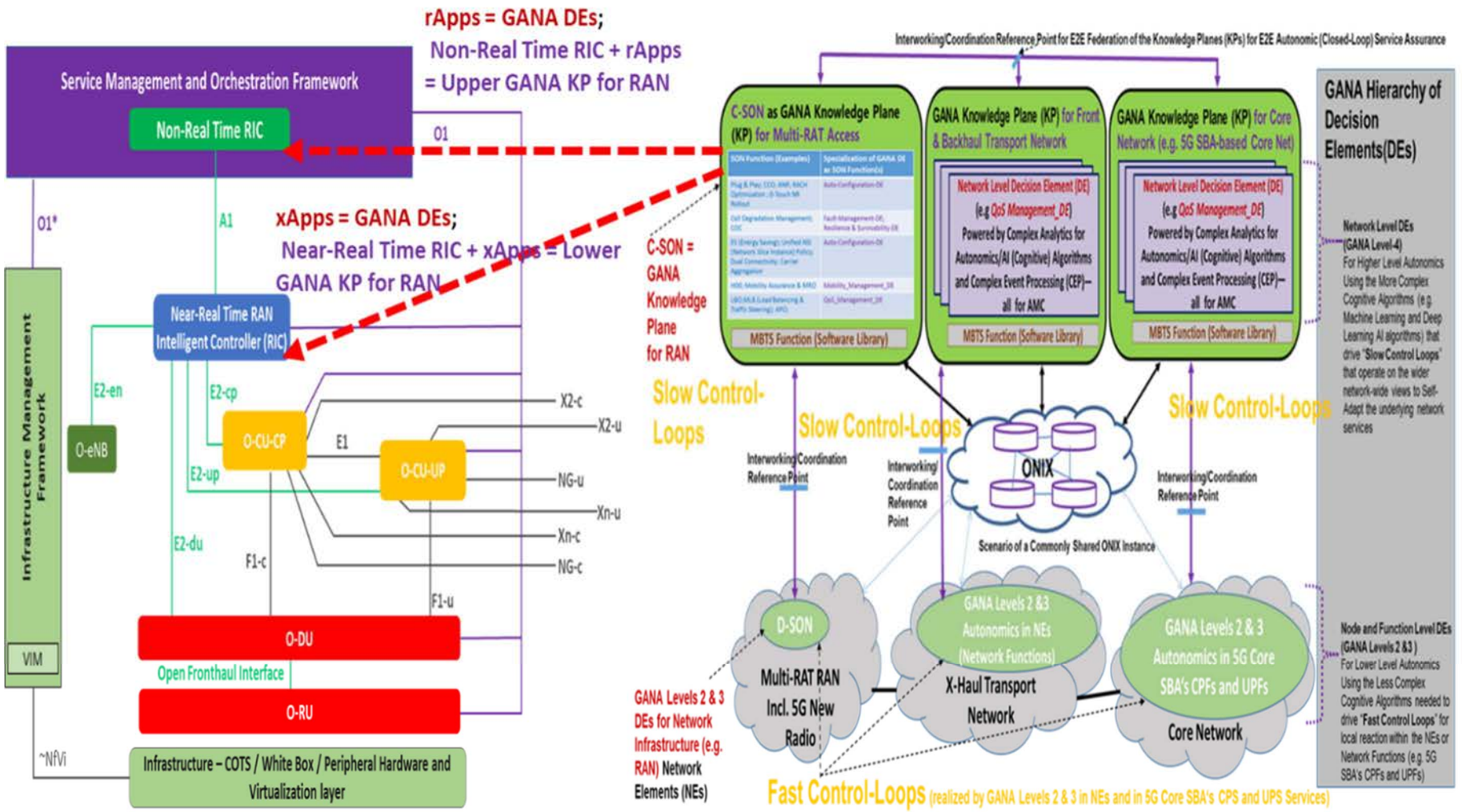


Figure 23: GANA for the RAN as represented by C-SON and D-SON for traditional RAN, and by a combination of RICs and rApps/xApps and dApps in the case of the O-RAN Alliance Architecture, with consideration that the GANA KPs for each network segment should be federated for E2E Federated AMC

KP DE (QoS DE) can be used to share QoS information across Radio, Transport, Core domains of the network to manage e2e QoS of all the network domains.

NOTE: GANA for Fixed Access is defined in ETSI TR 103 473 V1.1.2 [i.4] and BroadBand Forum (BBF) oneM2M TR-436 [i.68].

8.2.3 GANA Autonomics for Multi Layer Transport SDN Architecture

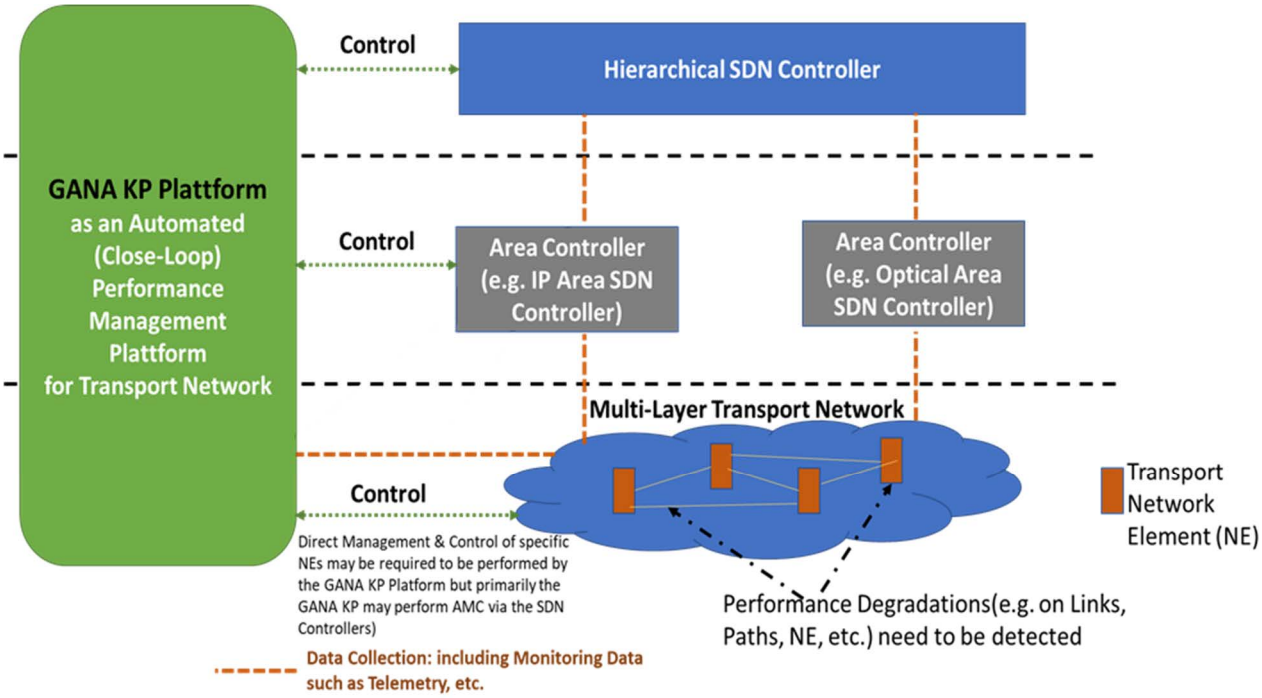


Figure 24: Integration of the GANA Knowledge Plane (KP) Platform with SDN Controllers for Multi-Layer Transport SDN Network

Figure 25 presents Integration of the GANA Knowledge Plane (KP) Platform with OSS/BSS, E2E Service Orchestrator, Domain Orchestrators, SDN Controllers for Multi-Layer Transport SDN Network, and Test Access Points (TAPs) and Switched Port Analyser (SPAN) Visibility architectures for Probing and Performance and Fault Management of the Transport Network.

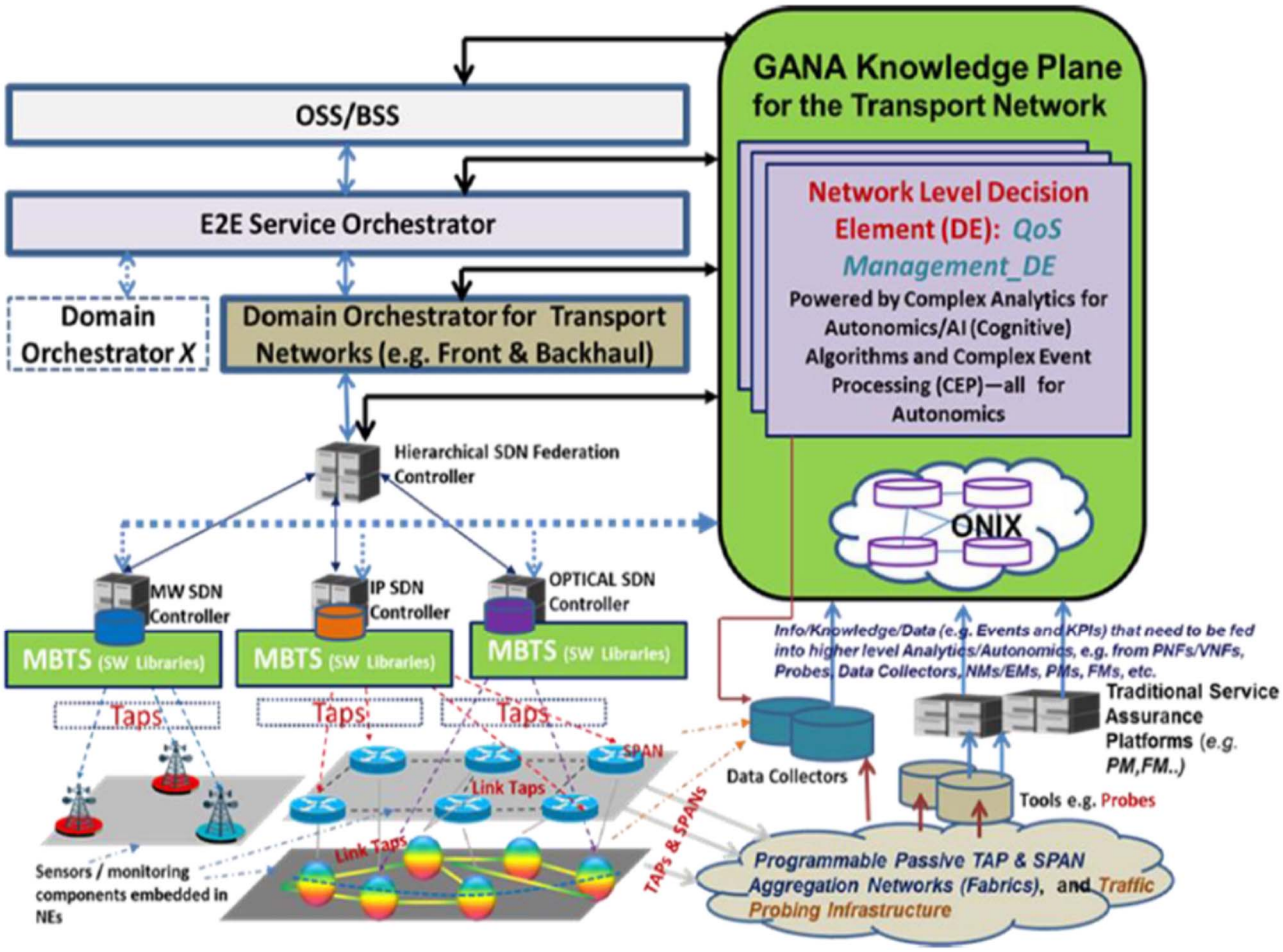


Figure 25: Integration of the GANA Knowledge Plane (KP) Platform with OSS/BSS, E2E Service Orchestrator, Domain Orchestrators, SDN Controllers for Multi-Layer Transport SDN Network, and TAP and SPAN Visibility architectures for Probing and Performance and Fault Management of the Transport Network

Figure 26 presents GANA Multi-Layer (Multi-Level) Autonomics for Multi-Layer Transport Network.

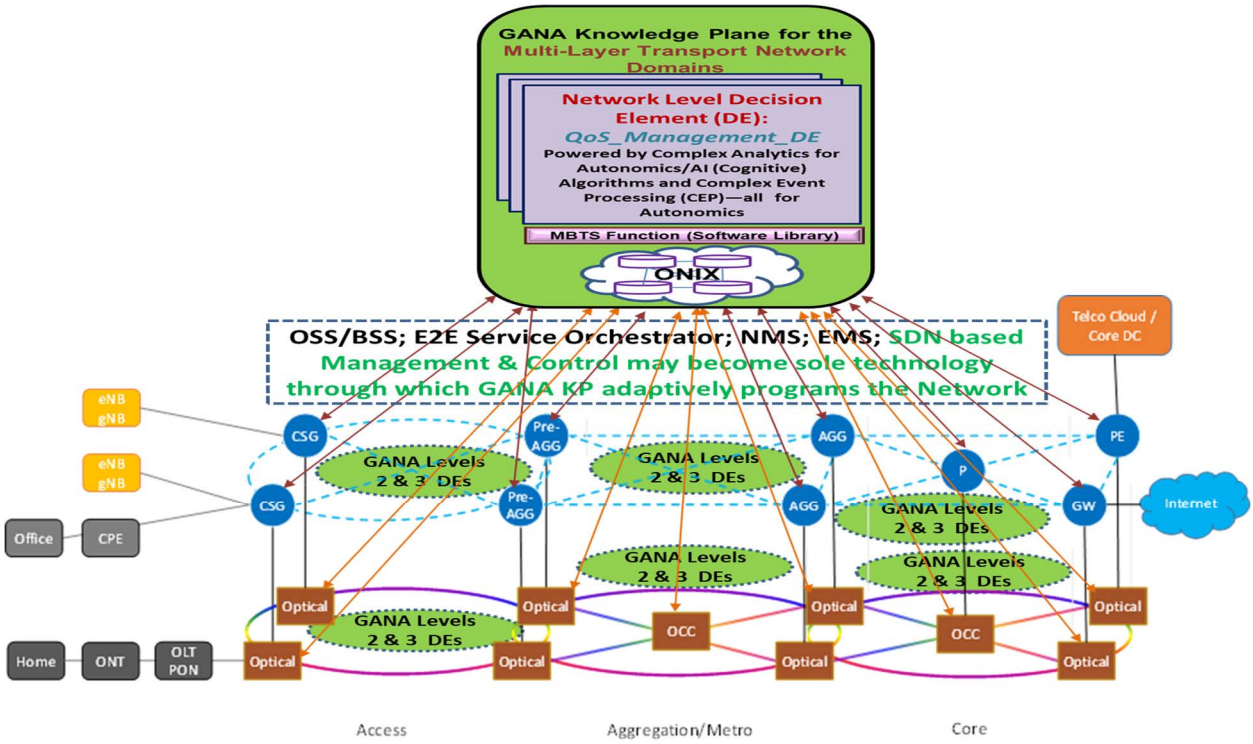


Figure 26: GANA Multi-Layer (Multi-Level) Autonomics for Multi-Layer Transport Network

8.2.4 GANA for 5G Service Based Architecture (SBA)

Regarding GANA for 5G SBA Architecture, the three levels of GANA DEs hierarchy apply, namely GANA levels 2&3 that can be introduced into Network Functions (or Services in the case of the SBA) and GANA level (network level). However, GANA Levels 2 and 3 DEs should be implemented as micro services in SBA. The GANA Knowledge Plane (KP) for the SBA should be implemented as overlay on top of the 5G SBA and made to integrate with Analytics Functions or Services as illustrated in the figure in clause 4 on "Integration of the GANA Knowledge Plane (KP) with various management and control systems through which the Knowledge Plane can selectively program the network; and KP integration with Event Sources, Data Sources and Info/Knowledge Sources". As described in clause 4.3, functions such as the Network Data Analytics Function (NWDAF) [i.8] and the Management Data Analytics Service (MDAS) [i.9] need to be integrated with KP Platform so that events and KPIs data from the functions can be used by KP DEs in their autonomic operations. DEs of the KP Platform should be implemented as micro services too.

NOTE: Figure 1 in clause 4 on GANA instantiation onto the 5G core reference architecture (ETSI TS 123 501 [i.22]) with functional distribution in a 3-levels DCs structure, offers useful insights.

8.2.5 GANA Autonomics for MEC Architecture

Figure 27 presents GANA Autonomics for MEC Architecture. It shows the GANA Levels where DEs can be introduced into the architecture.

NOTE: The lower level GANA DEs introduced in some components of the architecture may be limited to GANA Node-level DEs (GANA Level 3 DEs such as Auto-Configuration DE, Fault- Management DE, Security Management-DE, etc.).

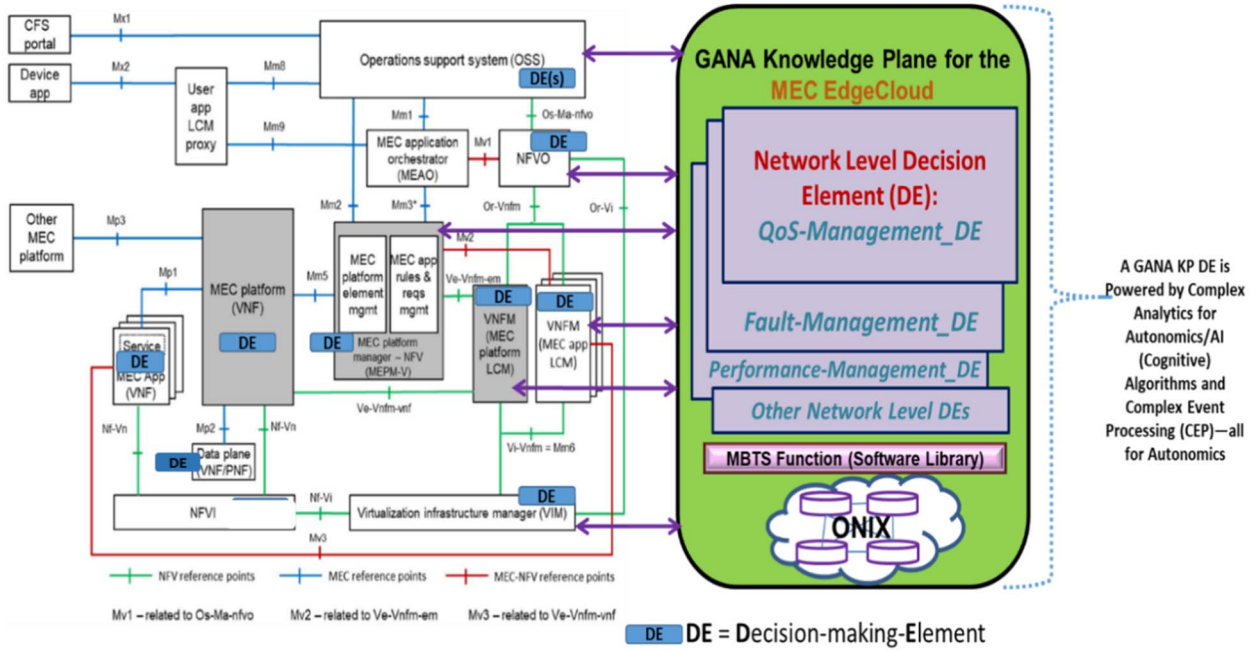


Figure 27: GANA Autonomics for MEC Architecture

9 Executing PoCs Program on the Framework for Implementing Autonomic/Autonomous IPv6 based 5G/6G Networks powered by GANA, AI, and IPv6

This clause describes the steps that should be pursued in running a Proof of Concept (PoC) on the Framework for Implementing Autonomic/Autonomous IPv6 based 5G and Beyond Networks, powered by GANA Multi-Layer AI & Multi-Layer AMC and IPv6 Capabilities. The PoC can serve the purpose of guiding the industry on how to implement the standards that underpin the PoC and provide feedback to TC INT on any implementation challenges and interoperability issues so that the feedback can be used to improve and evolve GANA related standards or to create new standards in TC INT or other Standardization Groups with competence on the related technical topics.

PoC Scope: Framework (presented by the present document) for Implementing Autonomic/Autonomous IPv6 based 5G/6G and Beyond Networks powered by ETSI GANA Multi-Layer Autonomics & Multi-Layer AI/ML-Algorithms and IPv6 Capabilities (including Segment Routing). The Reference work would be ETSI TR 103 858 (the present document):

- Objectives of a PoC (among multiple PoCs that may be targeted as deriving from the Framework that can be considered to start with), and Expected Output:

  1) Implement a part of the Framework (Guide) described by the present document (ETSI TR 103 858) on Implementing Autonomic/Autonomous IPv6 based 5G Networks, by leveraging the ETSI GANA Multi-Layer AI / Multi-Layer Autonomic Management and Control Model and IPv6 Capabilities & Extensions that enable to Build Autonomic Networks. The Framework prescribes how to introduce software components called Autonomic Functions (ETSI GANA Decision-making-Elements (DEs)), e.g. Autonomic-QoS-Management-DE, Autonomic-Security-Management-DE, etc., in the IPv6 based 5G Architecture and its associated Management and Control Architecture. The DEs and their associated Algorithms (including analytics, optimization and AI/ML algorithms) are meant to drive control-loops within Network Functions of the 5G network infrastructure and/or drive control-loops at the higher level of abstraction for self-management functionality that is positioned within the outer Management and Control realm of a 5G Network Infrastructure - within a platform called the GANA Knowledge Plane (KP) Platform. The selected part of the Framework that can be targeted by the first PoC is one that involves Adaptive Autonomic provisioning and tear-down of IPv6/SRv6 based Network Slices and Segment Routing in the SDN Programmable Multi-Layer Transport Network by the GANA Knowledge

Plane for the Multi-Layer Transport Network as illustrated in Figure 8 and NOTE: Multi-Layer aspect in transport networks usually implies IP and Optical Level.

Figure 10. The Adaptive Autonomic provisioning and tear-down of Slices is driven by various factors that include new SLAs and changes, and SLA and security assurance in the advent of challenges observed in the transport network that include faults/errors/failure manifestations, security problems and certain workload scenarios encountered, and other factors.

10 Ongoing PoCs Program on GANA in ETSI 5G PoC Implementations by the Industry

The link to the ETSI INT PoC program is the following https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.

11 Conclusion and Further Work

DE algorithms are not subject to standardization as they provide for the space for innovation and DE and Algorithm supplier differentiations. Examples of Autonomic Functions (i.e. GANA DEs) are: QoS-management-DE, Security-management-DE, Mobility-management-DE, Fault-management-DE, Resilience & Survivability-DE, Service & Application management-DE, Forwarding-management-DE, Routing-management-DE, Monitoring-management-DE, Generalized Control Plane management-DE.

Some aspects of the present document about interoperability with legacy networks and multivendor systems (e.g. European Advanced Networking Test Center (EANTC) SRv6 interoperability test [i.64]), as well as the reference points needed for new use cases such as fault, configuration and monitoring management (e.g. autodiscovery of the network) are in need for further investigation in future releases.

Annex A:
Supplementary Information

TC INT AFI WG is a standardization group that has strong competence in the area of Autonomic Management and Control (AMC) standards and has established various liaisons with various key SDOs/Fora on the subject of introducing autonomics in their network architectures in standardized way. Figure A.1 below shows the various liaisons established between TC INT AFI WG and key SDOs/Fora as shown below, and the kinds of deliverables produced as a result of the various collaborations established.

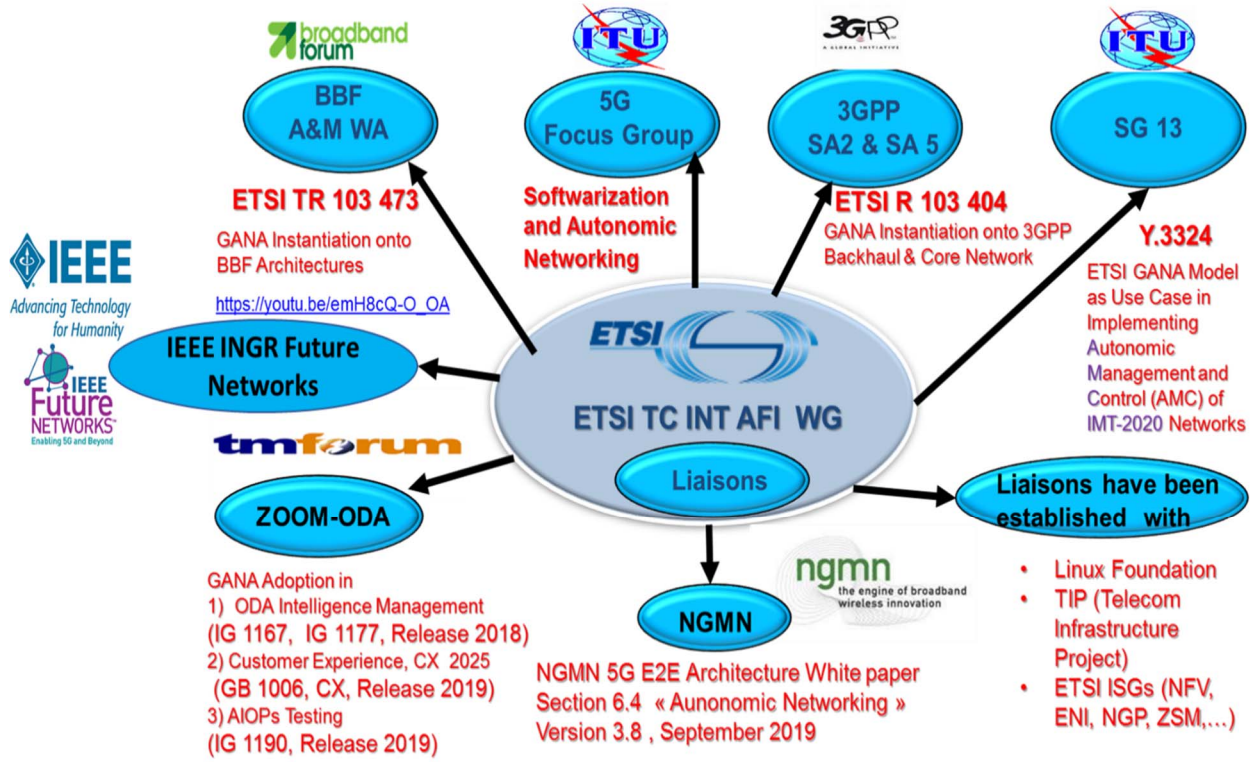


Figure A.1

As described in ETSI TS 103 195-2 [i.2] and NGMN's 5G End-to-End Architecture document [i.10], the ETSI GANA Model is a Hybrid Model for realizing the AMC paradigm and is very much compatible with and embraces the Hybrid Self-Organizing Network (SON) Model (consisting of Distributed-SON and Centralized-SON complementing each other and made to interwork together by way of C-SON policy-controlling D-SON). The GANA Model applies not only to designing and implementing AMC for Radio Access Network (RAN) but is a generic model that can be applied to other network segment types such as Cable Access, Fixed Network Access, MEC(Multi-Access Edge Computing), X-Haul Transport and Core Network as illustrated in various GANA instantiations onto target architectures such as GANA in BBF architecture scenarios (ETSI TR 103 473 [i.4]) and GANA in 3GPP Backhaul and EPC Core Network (ETSI TR 103 404 [i.5]). Recommendation ITU-T Y.3324 [i.71] also provides insights on the AMC paradigm in IMT-2020 and how to use the ETSI GANA Model to realize AMC in IMT-2020. There are other deliverables produced by INT AFI WG on the subject of introducing GANA autonomics in network architectures (including GANA implementation onto Heterogeneous Wireless Access Technologies using Cognitive Algorithms (ETSI TR 103 626 [i.66])). AFI WG work on introducing GANA autonomics in various network architectures and their associated management and control architectures continues.

Figure A.2 presents an illustration of the Interaction between a DE in the Knowledge Plane (KP) level with a DE implemented in NE/NF.

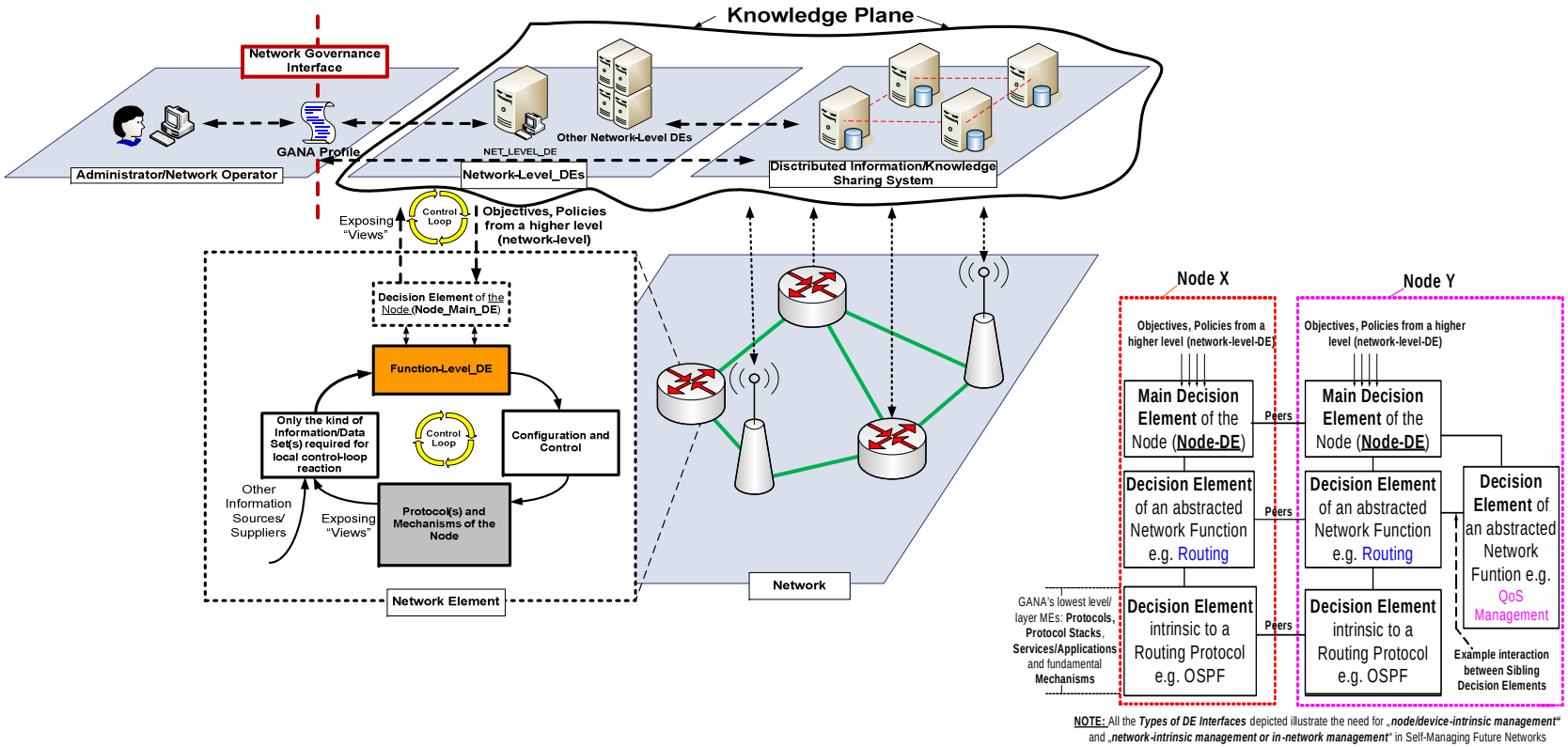


Figure A.2: Illustration of the Interaction between a DE in the Knowledge Plane (KP) level with a DE implemented in NE/NF

Figure A.3 presents an Illustration of the interworking of fast control-loop and slower control-loop for routing management (can be applied both to IPv6 and IPv4 environments).

NOTE: More details on this subject can be found in ETSI White Paper No.16 [i.1].

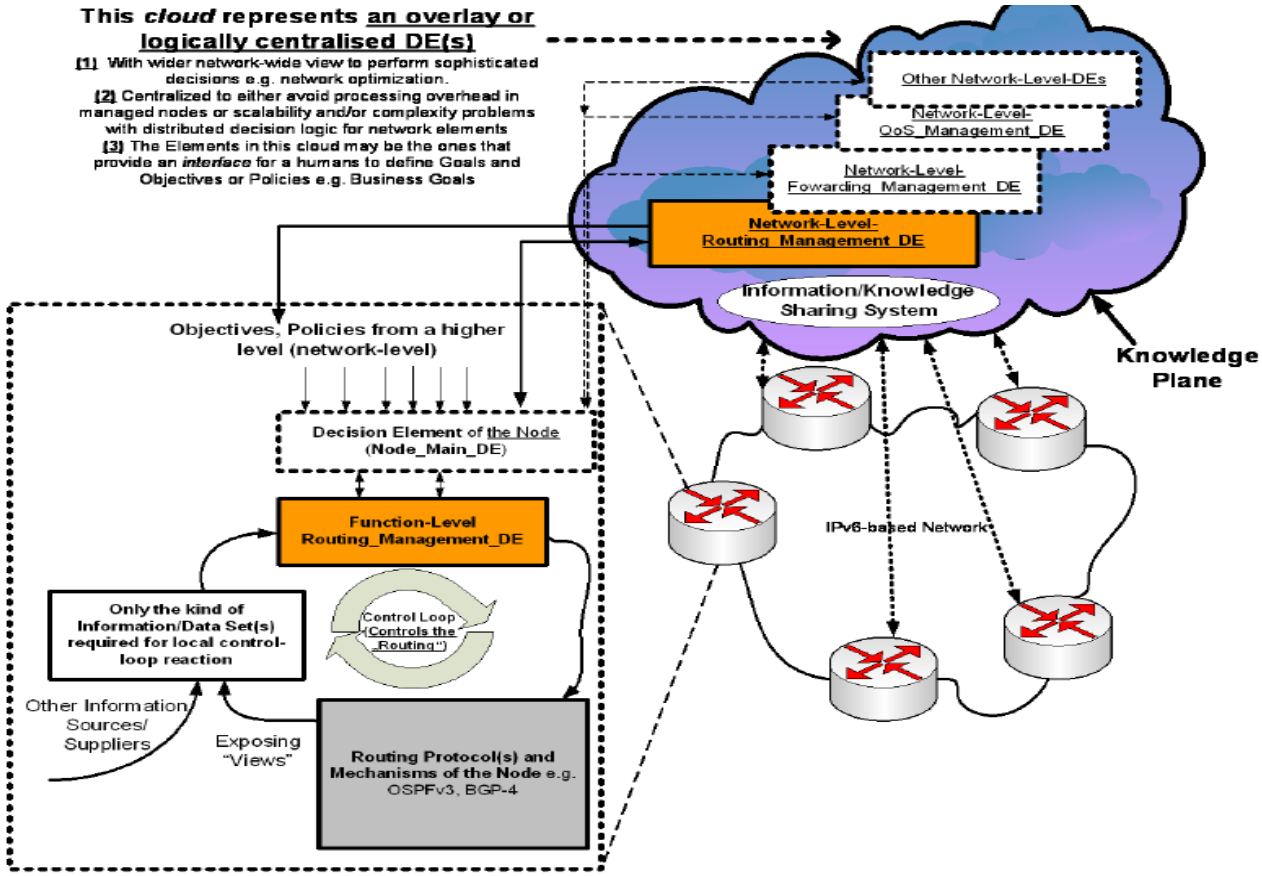


Figure A.3: Illustrating the interworking of fast control-loop and slower control-loop for routing management (can be applied both to IPv6 and IPv4 environments)

Annex B: Bibliography

- 5G security - Package 3: Mobile Edge Computing / Low Latency / Consistent User Experience: by NGMN Alliance: 20 February 2018, by NGMN 5G security group.
- IBM White paper: "An architectural blueprint for autonomic computing", MAPE-K, June 2005.
- Andrew Lerner: "AIOps Platforms", Gartner® Blog, August 2017.
- N. Miloslavskaya, A. Tolstoy: "Big Data, Fast Data and Data Lake Concepts", Elsevier Procedia Computer Science, vol. 88, pp. 300-305, October 2016.

History

Version	Date	Status
V1.1.1	March 2026	Publication