ETSI GR IPE 005 V1.1.1 (2022-05)

GROUP REPORT

IPv6 Enhanced Innovation (IPE);
5G Transport over IPv6 and SRv6

Disclaimer

The present document has been produced and approved by the IPv6 Enhanced Innovation (IPE) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGR/IPE-005

Keywords

IP, IPv6, security

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

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

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

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) IPv6 Enhanced Innovation (IPE).

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

As 5G networks are deployed worldwide, new services appear and rise new requirements on backhaul network. The main goal of the present document is to show how to implement new IPv6/SRv6 technologies to fit the requirements of the current 5G mobile networks and open opportunities to extend the backhaul features and resources to respond to further services requirements.

The present document explains how to integrate these new IPv6/SRv6 technologies and put together all technical blocks as SDN manager, OAM tools, telemetry to build a new future proof backhaul.

The present document discusses briefly the implementation constraints from a brown field installation or a green field installation. MPLS existing networks can be considered as the most common brown field installation nowadays. The present document tries to explain the gain to implement directly IPv6/SRv6 versus SR-MPLS technology.

The present document can be seen as a Best Practice Guide for implementing 5G backhaul with the newest and future proof technologies at the present time.

Introduction

The present document provides a high-level view of IPv6-based network infrastructure for delivering 5G services. The foundational technologies for such an architecture are IPv6 and SRv6.

IPv6 is not a new protocol, as its initial design dates back to the origins of the Internet. On the other hand, it has gained renewed interest lately due to several technical and regulatory reasons. From a technical standpoint, IPv6 overcomes the limitations of IPv4. In particular, it supports an address space suitable to the new applications enabled by 5G. In addition, the IETF has stated they will not support any longer the protocol evolution of IPv4. Several countries have also issued national strategic projects for the evolution of public networks mandating the usage of IPv6.

Segment Routing (SR) is a much newer technology developed to enable better control over the steering of IP packets across the network data plane. The instance of SR considered in the present document is SRv6, meaning that the SR mechanisms are activated over an IPv6 data plane. Through SRv6, applications such as network slicing and resource-based traffic steering can be realized.

The present document is structured to articulate the description of a 5G backhaul and transport network architecture using both IPv6 and SRv6. Clause 4 will provide an overview of 5G and its characteristics. Clause 5 will discuss the main network requirements and the base technologies adopted in the network architecture. Clause 6 will dig into the network architecture, providing the details of IPv6 and SRv6. Clause 7 will extend the discussion providing a view on how the backhaul and transport network interacts with the cloud.

1 Scope

The present document discusses implementing 5G Backhaul based on IPv6/SRv6 technologies.

Implementation investigation is split into four major blocks:

- 5G network and services requirements
- Backhaul network pre-requisites
- IPv6/SRv6 backhaul network implementation
- 5G and Cloud interactions

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

[i.1] Recommendation ITU M.2410-0: "Minimum requirements related to technical performance for IMT-2020 radio interface(s)".

[i.2] IETF RFC 8200: "Internet Protocol, Version 6 (IPv6) Specification".

[i.3] IETF RFC 791: "Internet Protocol".

[i.4] RIPE NCC: "Create an Addressing Plan".

NOTE: Available at https://www.ripe.net/publications/ipv6-info-centre/deployment-planning/create-an-addressing-plan.

[i.5] IETF RFC 4364: "BGP/MPLS IP Virtual Private Networks (VPNs)".

[i.6] IETF RFC 7432: "BGP MPLS-Based Ethernet VPN".

[i.7] IETF RFC 4664: "Framework for Layer 2 Virtual Private Networks (L2VPNs)".

[i.8] IETF RFC 4761: "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling".

[i.9] IETF RFC 4762: "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling".

[i.10] IETF RFC 8402: "Segment Routing Architecture".

[i.11] IETF RFC 8986: "Segment Routing over IPv6 (SRv6) Network Programming".

[i.12] IETF draft-ietf-teas-ietf-network-slices: "Framework for IETF Network Slices".

[i.13] IETF draft-ietf-spring-sr-for-enhanced-vpn: "Segment Routing based Virtual Transport Network (VTN) for Enhanced VPN".

[i.14] IETF draft-dong-lsr-sr-enhanced-vpn: "IGP Extensions for Scalable Segment Routing based Enhanced VPN".

[i.15] IETF RFC 5120: "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)".

[i.16] IETF RFC 4915: "Multi-Topology (MT) Routing in OSPF".

[i.17] Recommendation ITU-T Y.1731: "OAM functions and mechanisms for Ethernet based networks".

[i.18] IETF RFC 5880: "Bidirectional Forwarding Detection (BFD)".

[i.19] IETF RFC 5881: "Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)".

[i.20] IETF RFC 7880: "Seamless Bidirectional Forwarding Detection (S-BFD)".

[i.21] IETF RFC 5357: "Two-Way Active Measurement Protocol (TWAMP)".

[i.22] IETF draft-ietf-6man-spring-srv6-oam-11: "Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Data plane (SRv6)".

[i.23] IETF draft-ietf-rtgwg-segment-routing-ti-lfa: "Topology Independent Fast Reroute using Segment Routing".

[i.24] IETF RFC 9087: "Segment Routing Centralized BGP Egress Peer Engineering".

[i.25] IETF draft-ietf-pce-segment-routing-ipv6: "PCEP Extensions for Segment Routing leveraging the IPv6 data plane".

[i.26] IETF RFC 8365: "A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)".

[i.27] IETF RFC 7752: "North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP".

[i.28] IETF RFC 8571: "BGP - Link State (BGP-LS) Advertisement of IGP Traffic Engineering Performance Metric Extensions".

[i.29] IETF draft-ietf-idr-segment-routing-te-policy-13: "Advertising Segment Routing Policies in BGP".

[i.30] IEEE 1588-2019™: "IEEE Standard for a Precision Clock Synchronisation Protocol for Networked Measurement and Control Systems".

[i.31] Recommendation ITU-T G.8275.1: "Precision time protocol telecom profile for phase/time synchronisation with full timing support from the network".

[i.32] IETF RFC 8754: "IPv6 Segment Routing Header (SRH)".

[i.33] ETSI White Paper No. 35: "IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward".

[i.34] ETSI TS 123 501: "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501)".

[i.35] IETF draft-ietf-v6ops-ipv6-deployment: "IPv6 Deployment Status".

[i.36] IETF RFC 6877: "464XLAT: Combination of Stateful and Stateless Translation".

[i.37] IETF draft-ietf-lsr-isis-srv6-extensions: "IS-IS Extensions to Support Segment Routing over IPv6 Dataplane".

[i.38] IETF RFC 4271: "A Border Gateway Protocol 4 (BGP-4)".

[i.39] ETSI TS 133 501: "5G; Security architecture and procedures for 5G System (3GPP TS 33.501)".

[i.40] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

[i.41] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[i.42] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[i.43] IETF RFC 4213: "Basic Transition Mechanisms for IPv6 Hosts and Routers".

[i.44] IETF RFC 4291: "IP Version 6 Addressing Architecture".

[i.45] IETF RFC 6164: "Using 127-Bit IPv6 Prefixes on Inter-Router Links".

[i.46] IETF RFC 8415: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[i.47] IETF RFC 3596: "DNS Extensions to Support IP Version 6".

[i.48] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[i.49] IETF draft-matsushima-spring-srv6-deployment-status: "SRv6 Implementation and Deployment Status".

[i.50] IETF RFC 6241: "Network Configuration Protocol (NETCONF)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

binding Segment IDentifier (SID): type of label introduced in Segment Routing

control plane: part of the router architecture that is concerned with drawing the network topology or the information in a routing table that defines what to do with incoming packets

data plane: part of the networking node that processes the data requests

Evolved Node B (eNodeB): element in E-UTRA of LTE, radio base station that supports LTE technology

Quality of Experience (QoE): measure of the delight or annoyance of a customer's experiences with a service

Quality of Service (QoS): description or measurement of the overall performance of a service

Segment Routing (SR): steering packets through an ordered list of instructions to realizes end-to-end policy without creating any per-flow state in the network

telemetry: in-situ collection of measurements or other data at remote points and their automatic transmission to receiving equipment (telecommunication) for monitoring

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
4G	The fourth generation technology standard for broadband cellular networks

5G	The fifth generation technology standard for broadband cellular networks
5GC	5G Core
5QI	5G QoS Identifier
AF	Assured Forwarding
AI	Artificial Intelligence
AMF	Access and Mobility Function
AN	Access Network
AR	Address Resolution
AS	Autonomous System
ASN	Autonomous System Number
BGP	Border Gateway Protocol
CIR	Committed Information Rate
DC	Data Centre
DHCP	Dynamic Host Control Protocol
DN	Data Network
DNS	Domain Name System
DoS	Denial of Service
DSCP	Differentiated Services Code Point
EF	Expedited Forwarding
eMBB	Enhanced Mobile Broadband
FCAPS	Fault, Configuration, Accounting, Performance and Security
FW	Firewall
HMTC	High-Performance Machine-Type Communications
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IoT	Internet of Things
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
mMTC	massive Machine Type Communications
NF	Network Functions
NMS	Network Management Systems
NRF	Network Repository Function
NSSAI	Network Slice Selection Assistance Information
O&M	Operations and Maintenance
OSPF	Open Shortest Path First
PCF	Policy and Charging Function
PDU	Protocol Data Unit
PIR	Peak Information Rate
QFI	QoS Flow ID
QoS	Quality of Service
RAN	Radio Access Network
SD	Slice Differentiator
SDN	Software Defined Networking
SEG	Security Gateway
SID	Segment Identifier
SLA	Service Level Agreement
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SR	Segment Routing
SRH	Segment Routing Header
SR-MPLS	Segment Routing - Multi Protocol Label Switching
SRv6	Segment Routing version 6
SST	Slice Service Type
TC	Traffic Class
TTM	Time to Market
UE	User Equipment
UPF	User Plan Function
URLLC	Ultra Reliable Low Latency Communications
V2X	Vehicle to Anything
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding

VTN	Virtual Transport Networks
WFQ	Weighted Fair Queuing

4 5G Overview and Requirements

4.1 5G Overview

5G Networks is a reality today as most European operators have already started the deployment of the 5G infrastructure. At the moment (2021), the operators focus their efforts on providing eMBB services and reusing or enhancing 4G infrastructure as possible to optimize their deployment cost.

To provide new eMBB services with high or better user experience, operators need to upgrade the backhaul infrastructure to increase bandwidth capacities.

5G roadmap deals with new enhanced services, which will be implemented little by little as the footprint and capabilities of 5G infrastructure will permit it. To implement new URRLC services that require low latency between source and end-user devices, and operators need to deploy a new enhanced clock distribution system.

4.2 5G Services Requirements

5G brings different families of services: Enhanced Mobile Broadband services (i.e. eMBB), IoT services, Ultra-Reliable and Low Latency Communications services (i.e. URLLC), High Requirements Private Networks services.

Enhanced Mobile Broadband (eMBB) service: eMBB service enhances the current 4G Internet Access. The goal is to use the new better bandwidth of 10 Gbps - 20 Gbps of the 5G Base Station to offer the end-user a better quality of experience. The target is to provide a 200 Mbps - 1 000 Mbps data rate for the user and a 4 ms one-way latency. The applications are 4K live streams, real-time gaming sessions, and Virtual Reality (VR) or Augmented Reality (AR) applications.

IoT service addresses massive Machine-Type Communications (mMTC) usage, targeting a high density of devices and connections. 5G capability expectation is 1 million connections per square kilometre. The applications are smart networks of connected devices for metering earth quake or temperature.

Ultra-Reliable and Low Latency Communications (URLLC) service focuses on high reliability, high availability, and low latency usage. According to Recommendation ITU M.2410-0 [i.1], the minimum requirement for one-way latency in the user plane is 1 ms, while control plane latency is 20 ms, and the minimum requirement for reliability is 99,999 %. The applications are Robotic networks or Smart Automated and Communicating Cars.

High Requirements Private Networks service: This service addresses the ability of 5G technologies to build dedicated and private networks with high requirements. The applications are Company Campus or Public Transportation.

4.3 Matrix of Requirements

Service Type	User Plane one way Latency	Control Plane Latency	Data Rate User Experience	Reliability	Clock Accuracy
eMBB	4 ms	20 ms	1 Gbps	99,99 %	1,5 µs
mMTC	4 ms	20 ms	Few Mbps	99,99 %	1,5 µs
URLLC	1 ms	20 ms	Few Mbps	99,999 %	350 ns
Private Networks	4 ms	20 ms	1 Gbps	99,99 %	1,5 µs

4.4 Quality of Service Requirements

Each type of service in the 5G Network receives an SLA and an associated QoS of service class. This class of service will be used further in the backhaul for committing the end-to-end SLA. In the Ethernet and IP world, the fields Dot1p and DSCP and the VLAN id are used for mapping the service class of service within the slice context.

4.5 Slicing Overview

The slicing feature is the ability of the 5G network to provide a dedicated context of resources and SLA for a specific application such as gaming, high-speed internet browsing or card assistance. The slice context of 5G has to be propagated to the backhaul network. This will be discussed in a further clause.

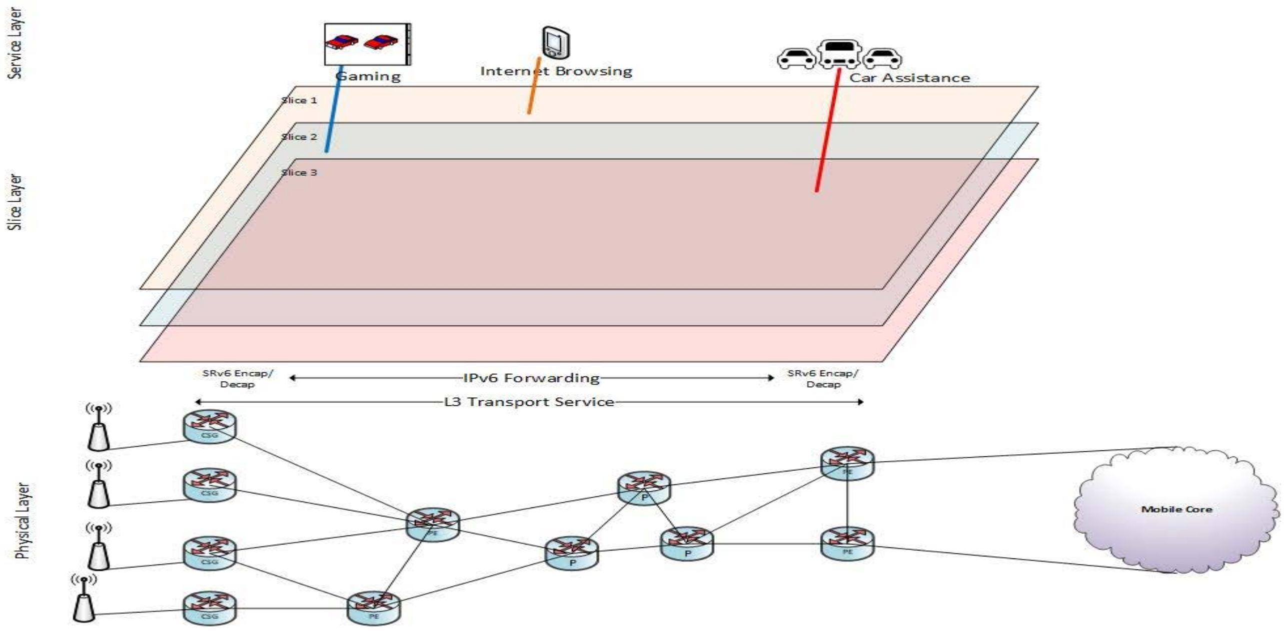


Figure 1: High-level slicing architecture

4.6 Security Overview

As in previous telecom networks, 5G network needs exchange points with other operators for roaming purposes. Then standard security concepts and guidance can be applied.

The newness in the 5G infrastructure is about the end-to-end encryption of data between Mobile Station Baseband and the Mobile Core infrastructure. To achieve this goal, a new IPSec Gateway is integrated into the backhaul infrastructure located in the Data Center border; Data Center is located the Mobile Core.

4.7 Clock Distribution Overview

5G Time Synchronization requirements depend on the applications: Basic Service as eMBB requires < ±1,5 µs of time accuracy compared to URLLC Service requires < ±350 ns of time accuracy end to end.

GPS and Caesium ground sources are the two types of clock sources. Even GPS time (< ±100 ns) is more accurate than Ground time (< ±350 ns by network build). The recommendation is to use a mix of both technologies to enforce the reliability of the clock distribution and follow the rules for the main parameters:

- Accuracy: GPS < ±100 ns, Ground < ±350 ns (By network build)
- Availability: High with multiple sources and physical medium (air + ground)
- Footprint: GPS fully or partially deployed on station site for cost efficiency. Ground fully deployed

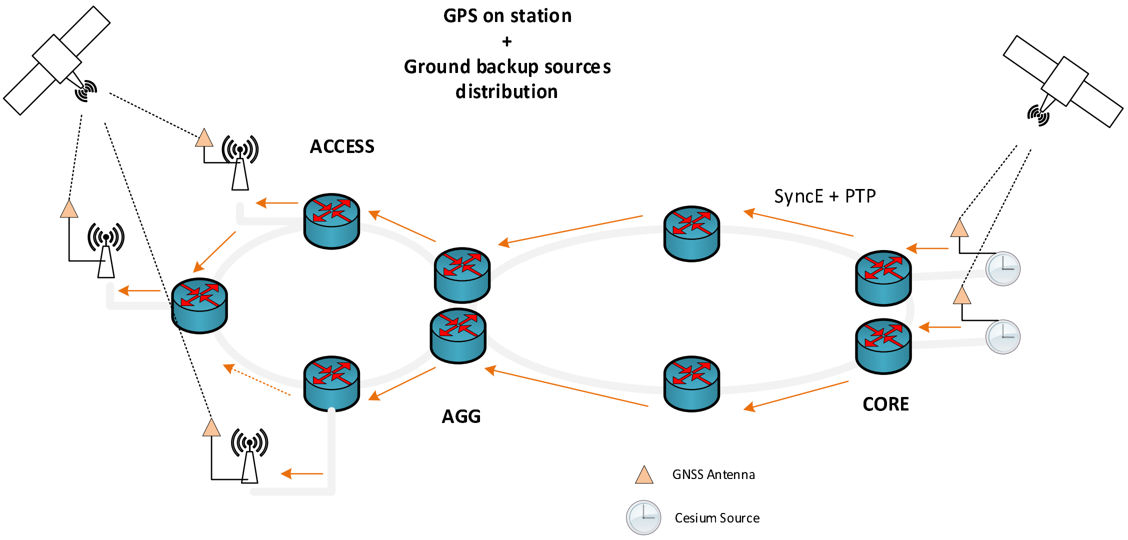


Figure 2: 5G clock distribution

5 Networking Pre-Requisites

5.0 Introduction

The scope of this clause is to introduce the most relevant pre-requisites of a 5G network at the networking layer.

The underlying assumption is that IPv6 is employed at both the service and network layers.

Specifically, the service layer, referred to as "overlay", allows an application on the user terminal to connect to a service (e.g. a Virtual Machine in the cloud, a stand-alone application on a server, etc.). An IPv6 overlaid connection is either natively carried over an IPv6 network or handled by transition/translation mechanisms for transport over an IPv4 network. This has been extensively discussed in ETSI White Paper No. 35 [i.33], and the main concepts are summarized in clause 5.7.

Most of this chapter focuses on technologies applicable to the network layer, also named "underlay". For the scope of the discussion, underlay is considered IPv6-capable, no matter whether the network is IPv6-only or Dual-Stack enabled.

The next clauses will provide a functional description of the technologies considered as networking pre-requisites. The architectural description of a 5G network, encompassing all the elements just described here, will be provided in clause 6.

5.1 Required Protocols

Internet Protocol version 6 (IPv6) [i.2] is the foundational protocol of the architecture under discussion throughout the present document. IPv6 was designed by the Internet Engineering Task Force (IETF) to overcome the limitations of Internet Protocol version 4 (IPv4) [i.3]. A discussion of the differences between the two protocols can be found, as an example, in [i.33]. [i.35] also discusses the possible steps to migrate a network to IPv6-only. In particular, [i.35] discusses how to support the transition of the carriers' networks to IPv6 through the adoption of IPv6-only overlay services based on translation mechanisms such as 464XLAT [i.36], handling the residual IPv4 traffic as a service (IPv4aaS).

Segment Routing version 6 (SRv6) [i.10] is the flavour of SR that leverages IPv6 on the data plane. SR provides control over the forwarding paths by combining simple network instructions. As a precondition to run SRv6, the IGP protocols active on the network control plane need to support the necessary extensions to encode the Segment Identifiers (SID) and their behaviours, as explained in clause 5.2.

The IPv6 control plane is based on the same protocols used in an IPv4 network. Either Intermediate System to Intermediate System (IS-IS) [i.15] or Open Shortest Path First (OSPF) [i.16] can be used as the IGP to propagate routing updates within the network domain. If IS-IS is considered, also [i.37] applies. In contrast, Border Gateway Protocol (BGP) [i.38] takes care of exchanging routing information across multiple domains. For either IS-IS or OSPF, it is required to run their multi-topology extension to support virtualised topologies. This will be further detailed in clause 5.3 to support network slicing.

In clause 6 more information will be given on how to apply the protocols just described here. More will also be provided about the protocols used on the management plane.

5.2 SRv6 Concepts and Common Foundations

Segment Routing (SR) is introduced in IETF RFC 8402 [i.10] to enable source routing. A network ingress node may steer a packet across an ordered list of instructions, called "segments", sometimes also referred to as "policies". A segment can represent any topological or service-related instruction. An example of topological instruction is "steer packet to a destination using the path that minimizes latency". An example of service-related instruction is "process packet with a certain QoS treatment".

The network ingress node is the only one that maintains a per-flow state. In contrast, the other nodes limit their activity to per-flow explicit routing (according to the instruction associated with the received packet).

SR can be applied to an already existing MPLS architecture without changing the forwarding plane. This SR variant is named SR-MPLS. A segment is encoded as an MPLS label, while an ordered list of segments is encoded as a stack of labels. Instead, when SR is enabled on IPv6 architecture, it is named SRv6.

The decision of whether to enable SR-MPLS or SRv6 in a network depends on factors and criteria specific to an operator (more on this in clause 5.8). These particular arguments are out of the scope of the present document, which instead focuses on SRv6.

In such case, a new IPv6 routing header is used (Segment Routing Header, or SRH). A segment is encoded as an IPv6 address, so that an ordered list of segments is encoded as an ordered list of IPv6 addresses in SRH [i.32].

While for SR-MPLS, the active segment is the top label in a stack, in SRv6, the active segment is indicated by the packet's Destination Address (DA). A pointer indicates the next active segment in SRH. The full list of ordered segments is obtained by visiting all the addresses stored in SRH.

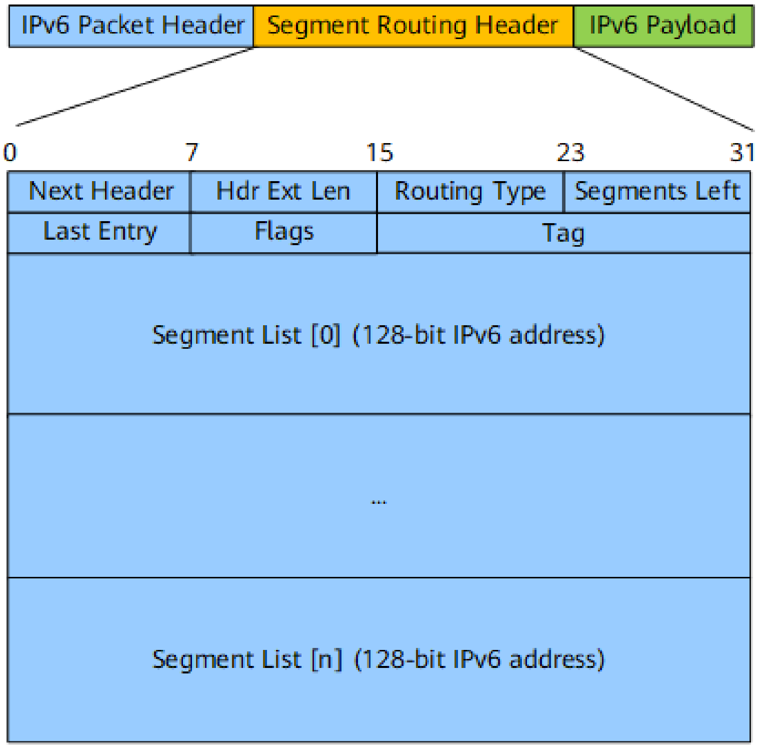


Figure 3: SRv6 SRH

IETF RFC 8986 [i.11] defines the SRv6 Network Programming concepts, extending the base SRv6 behaviour.

An ingress node keeps on steering packets through the ordered list of segments. Each of these instructions represents a function to be called at a specific location in the network. A function is locally defined on the node where it is executed and may range from simply moving forward in the segment list to any complex user-defined behaviour.

SRv6 network programming combines segment routing functions that combine packet routing and packet processing.

The overall forwarding process of SRv6 is shown in Figure 4, where a SRv6 path composed of five nodes is represented. The source node is located on the left hand side and the steering follows the arrow until packets reach the destination node on the right.

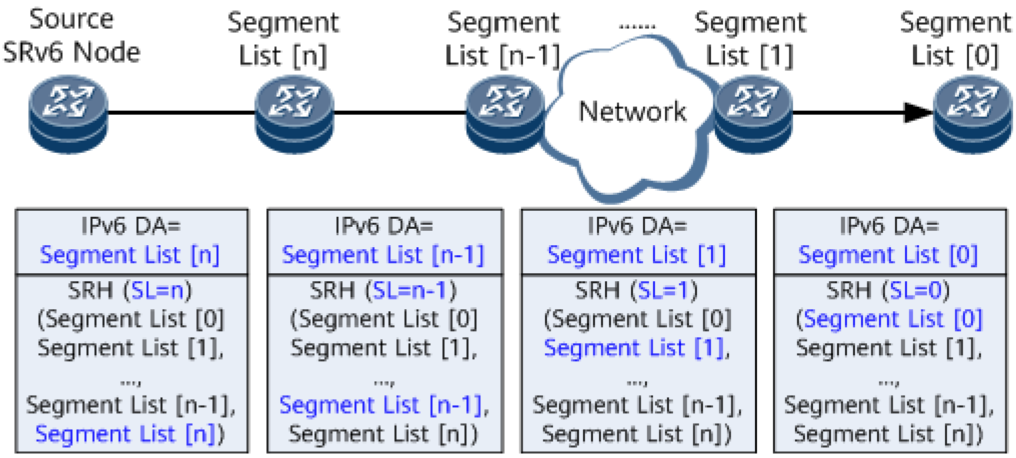

Source SRv6 Node
Segment List [n]
Segment List [n-1]
......
Segment List [1]
Segment List [0]
Network
IPv6 DA= Segment List [n]
SRH (SL=n) (Segment List [0] Segment List [1], ..., Segment List [n-1], Segment List [n])
IPv6 DA= Segment List [n-1]
SRH (SL=n-1) (Segment List [0] Segment List [1], ..., Segment List [n-1], Segment List [n])
IPv6 DA= Segment List [1]
SRH (SL=1) (Segment List [0] Segment List [1], ..., Segment List [n-1], Segment List [n])
IPv6 DA= Segment List [0]
SRH (SL=0) (Segment List [0] Segment List [1], ..., Segment List [n-1], Segment List [n])

Figure 4: SRv6 steering process

The segment list (SID list) imposed by the source node contains the identifiers of the segments to be visited along the path, stored in the SRH. The depth of the list is n (in our case n = 4). This is also indicated by the Segment List (SL) counter, located in the SRH. The IPv6 destination address contains the ID of the next node to be visited, in this case n. Each node crossed decrements the SL counter until SL = 0, and copies the ID of the next node into the destination address of the packet.

IGP protocols and BGP carry and propagate the SRv6 SID information in a distributed model. Since SRv6 complies with the SDN architecture, it is expected that the centralized model will be often adopted. The centralized controller performs the function of computing the requested paths, assigning the SIDs and push the SID list to the ingress node. This way, the ingress node just adds an SRH to each IPv6 packet without extra processing.

5.3 Slicing over SRv6

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.

3GPP defined network slicing as a critical 5G Core (5GC) feature in ETSI TS 123 501 [i.34]. 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.

Each slice may serve a particular service type, set of applications or group of customers, each with an agreed upon Service Level Agreement (SLA).

Network Slices are identified through the Single Network Slice Selection Assistance Information (S-NSSAI). A UE signals to the network S-NSSAI wishes to connect to through the NSSAI (Network Slice Selection Assistance Information). NSSAI is carried in the signalling messages exchanged between the UE and the 5GC.

An S-NSSAI is comprised of a few parameters:

- A Slice/Service Type (SST), which refers to the expected Network Slice behaviour in terms of features and services.
- A Slice Differentiator (SD) is an optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices of the same Slice/Service type.

SST has been standardized for five major classes of applications, according to the latest version of ETSI TS 123 501 [i.34], defining the basic behaviour and characteristics of a slice carrying that type of application. Table 1 shows the SST currently defined (it is taken from clause 5.15.2.2 of [i.34]).

Table 1: SST defined by 3GPP (ETSI TS 123 501)

Slice/Service type	SST value	Characteristics
eMBB	1	Slice suitable for the handling of 5G enhanced Mobile Broadband.
URLLC	2	Slice suitable for the handling of ultra- reliable low latency communications.
MIoT	3	Slice suitable for the handling of massive IoT.
V2X	4	Slice suitable for the handling of V2X services.
HMTC	5	Slice suitable for the handling of High-Performance Machine-Type Communications.

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 represented in Figure 5, which shows two different slices (both Red and Green).

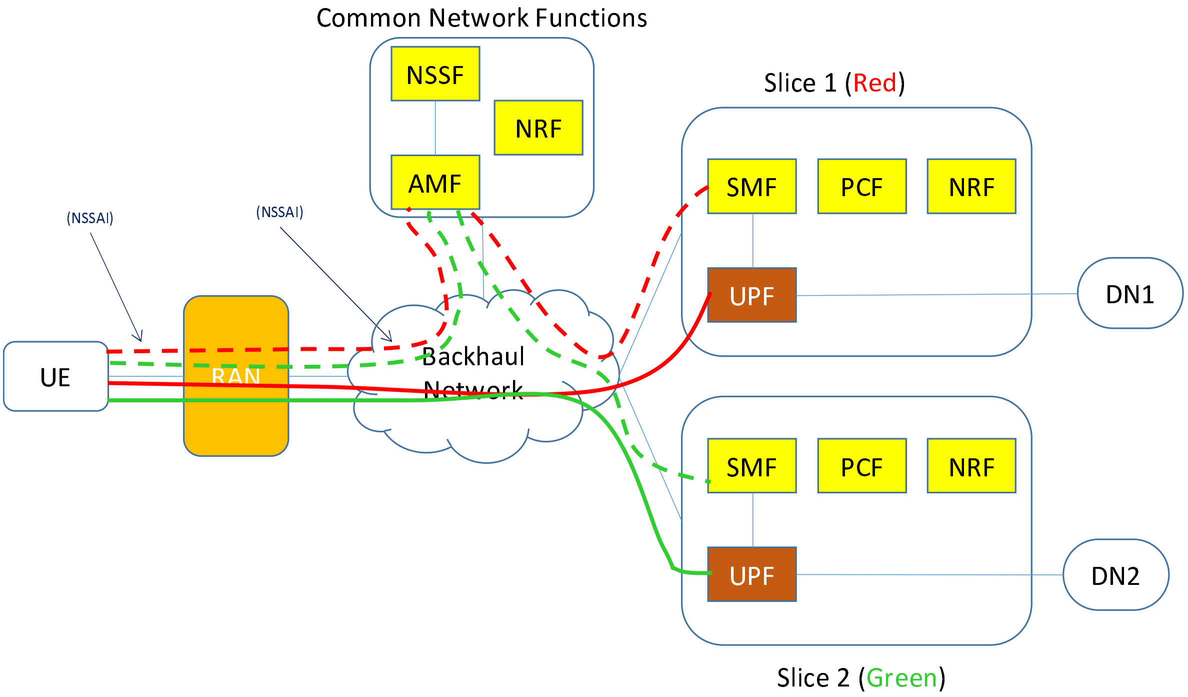


Figure 5: Network slicing high-level architecture

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 interact with the Network Slice Selection Function (NSSF) to select the appropriate Network Slice instance (e.g. based on Allowed S-NSSAIs).

A Protocol Data Unit (PDU) session is associated with one S-NSSAI and one DN (Data Network). The AMF discovers candidate Session Management Functions (SMF) using multiple parameters, including the S-NSSAI provided in the UE request and selects the appropriate SMF. The SMF performs the selection of the User Plane Function (UPF) and uses the S-NSSAI. The Network Repository Function (NRF) is used to discover the required Network Functions (NF) using the selected network slice instance. The data transmission occurs after a PDU to a Data Network session is established in a network slice. The S-NSSAI associated with a PDU session is provided to the Policy and Charging Function (PCF), to apply slice specific policies.

In the IPv6-based 5G transport network, SRv6 programmability is essential to support 5G network slicing. The IPv6 data plane still uses both IGP and BGP protocols to carry the routing and reachability information of the network nodes. The only extension requested is the support of multi-topology in [i.15] and [i.16]. In addition, SRv6 network programming [i.11] enables network slicing support through fine-graned packet handling and steering.

From the network's perspective, the concept of slicing is discussed in [i.12]. There, "network slicing" is analysed within the context of IETF. [i.12] 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.

A way to implement an "IETF Network Slice" over SRv6 is explained in [i.13] through the Enhanced VPN (VPN+) construct. A segment can further be associated with network resources used to execute the instruction. Such a segment is called a resource-aware segment. Resource-aware Segment Identifiers (SIDs) may be used to build SRv6 paths with a set of reserved network resources. A group of resource-aware SIDs may be used to build SRv6-based virtual underlay networks with customized network topology, and resource attributes required by one or a group of either or both customers and services. Such virtual networks are the SR instantiations of Virtual Transport Networks (VTNs).

It is expected that different SRv6 SIDs represent network resources allocated on each segment for different network slices on the data plane. In simple terms, each node receives as many SIDs as the slices it is part of. Each SID has a locator that is dedicated to a specific slice.

The technical implementation of this architecture is detailed in clause 6 and, more specifically, in clause 6.2.6.

5.4 Security Overview

3GPP has recommended the use of Security Gateways (SEG) to secure the RAN to 5GC communications, ensuring service continuity and confidentially, see [i.39] and [i.40]. SEGs relies on IPSec [i.41] and key exchange or certificate management capabilities [i.48] to provide access control through authentication and traffic confidentiality and integrity through encryption.

The outcome is securing the transport of N2 and N3 interfaces from a gNB and 5GC. The same mechanisms are also adopted to secure the Xn interface.

The high-level representation of the security architecture for 5G is shown in Figure 6.

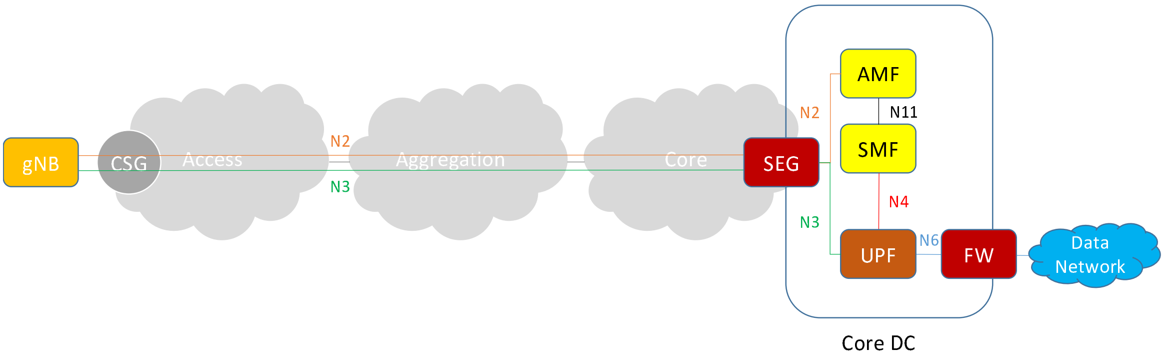


Figure 6: 5G security architecture

For simplicity, in Figure 6 a single, centralized SEG deployed in front of 5GC is considered. IPsec connectivity is granted between gNB and SEG. Even if Figure 6 shows just the N2 N3 interfaces, all traffic directed to/from the gNB may be encapsulated, including OAM.

Figure 6 also assumes that all core functions are located in a single DC. As discussed in the previous clauses, the diversified requirements posed by the 5G classes of applications may bring to deploy part of those functions in locations closer to the access. For example, URRLC applications may be located in Edge DC. In this case, the SEG may also be deployed in front of those functions to support the same security requirements.

The connectivity from UPF to external data networks, such as the Internet, may be subject to potential threats. Figure 6 above also shows the presence of a Firewall (FW) function, which implements N6 security. This may include mechanisms to prevent Denial-of-Service (DoS) or support Intrusion Detection/Prevention and other mitigation techniques. This function may be distributed across the network, depending on where the points of external connectivity are located.

5.5 SDN Platform and Automation

Network Management Systems (NMS) have progressively incorporated functions beyond traditional management processes usually known as Fault, Configuration, Accounting, Performance and Security (FCAPS). Examples of these new functions are the handling of the network control plane and the capability of analysing the data collected through network telemetry.

In the context of a 5G network where IPv6 and SRv6 are used to transport services that pose differentiated requirements on the network, often specific to an application, a tenant or a group of customers, the automation of network processes becomes of paramount importance.

Software Defined Networking (SDN) platforms are seen as the proper framework to deal with such requirements and cope with the dynamic changes requested to the network infrastructure, particularly the support of network slicing and the relevant virtualisation of the physical network resources.

SDN systems implement proactive O&M of physical networks and intent-driven service automation. Also, they achieve real-time awareness of the network status and perform predictive maintenance. Apart from making the network management more efficient, they enable faster Time to Market (TTM), accelerating the introduction of new network services and supporting enhanced service transformation and innovation.

SDN systems typically provide a few major functions, here just summarized:

- Full Lifecycle Automation. The manual operations, e.g. configuration delivery, test and upgrade, are replaced with automated processes. O&M current operation model changes from "In the Loop" (manual intervention in a process) to "On the Loop" (designing and managing a process, using rules, policies, and procedures). This greatly improves work efficiency in addressing the heavy maintenance workload caused by massive connections and large-scale networks imposed by 5G. The time required for network construction and service provision is significantly reduced.

- Proactive maintenance. Passive O&M, triggered by customer complaints and performs troubleshooting within days, transforms into proactive O&M completed in minutes. In proactive O&M mode, predictive maintenance is conducted using an in-depth analysis of large volumes of historical data. O&M personnel can proactively identify, locate, resolve, and if required, notify customers of problems. This greatly enhances network exception identification and analysis capabilities and continuously improves network running quality and service experience.

- Machine-based decision-making. Traditional O&M relies on expert experience change. Under certain conditions (specified networking, underlying bearer technologies, and security authorization), network O&M is driven by data leverage AI machine learning and make decisions under human supervision. This enhances the system's capability to cope with complex and uncertain issues, greatly improving the response speed and resource and energy efficiency of network services.

- Open-loop management to data-driven, closed-loop autonomy of assured service experience. Traditionally, network planning, construction, maintenance, and optimization are independent of each other. Upstream and downstream data is transferred between processes and manual operations, without full-process data sharing and intelligence to ensure full-lifecycle experience. Network and service related data flows contribute to achieve closed-loop autonomy. The network SLA is specified in the network planning phase, including, but not limited to, the network QoS, time to provision, and time to repair. The construction, maintenance, and optimization phases are automatically driven according to this SLA for autonomy. This enables the network and service experience to be assured and encourages business innovation of differentiated network services.

The ultimate goal of enabling SDN is to achieve network automation, self-healing, self-optimization, and autonomy based on data and knowledge. More specifically, new services can be enabled with the optimal customer experience and automatic O&M, resource and energy utilizations are maximized, and network self-evolution towards autonomy is achieved based on automation, self-optimization, and self-healing.

How SDN contributes to achieve O&M automation in an IPv6/SRv6 network is further discussed in clause 6.2.7.

5.6 Quality of Service Requirements

The 5G QoS model [i.34] is based on the concept of QoS Flows. A QoS Flow represents the finest granularity of QoS differentiation in a PDU Session. A QoS Flow ID (QFI) is used to identify a QoS Flow in the 5G System. User Plane traffic with the same QFI within a PDU Session receives the same traffic forwarding treatment (e.g. scheduling, admission threshold). The QFI is carried on N3 (and N9); the SMF controls and configures it during session establishment. Any QoS Flow is characterized by a profile that contains, among others, the 5G QoS Identifier (5QI). This is a scalar used to reference 5G QoS characteristics that control QoS forwarding treatment for the QoS Flow.

On N3, each PDU is associated with one 5QI via the QFI carried in the encapsulation header.

While 5QI values describe the characteristics of a flow in the 5G system, the 3GPP does not provide any recommendations on mappings between them and the QOS code points used in a packet network. In general, the operator does this mapping based on local policies or proposed by a vendor according to configuration guidelines.

The assumption used here is that, for simplicity, eight code points are available. These eight values may be carried in an Ethernet frame using 802.1p bits (at layer-2) or associated to eight Differentiated Services Code Points (DSCP) values (at layer-3) [i.42].

In the case referenced here, a gNB is responsible for assigning a code point to the packets sent to the network based on the application or service type.

Depending on the chosen configuration, one or two code points are normally reserved for controlling and managing traffic between the gNB and the core network. The remaining ones may be associated to different classes of services.

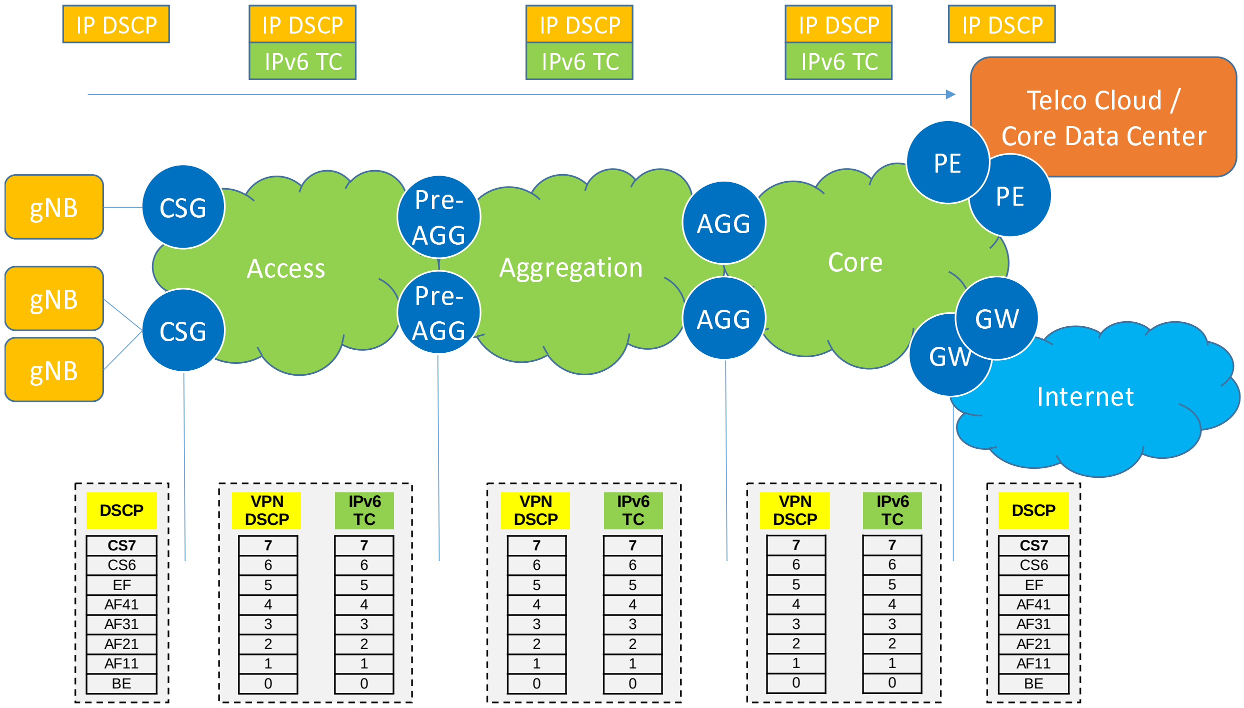
As an example, signalling, mission-critical and conversational voice traffic may be associated to the highest available code point(s), usually corresponding to Expedited Forwarding (EF) behaviour (or any other high-priority traffic handling). Such behaviour is often associated to priority queues.

Real-time gaming, streaming or conversational video may take the code points left free immediately after the first one or two. These code points are associated with Assured Forwarding (AF) behaviour, handled by Weighted Fair Queuing (WFQ) algorithms or a combination of Peak and Committed Information Rate (PIR/CIR).

TCP-based applications such as web, email, chat, File Transfer Protocol (FTP) are associated to the lowest code point, corresponding to Best Effort, prone to be discarded in case of network congestion.

As already discussed, the network employs SRv6 transport based on IPv6 forwarding. IPv6 Traffic Classes (TC) can identify service priorities throughout the network.

The mapping between the priorities used by a gNB and those used in the transport network is shown in Figure 7.



DSCP
CS7
CS6
EF
AF41
AF31
AF21
AF11
BE

VPN DSCP	IPv6 TC
7	7
6	6
5	5
4	4
3	3
2	2
1	1
0	0

VPN DSCP	IPv6 TC
7	7
6	6
5	5
4	4
3	3
2	2
1	1
0	0

VPN DSCP	IPv6 TC
7	7
6	6
5	5
4	4
3	3
2	2
1	1
0	0

DSCP
CS7
CS6
EF
AF41
AF31
AF21
AF11
BE

Figure 7: QOS handling

The QoS priorities of core, aggregation and access layers are streamlined in uniform mode (e.g. all network domains handle the same number of priorities). IPv6 TCs are used to identify service priorities and are derived from the DSCP values of the original packet sent by the gNB.

At the network border, a CSG applies proper treatment (e.g. it associates the IP DSCP with an IPv6 TC). SRv6, with or without SRH, encapsulates the original packet.

As further explained in clause 5.7, a L3VPN is considered at the service layer. The N2, N3 traffic by a gNB enters a dedicated VPN. Virtual Routing and Forwarding (VRF) is configured at the border elements (e.g. CSG and PE) to provide steering directives.

5.7 Service Layer Requirements

The perspective of the present document is to describe an IPv6-based 5G architecture at the network level, often referred to as the underlay infrastructure.

The main task exploited by such a network is 5G mobile service delivery.

It could be straightforward to say that, as the underlay infrastructure is IPv6-only, the same should happen at the service layer. Clearly, this may not be the case, as operators may have different strategies in coping with the introduction of IPv6 at both layers. This may depend on the fact that different teams handle the network and the services, or the local market requires to maintain some IPv4-based service offers for continuity or compatibility.

This clause then describes the typical approaches to deploying IPv6 at the service layer, also named the service overlay. These are often referred to as:

- IPv6 introduction; and
- IPv6-only service.

Depending on their preference, a service provider may adopt either of the two.

An operator may choose the former in the case they aim at delivering the service in a controlled manner, keeping the traffic volume of IPv6-based services minimal. Changes in IPv6 services may trigger the adoption of the second approach: as an example, the traffic volume may exceed a certain threshold. In that case, the transition to IPv6-only may occur, and the residual IPv4 traffic can be handled as a service (IPv4aaS).

On the other hand, an operator may prefer to adopt directly the second approach due to specific market or business opportunities, thus avoiding a step in the transition to IPv6-only service.

The two stages have technical differences.

The former is typically based on the enablement of Dual-Stack (DS) [i.43] in user's devices. With DS, IPv6 can be progressively introduced in some network portions, avoiding a major upgrade of expensive IT components, such as the management and support systems. Hosts and content can still operate in IPv4 and/or IPv6. For example, NAT64 can enable IPv6-only hosts to access IPv4 servers. As said, when the IPv4 traffic portion decreases below a determined threshold, it is not convenient to manage two protocol stacks.

The transition to IPv6-only may then begin. Usually, transition mechanisms have to be applied, with 464XLAT [i.36] being the most adopted in mobile networks [i.35]. Such stage may be facilitated by the natural upgrade or replacement of user's devices, which are nowadays already IPv6-capable.

5.8 SR Protocol Introduction

Operators enabling SR in their network may find themselves at different stages of the evolution path. Typical scenarios are:

1) The network is based on IPv4 and MPLS (no SR enabled).

2) The network runs SR-MPLS over IPv4.

3) The network is IPv6-based, with no SR enabled.

Different evolution paths are clearly possible to achieve the final target of having SRv6 enabled over an IPv6 network.

Operators finding at stage #1, may want to move to stage #2, at first. The advantage is to enable SR based on the existing MPLS data plane.

SR-MPLS simplifies network configurations, as it provides a simpler control plane. Protocols such as LDP or RSVP-TE are not required any longer, as only IGP/BGP extensions for label distribution and synchronization are requested. Alternatively, a SDN controller is used to uniformly distribute SR labels and deliver or synchronize them to devices. SR-MPLS reuses the existing MPLS forwarding plane at the data plane, enabling network devices to support SR forwarding through simple upgrades or without any modification. In SR-MPLS, segments can be mapped to MPLS labels, and paths can be considered as label stacks.

Overall, SR-MPLS is a choice for brown field operators, which have not begun the transition to IPv6 in the underlay network yet.

Networks that are already IPv6-based (either IPv6-only or in the transition process) can be brought to step #3. This is also applicable for greenfield operators that simply want to skip step #2.

The core components of SRv6 (the architectural framework and network programming) have already been standardized [i.10] and [i.11]. Most of the drafts specifying the OAM procedures are in their final stage.

While it is not possible to state, at the current stage, that SRv6 is complete in all of its parts, several real-world implementations [i.49] already exist, witnessing that SRv6 is entering its maturity stage.

6 IPv6/SRv6 Infrastructure for 5G Data Transportation

6.0 Introduction

This clause describes the architecture of an IPv6/SRv6-based network capable of transporting 5G services. The target is to provide operators with a high-level blueprint serving as a model to plan, design and operate their infrastructure.

The network architecture described here supports the following general characteristics:

- It is based on IPv6 and embeds the foundation technologies listed in in clause 5.
- It supports convergent services. It is designed to transport 5G mobile services. Still, previous generations of mobile services (e.g. 4G), as well as wireline services, may be carried as well (either consumer or business).
- It also supports native, end-to-end IPv6 services. The assumption is that end-to-end connections from the end-users to the services they connect to are natively transported over IPv6 without translation mechanisms.
- Services are differentiated based on SLAs or policies and handled by the network accordingly.
- It allows flexible operations. Automated provisioning and analytics-based monitoring should be enabled to ease the operational tasks.
- It is secure, as security is a key design element from scratch.

Clause 6.1 will discuss the physical architecture of a 5G transport network, highlighting the key network components and their role to fulfil the requirements of 5G (such as capacity, latency, timing, etc.). Clause 6.2 will enter the details of the IPv6 and SRv6 layers.

6.1 Physical infrastructure

6.1.1 Introduction

The scope of this clause is to describe the components of a 5G transport network, also referred to as a 5G backhaul network. The description will stay at a general level, highlighting the components that typically find their place in such an architecture. Real-world implementations may also include components not described here due to the specificity of the market where they operate or the services they support.

The architectural view of a 5G transport network is sketched in Figure 8.

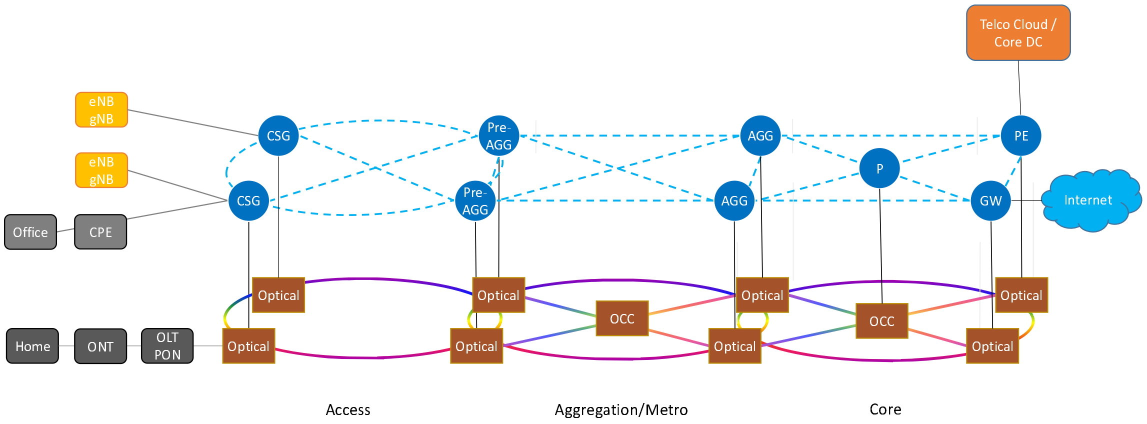


Figure 8: Typical architecture of a mobile transport network architecture

Under consideration, the 5G transport network follows the usual organization based on network domains. Usually, three main domains find their place in a mobile transport architecture, namely (left to right):

- The access network domain provides network connectivity to radio access, including equipment such as antennas and baseband units, on a geographically limited area. In a convergent network, this domain provides connectivity also to business and consumer fixed services.
- The aggregation network sometimes called metro network, domain consolidates the traffic generated by several access networks on a regional basis.
- The core network domain provides National and International connectivity, granting the end-users of a Service Provider access to the requested applications and services. The core Data Centres (DC) of an operator, hosting the Telco Cloud functions (e.g. the mobile core stack), typically connect to the core network domain. The core network is also connected to the Internet through gateways.

Such a physical 5G transport network will consist of integrated transmission technologies.

The IP layer provides end-to-end connectivity to the users and the applications served by the 5G network. Being the focus of the present document, the IPv6 layer is detailed in the next clauses, where the meaning and the role of the equipment depicted in Figure 8 is given.

The physical layer is usually based on Wavelength Division Multiplexing (WDM) or Optical Transport Network (OTN). WDM allows multiplexing several optical signals on a single optical fibre by using different wavelengths. OTN adds functionalities useful at the client-side. For example, e.g. it adapts and multiplexes electrical and optical signals in Optical Data Unit (ODU) structures, which are then sent on the line using WDM.

Such optical infrastructure is the preferred choice by operators to scale incapacity, to maximize the fibre utilization and provide the necessary resiliency level. Both technologies are represented in Figure 8 through the function called "Optical". The need for copying with higher throughput at higher resilience has recently motivated a change in the optical network topology. New elements, such as the Optical Cross-Connect (OCC, also named OXC), are now being deployed. To switch high-speed optical signals in an optical meshed network (thus moving away from the more traditional design based on rings).

Several networks employ an optical transmission layer end-to-end, from core to access. Other technologies may be employed in other cases, where fibres are widely available. This is the case of Ethernet or IP over dark fibre (Layer 2 or Layer 3 point-to-point connectivity). This solution finds its place particularly in access, where direct connectivity from a cell site to the packet access equipment is requested.

Another transmission technology employed in access is the microwave. Such a solution allows a remote cell to be connected to the access network through a wireless link operating in the range 4 GHz - 38 GHz (traditional microwave frequencies) or 60 GHz - 80 GHz (millimetre-wave frequency bands). Microwave often complements a wireline infrastructure in those cases where fibre is absent.

Independent of the specific choice, the transmission technologies just described provide an optimal transport of the 5G services supporting some key characteristics.

1) High network reliability, integrated with fast fault convergence:

   The protection schemes enabled by the IPv6 protocol stack are likely to be integrated with those enabled by an automated control plane active at the optical layer, e.g. Automatically Switched Optical Network (ASON).

   An active optical control plane supports functions such as automatic end-to-end provisioning, dynamic set up of connections, and fast and efficient re-routing. These functions contribute to achieving high reliability at the optical layer.

   Evolved Network Management Systems (NMS) or Software Defined Networking (SDN) platforms may coordinate protection at the different layers, triggering the requested actions to achieve fast fault convergence.

2) Unified Operations and Management (O&M):

   The management of a multi-domain, multi-layer network is often fragmented across different network departments.

   Unified operations and management are expected to be achieved by employing enhanced NMS/SDN systems leveraging higher integration and automation of the management processes. The different phases of the Network Elements (NE) lifecycle, including commissioning, configuration, provisioning and control, adapt to the frequent changes in mobile services, preventing configuration errors.

6.1.2 Impact of 5G core over the transport network

As outlined in clause 4, the distribution of the functions comprising the 5G core across the network domains and closer to the end-users may influence the way the transport network is designed. This is, at least, partially new with respect to the previous generations of mobile services.

The functional disaggregation has the merit of moving some functions closer to the end-users to support the Key Performance Indicators (KPI) determined by specific classes of applications. As an example, applications belonging to the uRLLC group typically require a network transport service characterized by tightly controlled delay (e.g. in the order of a few milliseconds).

Some functions have to move to a network location closer to the end user (i.e. at the edge of the transport network) to enable low latency communications. From an implementation perspective, this is realized through the deployment of a smaller-scale DC hosting the functions that serve the low latency applications.

As a result, a 5G transport network may consider the presence of multiple layers of DCs hosting the 5G core functions that serve different groups of applications. Figure 9 highlights a 3-layers DCs infrastructure.

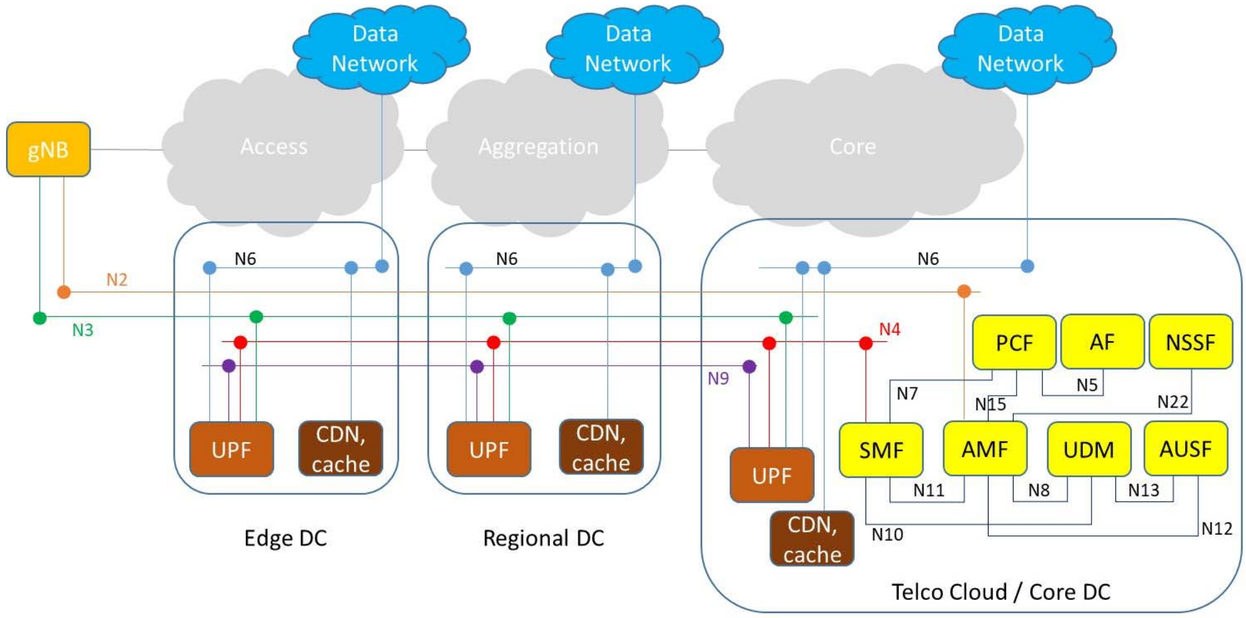


Figure 9: 5G core reference architecture (ETSI TS 123 501) with functional distribution in a 3-levels DCs structure

Moving from right to left, the first layer is represented by the core DCs where most of the functions part of the control plane is located. This core layer is expected to include a small number of DCs on a nationwide basis.

The next layer may be located further down along the network path, for example, at a regional basis. Some control functions may be moved (if needed), while the tasks that are part of the user plane and are needed to support faster communications with an end-user are deployed.

A third level may be enabled if very fast communications are requested. In such a case, it is expected that uRLLC user-plane functions are deployed at the edge of the network.

A multi-layer DC infrastructure is an integral component of a 5G transport network. As such, it has to be included from the beginning in the overall network design.

6.2 IPv6 and SRv6 Layer

6.2.1 High-level View

No matter the IP protocol family, a layer-3 networking solution consists of forwarding devices with specific roles based on their position in the network architecture described in clause 6.1.

Figure 10 highlights all the relevant networking devices located in the relevant domain.

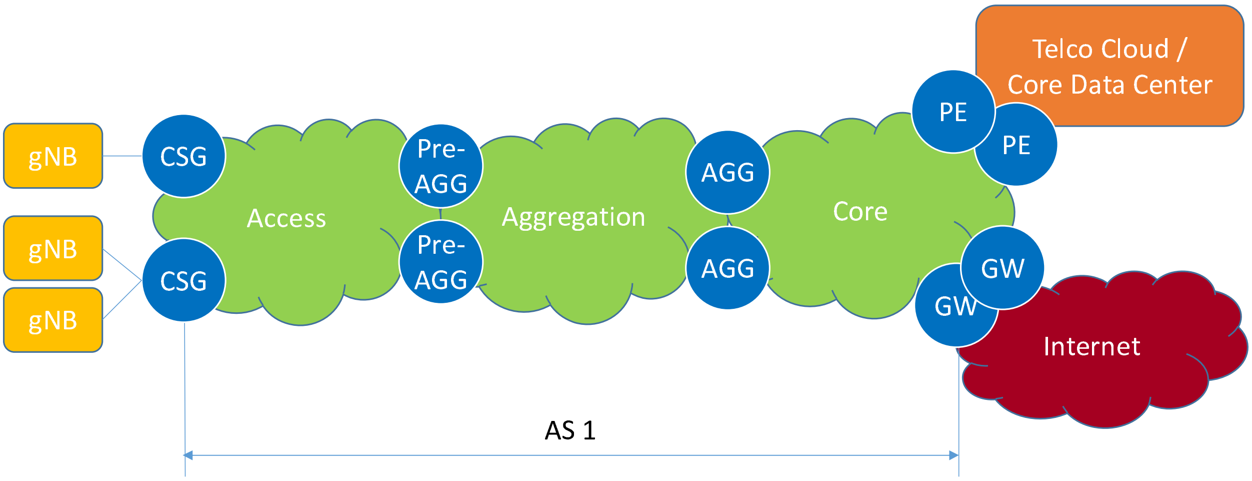


Figure 10: High-level architecture of a packet-based (layer-3) mobile transport network

At the border of the access domain, Cell Site Gateways (CSG) provide IP connectivity to the cell sites (gNBs). The access domain also includes Pre-Aggregation devices (Pre-AGG) that consolidate the traffic on behalf of an aggregation area. An aggregation domain further grooms the traffic generated by users and services in access domains and move it to the core through Aggregation devices (AGG). The core usually hosts International Gateways (GW) to connect to the Internet, peering points and other carriers.

Along the network domains, Provider Edge (PE) routers are found whenever there is a need to interface to external services like the 5G core DCs.

The network represented in Figure 10 is assigned a single Autonomous System Number (ASN). This may be the case of a network spanning a country or a region.

Other cases may exist, particularly when the network footprint covers a wider area (e.g. it is segmented in several administrative domains or extends across multiple countries). In such a case, the network design may consider employing multiple ASNs, as highlighted in Figure 11.

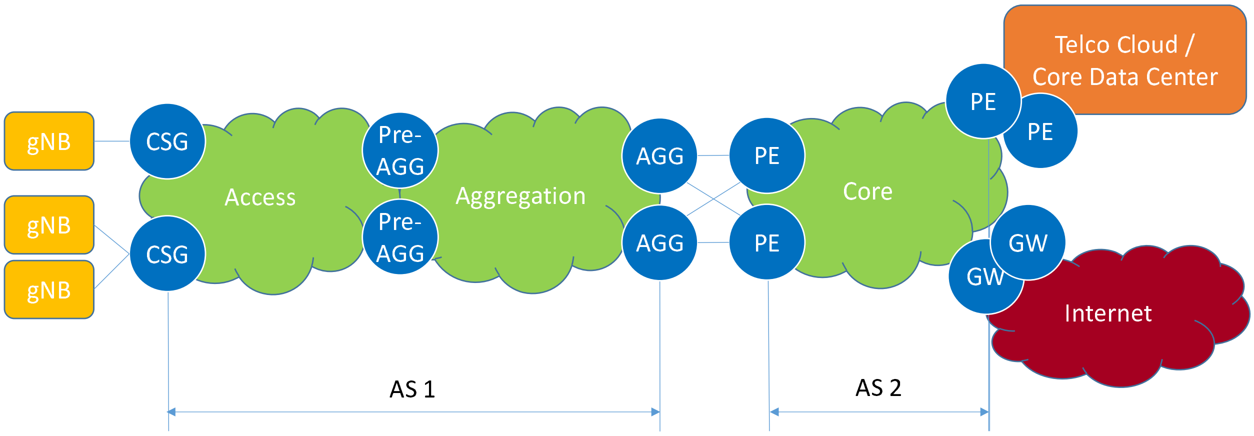


Figure 11: Multiple ASNs in a mobile transport network

The routers at the border of the two ASes (different administrative domains) represented in Figure 11 have to coordinate the exchange of both routing. Service-related information is exchanged, e.g. through eBGP updates.

The current version of the present document focuses on the single-AS case, as per Figure 10. A future release will also include the multi-AS case.

6.2.2 Introduction to the IPv6 Architecture

The scope of this clause is to summarize the main steps that are propaedeutic to the introduction of more advanced transport mechanisms (subject of the next clauses).

A few key elements can be considered:

- The availability of IPv6-based address plan.
- The deployment of the basic management services (e.g. DNS, DCHP).
- The choice of the routing protocols active on the control plane.
- The deployment of a management plane and Data Control Network (DCN).

These items are discussed next.

Numbering plan

For the addressing plan, it is assumed that the network operator has its own address space already allocated (e.g. a /32 network prefix assigned by a Registry). Here, it is assumed that they are Global Unicast Addresses (GUA), routable over the Internet.

Possible options (not exhaustive) suggest to:

- Allocate an address block for loopback interfaces (e.g. /48) and assign each loopback interface a /128 network prefix [i.44].
- Allocate an address block for point-to-point links (router-to-router) and assign each link a /64 prefix [i.44] or a /127 prefix [i.45]:
  - IETF RFC 4291 [i.44] discussed using a modified EUI-64 format to build the 64-bit interface identifier (IID). In summary, IID is obtained from the interface MAC address inserting between the Organization Unique ID (OUI, the first 3 bytes) and the Network Interface Card specific (NIC, the last 3 bytes) 2 additional bytes (coded as 0xFFFE). This format is quite old but still commonly used in live networks.
  - IETF RFC 6164 [i.45] proposes /127 prefix allocation for a point-to-point link. The advantage stands in an optimization of the use of addresses and a straightforward forwarding process at the router interface. From a numbering perspective, it is advisable to allocate a /64 prefix for a point-to-point link and, eventually, assign a /127 prefix. Some operational guidelines also consider using a /126 prefix instead of /127.
- Even if not represented in Figure 11, further network organization is possible. For example, a geographic Point of Presence (POP) may be assigned a dedicated prefix (e.g. /48) for easier localization and troubleshooting.

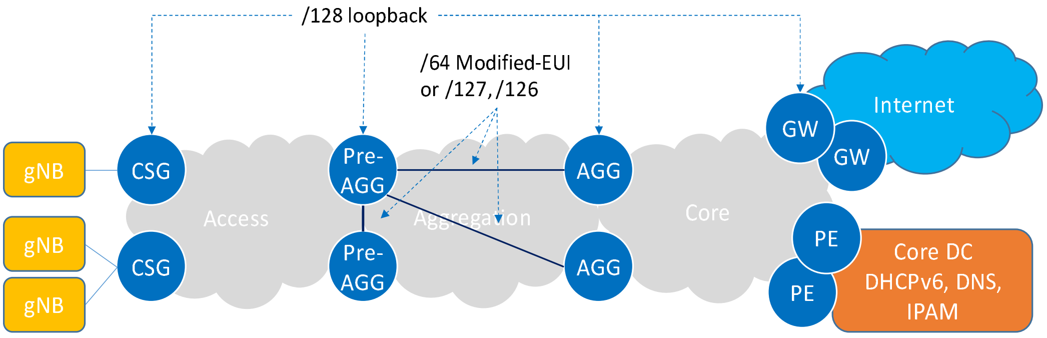


Figure 12: Example of IPv6 address plan

It has to be noted that only a few links are represented, e.g. those connecting the first Pre-AGG node at the top with 3 other nodes in the aggregation domain.

Several guidelines and Best Current Practises (BCP) are currently available from the Internet Registries that provide suggestions and common rules on developing an IPv6 address plan as per [i.4].

For SRv6 to operate properly, further considerations about the addressing plan need to be discussed.

Each node may need to assign SIDs on a local basis (e.g. to identify the locally attached nodes or prefixes). These SIDs may be assigned based on protocol exchange, local policies or through an SDN/management system.

Moreover, if SRv6 network programming is foreseen, some dedicated SIDs have to be considered. While such SIDs are still in the form of an IPv6 address, the address structure is partitioned to contain a node locator, a reference to the local function to be executed and possibly some associated arguments.

The structure of these SIDs is further discussed in the next relevant clause 6.2.3. For the scope of the addressing plan, at least another IPv6 address/SID has to be allocated for the network programming function. Figure 13 explodes a point-to-point link connecting two nodes (Node A and Node B, respectively) and the envisioned address allocations.

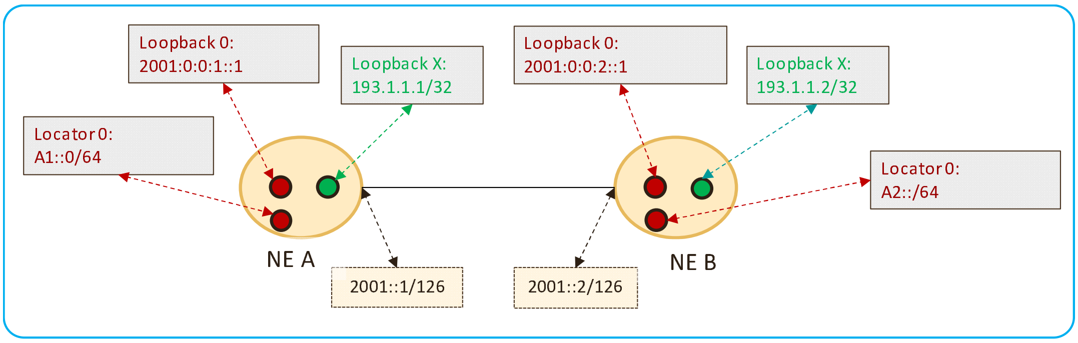


Figure 13: IPv6 addresses used by two nodes connected through a point-to-point link

The following addresses are considered.

Table 2: Addresses used on a network element

Type	Name	Address Planning	Function
Logical interface	Loopback 0	IPv6: 128-bit global address	Route advertisement in IGP domains and BGP peer relationship establishment.
	Locator	IPv6: global address with a user-defined mask	SRv6 deployment and SRv6 VPN addressing.
	Loopback X	IPv4: host address with a 32-bit mask	DCN management. While IPv6 is envisioned also in DCN, current systems are not still fully IPv6-ready. Recommended to maintain IPv4 support.
Physical interface	NNI	IPv6: global address with either /64, /127 or /126 bit mask. Figure 13 adopts a /126	IGP route reachability.

Basic Management Services (DHCP, DNS for IPv6) and IP Address Management (IPAM)

Depending on the operator's need and/or preference, different solutions to manage the IPv6 addressing plan and the address assignment may be considered.

The basic components are represented by Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) services.

DHCP for IPv6 (DHCPv6) [i.46] allows the configuration of IPv6 nodes with IP addresses, network prefixes, and network configuration parameters such as DNS [DNS] and NTP [NTP] server addresses. DHCPv6 allows two modes of operations: stateful or stateless. Assuming stateful mode, a server delivers a client a set of configuration parameters, including an address or a prefix and other information such as DNS-related.

DNS for IPv6 (DNSv6) [i.47], handles the mapping between names and addresses. Forward lookup (from a node name to its IPv6 address) is dealt with through the AAAA Resource Record; Reverse lookup (from the IPv6 address to the name) through the PTR Resource Record.

IPAM is a framework used for planning and managing the assignment and use of IP addresses. In some cases, a single solution integrates these functions with DHCP and DNS services.

The assumption followed by the present document is that all these services are supported by several redundant servers located in a centralized location such as the Core DC (see Figure 12 above).

Routing Protocols

The choice of the control protocols is usually operator-specific, but it is envisioned that:

- ISIS or OSPFv3 propagate internal reachability. To do that, IGP protocols partition the AS in areas to achieve better scalability (e.g. for ISIS a level-1 area covering access, a level 2 for aggregation, and a level-2 associated with the core domain).
- iBGP is used to exchange global prefixes (e.g. destinations external to the network's AS) typically to the edge routers (e.g. PE, CSG, etc.).

The control of the distribution of the iBGP routes is done using some Route Reflectors (RR) deployed in all the domains. RRs allow all iBGP speakers within a network domain to learn about the available routes without introducing loops and avoiding a full-mesh of iBGP peers, which would add complexity to the network configuration.

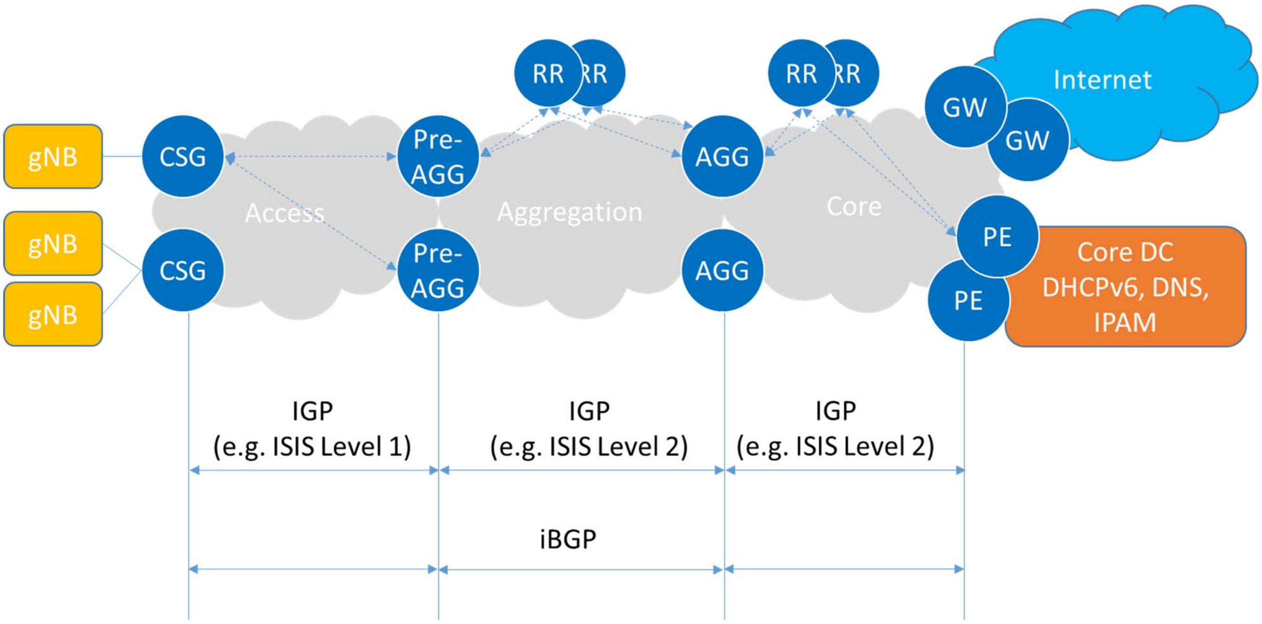


Figure 14: Routing architecture

Data Control Network (DCN)

While not explicitly represented in the previous pictures, a DCN is always present in an operator's network. Its function is to allow the operational staff to connect through dedicated in-band or out-of-band channels to physical equipment for OAM and troubleshooting.

It is envisioned that, at present, the DCN still relies on IPv4 connectivity or be Dual-Stacked. As highlighted by several operators, the reason for that is the non-complete availability of single-stack IPv6 management and operations support systems.

This has been highlighted both in Figure 13 and Table 2 with an IPv4 loopback interface specifically dedicated to management purposes.

End-to-end architecture

While the present document's focus is on the 5G transport network, portions of the RAN and of the Core DC that connects to the transport network have to be also considered.

Each gNB will also be assigned with one or more IPv6 prefixes. These prefixes will be associated with the VLANs carrying the traffic of the 5G interfaces. It is envisioned that a gNB may employ a VLAN for the N2 control traffic, one for the N3 data traffic, one for the X2/Xn traffic exchanged with neighbour nodes. Other VLANs may be used to carry OAM traffic and, if necessary, synchronization signals. The configuration of the gNBs network parameters may be performed by dedicated entities (RAN management systems or RAN controllers).

At the other side of the service trail, it is expected that a number of Virtual Machines (VM) host the mobile core functions and terminate the service relationship. As for the RAN, each VLAN is assigned a different prefix. The servers that run the VMs are connected to the DC infrastructure, based on the common leaf-and-spine approach. Depending on whether the Spine and the Leaf clusters are assigned the same or different ASNs either iBGP or eBGP may be employed to propagate the internal reachability. Border Switches (BS) exchange the routes internal to the DC with the network PEs through eBGP.

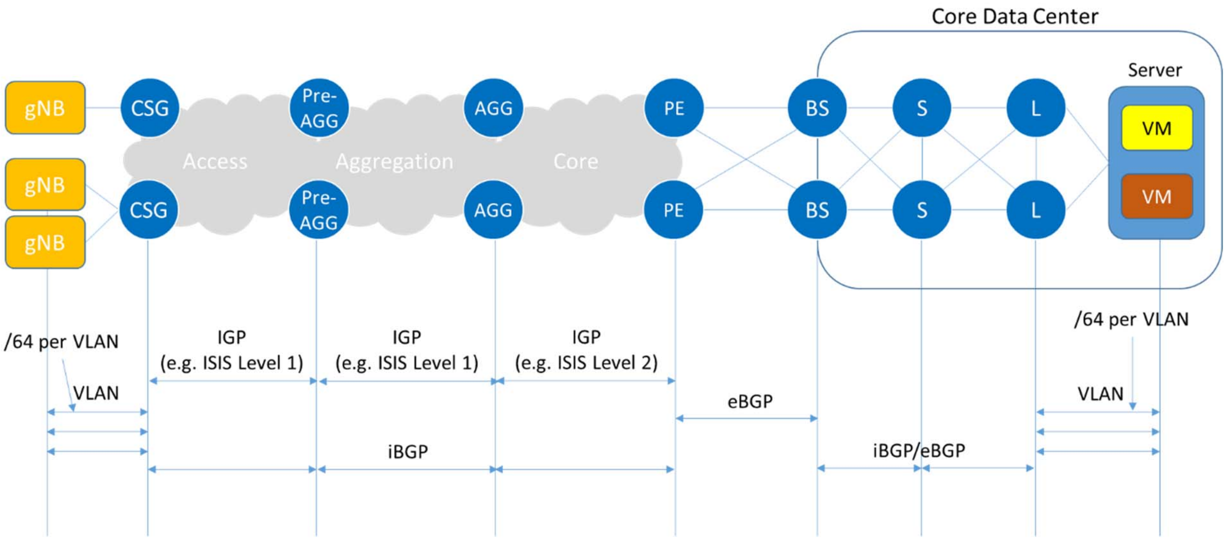


Figure 15: End-to-end view, including RAN and Core DC

6.2.3 SRv6

As introduced previously, SRv6 acts on the data plane. Its benefits include protocols simplification and a quicker deployment of multiple services. Based on SRv6 tunnels (Segment Identified list or SID list), the solution allows carrying mobile, fixed, and enterprise services together, reducing operators' investment and O&M costs. The Pre-requirement of SRv6 is the deployment of IPv6 in the network, as discussed in the clause 6.2.2.

For SRv6 to operate properly, further considerations about the addressing plan need to be discussed.

Each node may need to assign SIDs on a local basis (e.g. to identify the locally attached nodes or prefixes). These SIDs may be assigned based on a local policy or through an SDN/management system.

Moreover, if SRv6 network programming is foreseen, some dedicated SID have to be considered. While such SIDs are still in the form of an IPv6 address, their structure may be partitioned as represented in Figure 16 (providing only one of the many possible options).

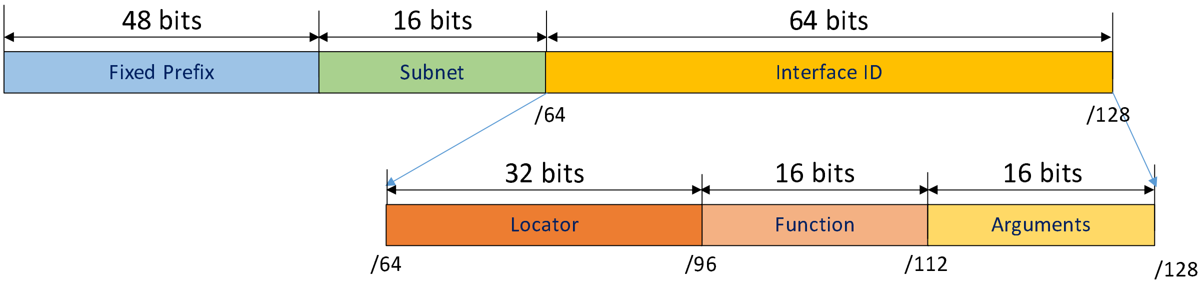


Figure 16: Locator, function and arguments for network programming

As specified in IETF RFC 8986 [i.11]:

- The locator is represented as the combination of the SRv6 SID block (IPv6 prefix allocated for SRv6 SIDs) and of local identifier.

- The function is an opaque identification of a local behaviour bound to the SID or, in simple terms, an action or policy associated with the SID (such as decapsulating the inner packet or forwarding it to a destination).
- The argument comprises additional information for processing a function (e.g. related to the flow or service). The semantics and format of the Argument bits are defined as part of the SRv6 Endpoint behaviour specification.

As shown in Figure 13, the bits of the locator can be used hierarchically, allowing to identify a specific region, area, POP or subnetwork. This way, the labelling of the equipment part of SRv6 domain results simplified.

6.2.4 Service View

The convergence of mobile and fixed networks is imperative to meet the increasing demands for mobile and fixed network services and the urgent need for operators to reduce investment and OPEX.

The converged network has to carry multiple services, including:

- Mobile services: 5G is carried on the same network as 4G and previous generations of mobile services. They implement communication between base stations and controllers/core network devices.
- Fixed services: HSI, VoIP, and IPTV, provide channels for dial-up access, access network devices (such as OLTs), and service platforms (such as IPTV service platform/DHCP servers).
- Private line services: Layer 3 and Layer 2 private line services enable enterprise sites to communicate with each other.

All these services are carried in an integrated way over the network discussed so far, even if our attention is on the transport of 5G services.

From an architectural standpoint, the 5G services discussed so far are carried over L3 VPN [i.5], as shown in Figure 17. As an alternative option, the same services may be transported over EVPN [i.6] or even L2 VPN [i.7], [i.8] and [i.9].

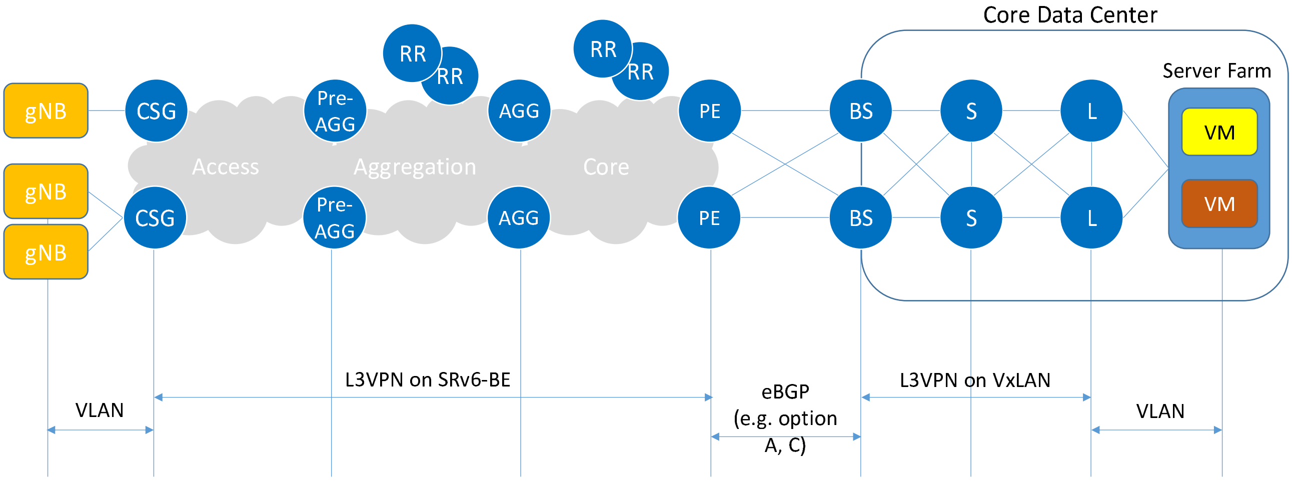


Figure 17: End-to-end transport of 5G services

While the network described throughout the present document is suitable for any service's transport, our focus is on 5G. Table 3 describes how the 5G services (interfaces) can be carried by the architecture shown in Figure 17. Based on the assumption that 5G services are carried over L3 VPN connectivity, each service/interface is served by a dedicated Virtual Routing and Forwarding table (VRF).

Table 3: 4G and 5G services carried over SRv6

Service Type	Service Description	Transport Technology
LTE S1	Services between LTE eNodeBs (base stations) and Evolved Packet Core (EPC) networks, including control plane data and user service data.	SRv6-based L3VPN
LTE X2	Interconnection services between LTE eNodeBs.	
5G N2, N3, N4, N9	Services between 5G gNBs and 5G Core (5GC) networks, and services between core NEs.	
5G Xn	Interconnection services between 5G gNBs.	

Figure 18 provides a high-level representation of the exchange of control information to enable the transport of the 5G services through an L3 VPN and the resulting forwarding path.

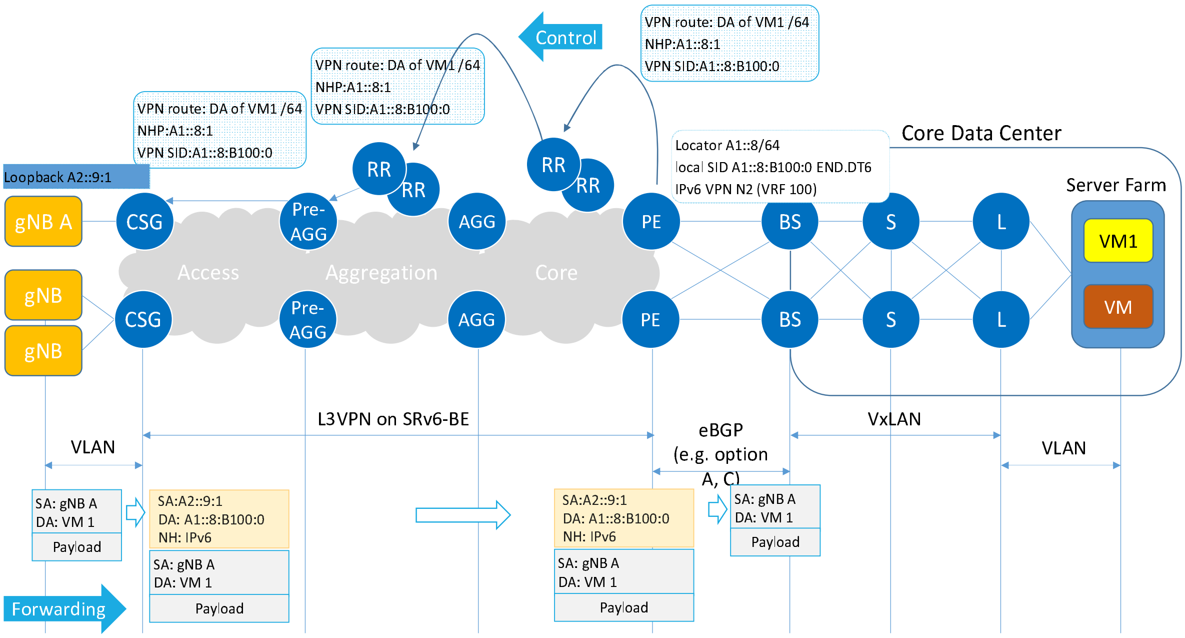


Figure 18: SRv6 transport of 5G services (L3VPN)

Figure 18 illustrates the basic mechanism to distribute the address of Virtual Machine 1 (VM1), which sits in the Core DC and, as such, is outside of the network domain. The two PEs at the border of the core domain have VM1 in their VRF table associated with the VPN that carries the traffic from the gNBs, on the left. For example, one of the PEs has addressed A1::1 (loopback), while the SID associated with the VPN processing is A1::8:B100:0. This latter address is structured to have a locator (A1::8), and a function identified, corresponding to B100. The arguments are set to 0.

B100 corresponds to a behaviour that consists of decapsulating the original packet generated by one of the gNBs and forwarding it to the next-hop (the first router at the border of the DC).

VM1 is distributed by the control plane, based on BGP, as shown in the top part of the picture.

The RRs have the function of consolidating the information received through BGP and of propagating it forward to the listening iBGP receivers. Assuming RRs are not in line, their role is to propagate the advertisement without changing the target address, which remains the original address of the PE injecting the VPN route (A1::8/64).

Figure 18 assumes to have an SRv6-BE forwarding plane. This way, the path followed corresponds to the one defined by the IGP Shortest Path Forwarding (SPF) policy (minimization of the link cost).

Figure 19 shows the configuration of the VFRs necessary to carry the foreseen 5G traffic across the network.

Three VPNs are considered:

- 5G network transport (backhaul). This VPN is responsible for transporting the N2, N3, Xn interfaces across the IPv6 network. Each node involved has a corresponding VRF configured for this purpose. This is named "BH VRF" in Figure 19 (BH stands for Backhaul).

- 5G Core. This is the VPN connecting the 5G core functions and associated with the control interfaces shown in Figure 9 (Figure 19 only shows the N2, N3 interfaces for simplicity). The corresponding VRF is named as "5GC VRF".
- Public VPN. The VPN normally carries the traffic of the N6 interface destined to destinations located in external networks. The corresponding VRF is named as "Public VRF".

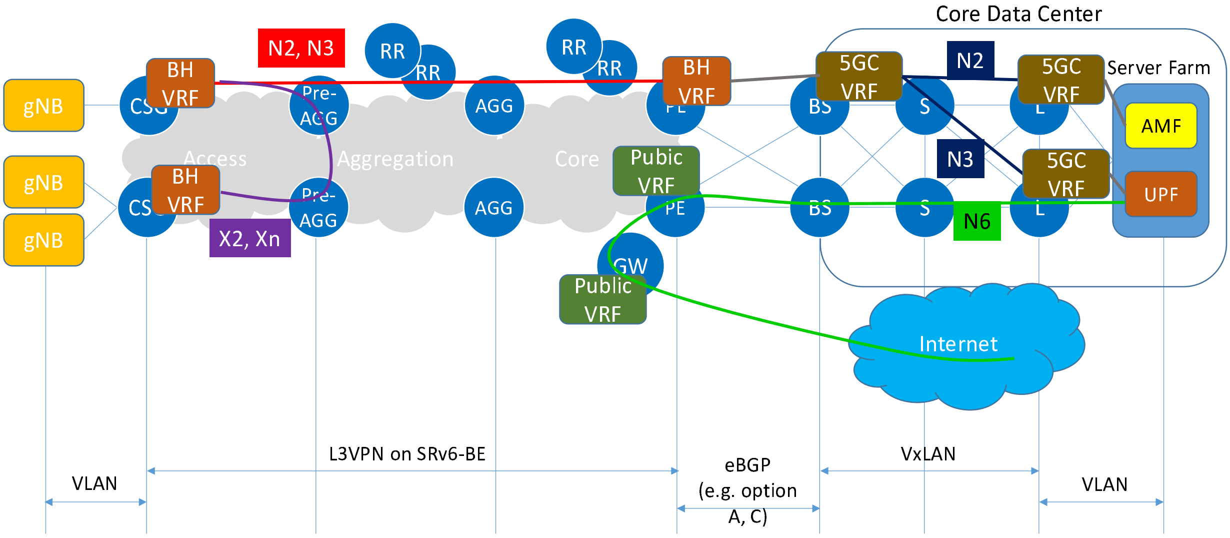


Figure 19: VRF-based Service Infrastructure

Figure 19 intends to provide a high-level description. Different architectural alternatives can be considered, depending on the protocols used and service requirements.

6.2.5 SRv6 Policy Forwarding

This clause discusses the policy forwarding mechanism supported by SRv6 traffic engineering (SRv6-TE). This is a key capability of SRv6, which allows the creation of network slices.

SRv6-TE uses a policy (a set of SIDs) to steer traffic through a network. The headend determines which policy to associate to a specific traffic flow. Each node in the network path uses the top SID to choose the next-hop, pops the SID, and forwards the packet to the next node. The packet is forwarded with the remainder of the SID stack until it reaches the ultimate destination.

An SRv6-TE policy is uniquely identified by a tuple (colour, endpoint). Colour is a 32-bit number, while the endpoint is a valid IPv6 address. Multiple policies can be created between two endpoints; the condition is that each policy has a different colour.

Through policies, it is possible to define differentiated handling for traffic flows. As an example, two policies between the same two endpoints, each with its colour (e.g. colour 1 and colour 2), may specify a low-latency path (e.g. identified by colour 1) and a high capacity path (colour 2).

The high-level behaviour is shown in Figure 20.

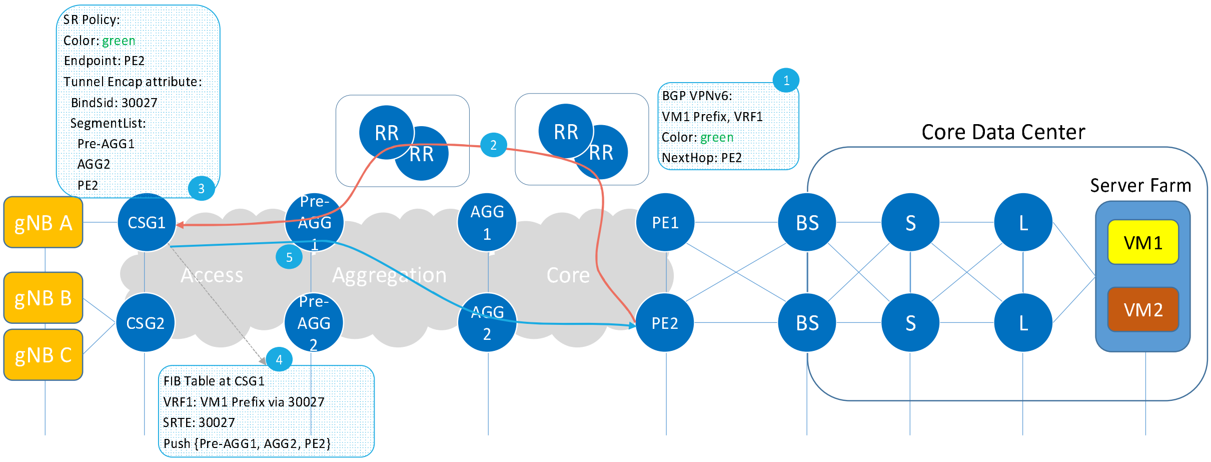


Figure 20: SRv6 Policy Procedure

1) As a first step, PE2 establish an MP-BGP peer relationship with CSG1, specifying VPN peer with colour extended community.

2) The headend (CSG1) receives a BGP user-specific network route with the COLOR extended community attribute.

3) The headend (CSG1) either imposes (if it is configured to do so) or receives (e.g. from a controller) a SRv6-TE policy (colour, endpoint, BSID, tunnel label stack); and generates a forwarding plane tunnel.

4) After the BGP route received by the headend matches the tunnel, a FIB entry is generated according to the colour and endpoint of the SRv6-TE policy.

5) During head end's traffic phase: ingress packets are steered to the SRv6-TE policy tunnel corresponding to the keys: colour + next-hop (Endpoint). A DSCP can also be associated with the combination: colour, next-hop (Endpoint).

The resulting forwarding process is shown in Figure 21.

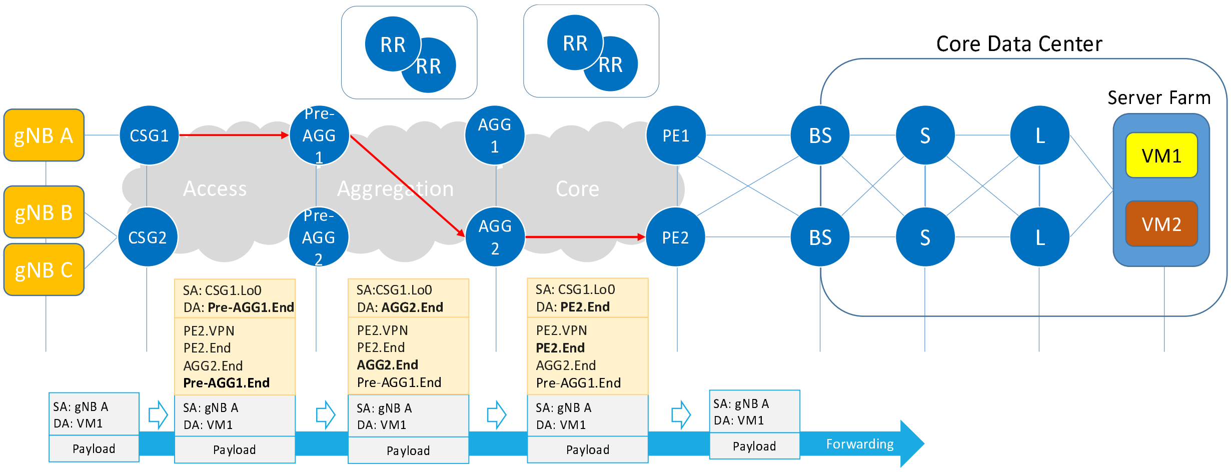


Figure 21: SRv6 Policy Forwarding

The mechanism shown in Figure 21 was already introduced in clause 6.2.4. Here, the policy-based forwarding is pushed forward: every node in the path takes independent decisions based on the SID list in the external SRH [i.11]. The red lines shown in Figure 21 illustrate the progression in the forwarding process.

CSG1 imposes an SRH to the original packet where the DA contains the information to reach the next-hop (in this case, Pre-AGG1) and the behaviour associated with the policy, specifically the function End. As explained in clause 4.1 of IETF RFC 8986 [i.11], the End behaviour operates on the same FIB table associated with the packet (i.e. identified by a VRF) and, if not the last node in the path, provides a swap of the DA in the SRH.

When the packet reaches PE2, the first action is again to perform an End function. When acting on the next SID, PE2 finds a function associated again to itself and requiring "VPN" handling. According to [i.11], this is an End.DT6 function, corresponding to decapsulation and specific IPv6 table lookup. SRH is removed, and the original packet is sent to its DA (VM1).

6.2.6 Network Slicing

The context around network slicing has been previously introduced in clause 5.3. As highlighted, the data plane is based on SR-v6 TE.

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

Each SID has a locator dedicated to a specific slice, as shown in Figure 22.

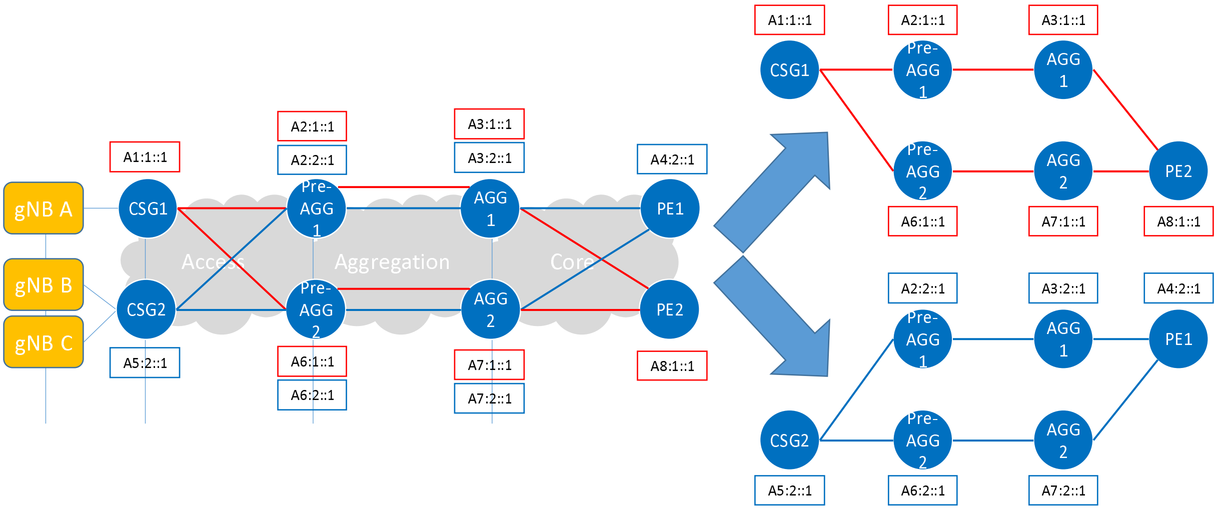


Figure 22: Network slicing based on locators

The identification of a network slice is guaranteed by a specific locator assigned to a node. The example above shows that CGS1 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 node Pre-AGG1 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-AGG1, while the following number is the slice identifier.

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 22. 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) have 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.15] and [i.16].

Specific extensions for SRv6-based network slicing have to be considered. As an example, these have been proposed in [i.14]. These extensions allow the creation of multiple virtual topologies in a physical network where each virtual topology has specific attribute customization. This way, the topology-ID parameter (the identifier of a topology) is re-used as a network slice identifier embedded in the locator information. Each topology advertises slice-specific SRv6 locators and SIDs and the resource attributes associated with SRv6 SIDs.

6.2.7 Network OAM

This clause discusses the Operations, Administration and Management (OAM) mechanisms applicable to network and service layers. An IPv6 network adopts the same mechanisms already available in an IPv4 network to detect faults or measure performance. Some extensions have to be considered specifically for SRv6.

Figure 23 highlights of the OAM protocols foreseen in an IPv6-based 5G transport network.

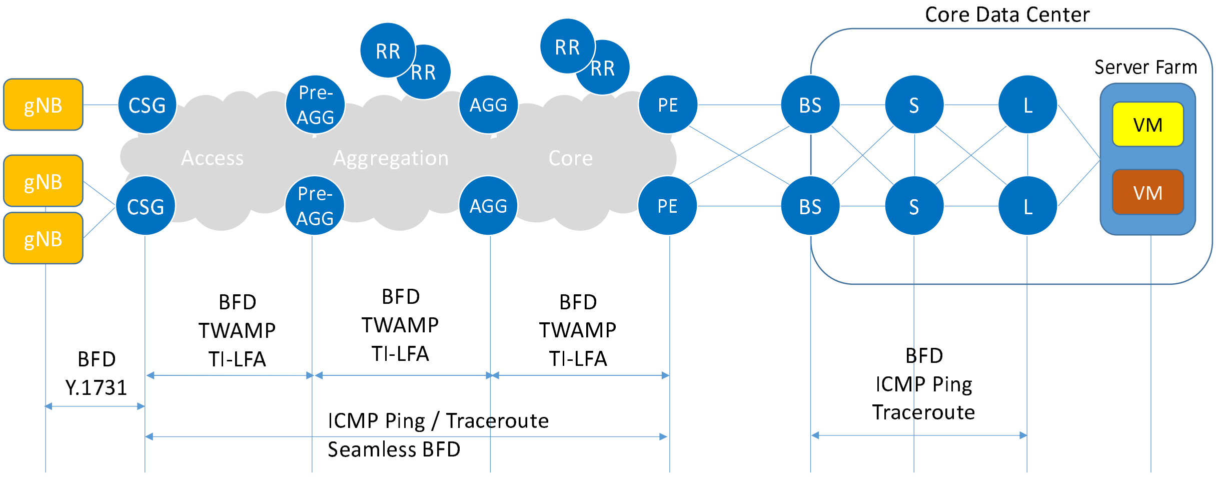


Figure 23: Network OAM protocols

It is envisioned that gNBs implement mechanisms to detect faults at layer-2 and layer-3. For example, Recommendation ITU-T Y.1731 [i.17] specifies mechanisms required to operate and maintain the network and service aspects of an Ethernet connection. Bidirectional Forwarding Detection (BFD) [i.18] and [i.19] works instead at layer-3 to detect faults between two routers or switches connected by a link.

Moving to the backhaul network domains, more protocols have to be considered.

In addition to BFD, Two-Way Active Measurement Protocol (TWAMP) [i.21] can be used to activate round-trip measurement capabilities, such as collecting data on latency, bandwidth or packet loss. Seamless BFD (S-BFD) [i.20] can also be considered to detect the reachability of an end node of a layer-3 connection, even when the end node is not directly connected.

Introducing an SRv6 data plane [i.10] also requires some specific mechanisms. In general, it is a matter of adapting traditional OAM mechanisms, such as ping and traceroute, to detect if a SID is reachable, to the presence of the new SRH [i.22]. Topology Independent Loop-free Alternate Fast Re-route (TI-LFA) [i.23] finally provides fast-rerouting capability, protecting node and adjacency segments.

6.2.8 Future View

It may be interesting to have a quick look at the foreseen evolution of the IPv6/SRv6-based 5G transport framework discussed so far. This mainly concerns the extension of the protocols introduced in the previous clauses from the edge to the network to the DC, providing convergence of the mechanisms adopted in both the network and the DC environments. The next diagram shows a possible target reference architecture.

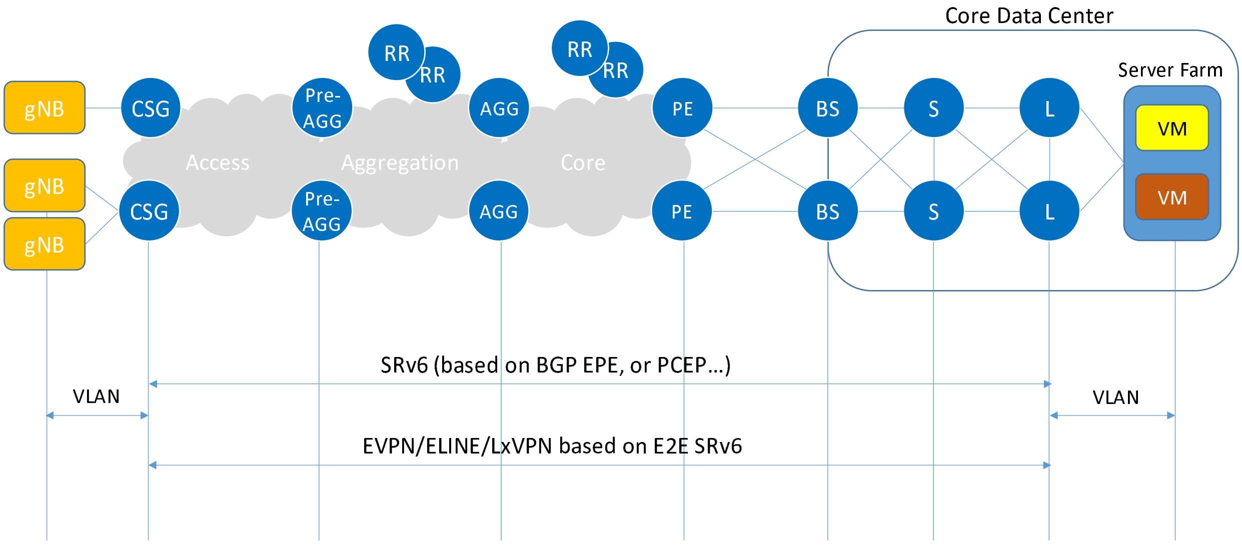


Figure 24: Evolution of the IPv6-based 5G transport architecture

The notable evolution aspect is SRv6 end-to-end across the network and the DC infrastructure. This provides an operational simplification as some functions currently deployed at the border of the two domains disappear, simplifying OAM. Different mechanisms can be enabled on the control plane for the distribution of the reachability information, such as BGP-based Egress Point Engineering (EPE) [i.24] or Path Computation Element (PCE) [i.25] extensions for segment routing.

At the service layer, all services are carried over SRv6, with Ethernet VPN (EVPN) [i.26] being the mechanism foreseen to achieve a converged transport of all services end-to-end.

6.3 Network Automation and SDN

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 25.

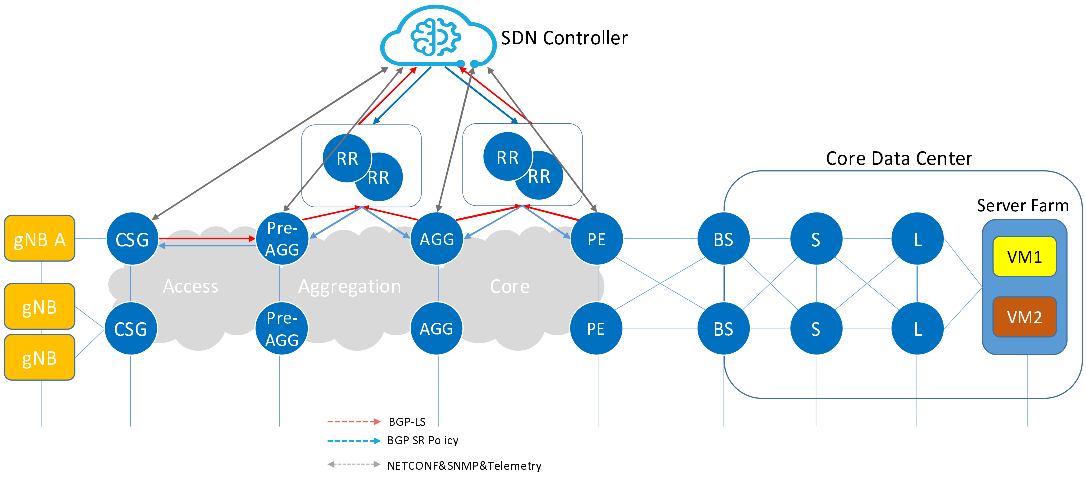


Figure 25: SDN role in an IPv6/SRv6 network

The SDN controller acts as the centralized repository of the configurations of all nodes, retrieved by several mechanisms or protocols, such as Netconf [i.50], 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 network is BGP Link-State (BGP-LS) [i.27] and [i.28].

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 25, 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 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 25) is through [i.29].

An SDN controller uses BGP SR to advertise an SR policy towards a headend node. The SR policy may include one or more candidate paths, each consisting of more segment lists.

6.4 Synchronization

Mobile services require high-precision time synchronization. A mobile operator may consider deploying GPS receivers at the cell sites to achieve the accuracy requested. This approach may be preferred to keep the transport network simple or when the transport network is not fully owned by an operator.

On the other hand, the transport of synchronization across the network may be considered to avoid the costs of deploying too many GPS receivers. In this case, at least two solutions may be considered:

- Deploy a few centralized master clocks (e.g. atomic oscillators) in network core and provide both frequency synchronization (synchronous Ethernet) and phase synchronization (IEEE 1588 [i.30] coupled with Recommendation ITU-T G.8275.1 [i.31] implementation profile) across all the NEs on a network path down to the cell site.
- If all the support of time synchronization mechanisms is lacking in some parts of the network, deploy local clocks, e.g. Building Integrated Timing System (BITSs) at the aggregation or the access stage and enable the hop-by-hop transport of frequency and phase signals only across a limited set of NEs.

A mix of both synchronization architectures can also be considered, depending on the operator's preference and attitude. Figure 26 shows a possible mix, on a high-level basis.

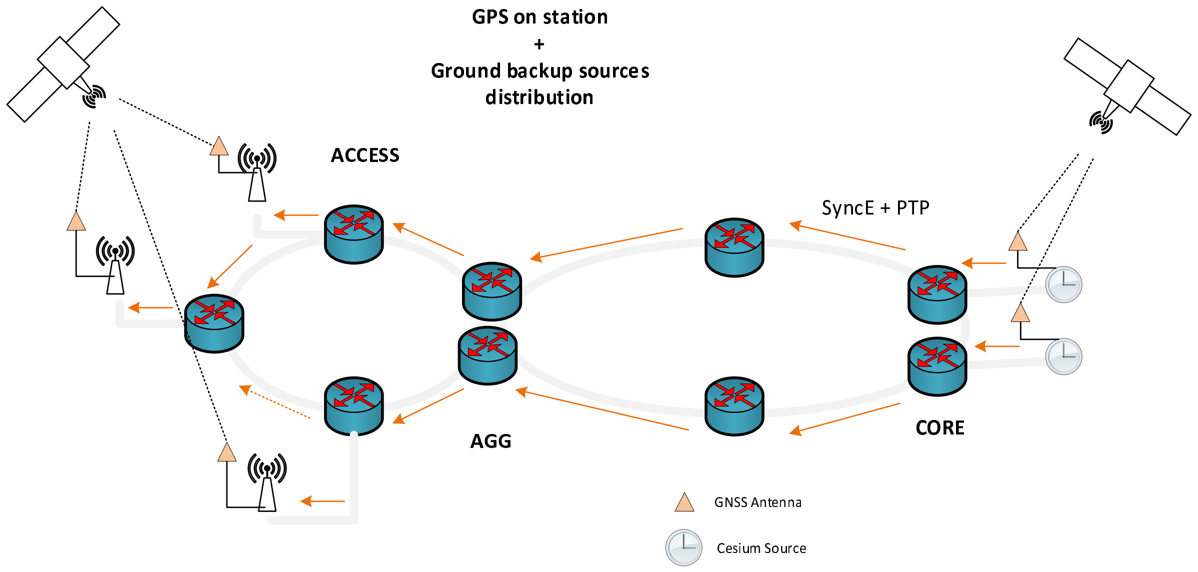


Figure 26: Synchronization architecture

Specifically, for the transport of synchronization signal across the network, some design rules have to be considered.

First, a couple of clock sources should be deployed in a synchronization area. These clock sources trace satellite synchronization clocks, and the built-in rubidium clock or external caesium clock provide the holdover capability.

Ethernet interfaces are recommended for the connection between clock sources and network devices. If neither clock sources nor network devices provide Ethernet interfaces, external 2 Mbit/s clock interfaces should be considered.

The number of synchronization nodes from a clock source to a base station cannot exceed 20. If the number exceeds 20, move the clock source downwards.

Each node across the path should have G.8275.1 Telecom Boundary Clocks (T-BC) configured for proper phase regeneration.

7 5G and Cloud interactions

7.1 Overview of 5G transport

5G Transport network is a kind of network infrastructure that mainly provides connections from the user equipment to a core network in 5G mobile networks. The advantage of the 5G transport network is that it helps operators leverage the same access connectivity to transport any kind of traffic, including Internet access, audio, video, and computation applications. Due to mobile-fixed convergence, operators also begin to provide fixed services to customers over the 5G transport network, which is the same to what happens in the legacy 4G mobile backhaul network. In addition, the cloud has been an essential part of information infrastructure. More and more applications will be cloudified. Serving the cloud-related scenario is the main duty of 5G transport.

7.2 Distributed architecture vs centralized architecture

The advent of the Internet of Things (IoT) and 5G applications renders the need for supporting both delay-tolerant and mission-critical applications in not only centralized but also distributed fashions thus it needs to integrate both centralized cloud computing and emerging Mobile-Edge Computing (MEC) with existing network infrastructures to enhance storage, processing, and caching capabilities, as shown in Figure 27. Traditionally, the centre or core network holds much of the computational power. This is the case with Cloud Computing providers, Telecoms, Internet providers, and large Enterprises. However, the situation is being changed now. For some 5G services, the network will have to deal with really high volumes of data, all at faster speeds and coming from a small geographical area. This results in decentralizing the data centre and pushing for more powerful computational resources at the network edge. Instead of sending all data to a cloud for processing, the network edge analyses, processes, and stores the data. Collecting and processing data closer to the customer reduces latency and brings real-time performance to high-bandwidth applications.

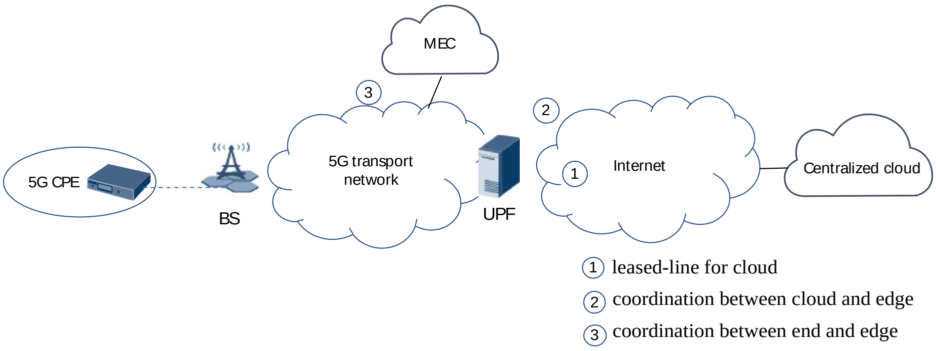


Figure 27: Distributed cloud architecture

7.3 Requirements to the 5G transport network

A given computation task may be split into several sub-tasks and then dispatched into several computation resource pools. Some may be processed in the centralized cloud, some may reside in the edge, some may run in the on-premises mini data centre. The typical cloud-related communication models include leased-line for cloud, coordination between cloud and edge, coordination between end and edge, etc. In combination with other networks, the 5G transport network provides transport services to interact.

The leased line for the cloud is designed for the enterprise customer CE to access the IT asset in the public cloud. As shown in Figure 28, leased-line for cloud is composed of several links on the network side, the link from CPE to BS, the link from BS to UPF, the link from UPF to cloud-POP, and that from cloud-POP to VPC within the cloud. The link from gNB to UPF is carried by 5G transport network. Same to the access of mobile UEs in legacy 4G network, the encapsulation protocol for the link from CE to UPF is GTP, which is an IP-based protocol suite used to carry General Packet Radio Service (GPRS) within the 3G, 4G and 5G mobile networks, and the underlay of the link is usually 5G transport network.

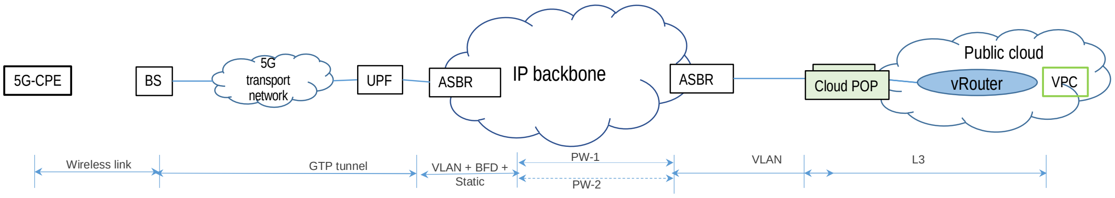


Figure 28: Leased-line to the cloud

From above, it can be noted that end-to-end cloud connections generally span over multiple networks, such as mobile core, Metro network, IP backbone and in-DC networks, etc. and 5G transport network is only one of them and provide sub-connection to the customers. In order to meet the needs of the cloud, 5G transport network will need to coordinate with other networks on an end-to-end basis.

In retrospect, the mobile transport network has experienced various network technologies such as SDH, PTN and IP RAN. The IP/MPLS technology has been widely used with the emergence of all-IP mobile base stations and large bandwidth IP/MPLS technology has been widely used. In the 5G era, cloud-based 5G 2C and 2B services require the network to provide flexible links, accurate and controllable paths, and precise resource awareness. These requirements are difficult to meet with the traditional MPLS technology. SRv6 comes into being to meet new business requirements and emerge as one choice for building a new-generation carrier-class mobile transport network.

7.4 Cloud-network coordination policies

It is evident that cloud network convergence is one of the major trends of information infrastructure, and it is shaping the whole industry globally. With more and more applications and data being moved to the cloud, the cloud will be the core of the information infrastructure sooner or later. As one part of the carrier network, 5G transport network planning and operation should follow the development of clouds, including the clouds of operators and third-party providers.

For operators, there should be cloud-network coordination policies. Due to the difference of market situation and enterprise development strategy, different operators have a further understanding of the 5G transport network, the cloud-network coordination policy of operators may differ from each other. For instance, some operators may implement 5G transport network in Metro network, i.e. the two networks share the same network physical infrastructure, some operators may build a standalone 5G transport network. Some network operators may provide cloud service, some may not, all these factors will affect Cloud-network coordination policies. Therefore, it is quite unrealistic to build a universal interconnection design between the 5G Transport Network and the Cloud Infrastructure.

7.5 IPv6 addresses planning

It is evident Data Centre will need IPv6 addresses for its own infrastructure and also for customers.

Regarding the infrastructure, the IPv6 plan follows the same rules described in clause 6.2.2.

Regarding the customer context, the common rule is to reserve one IPv6 /48 prefix and to provide to the customer the first IPv6 /56 prefix which can be split in /64 prefixes. If the customer requires more prefixes, then another /56 prefix may be allocated.

8 Conclusion

5G differentiates from its predecessors as it provides a superior quality of the experience for the end-user, higher throughput and faster connectivity. It enables innovative applications such as IoT and machine-to-machine communications, smart life, industrial communications.

To support the requirements posed by 5G applications and provide the expected experience quality, operators need to face the upgrade or restructuring of their backhaul and transport infrastructure.

A critical aspect of making the network future-proof is the adoption of IPv6 at the network layer.

Several operators worldwide have already chosen to transition their networks to IPv6-only. In addition, several countries have set their evolution plans considering IPv6 as the core network technology, opening the door to the sunset of IPv4 in the medium-term.

SRv6 complements IPv6 as it provides advanced mechanisms for fine-grain traffic steering across an IPv6 network data plane.

The combination of IPv6 and SRv6 supports the innovative 5G services, as discussed at the beginning of the present document, and their stringent network requirements. The description of a 5G backhaul and transport architecture based on IPv6 and SRv6 represents the core part of the present document. It can be considered as a high-level blueprint to be followed by operators interested in adopting a future-proof network design.

History

Document history		
V1.1.1	May 2022	Publication