Wireless
Convergence

5G Wireless Wireline Converged Core Architecture Technical Report

WR-TR-5WWC-ARCH-V03-200618

Notice

This Wireless technical report is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. You may download, copy, distribute, and reference the documents herein only for the purpose of developing products or services in accordance with such documents, and educational use. Except as granted by CableLabs® in a separate written license agreement, no license is granted to modify the documents herein (except via the Engineering Change process), or to use, copy, modify or distribute the documents for any other purpose.

This document may contain references to other documents not owned or controlled by CableLabs. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document. To the extent this document contains or refers to documents of third parties, you agree to abide by the terms of any licenses associated with such third-party documents, including open source licenses, if any.

© Cable Television Laboratories, Inc. 2019-2020

DISCLAIMER

This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	WR-TR-5WWC-ARCH-V03-200618			
Document Title:	5G Wireless Wireline Converged Core Architecture Technical Report			
Revision History:	D01 – 07/23/19 V01 – 08/20/19 V02 – 04/30/20 V03 – 06/18/20			
Date:	June 18, 2020			
Status:	~~Work in Progress~~	~~Draft~~	**Released**	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	**Public**

Trademarks

Contents

Figures

Tables

1 SCOPE

1.1 Motivations for Convergence

Operators compete across industries to provide revenue-generating services to their subscribers. Mobile operators are purchasing content and wireline assets, and MSOs are launching or expanding mobile services. The ecosystem response includes exploring the convergence of services, policy, and networks across wireless and wireline domains. The 3GPP R16 5G mobile core includes Wireless Wireline convergence requirements as documented in [3GPP 23.316] Other industry groups such as the Next Generation Mobile Network (NGMN) Alliance, Wireless Broadband Alliance (WBA), and Broadband Forum (BBF) also have active work in convergence. (See the references [BBF 5GC], [WBA 5G], and [WBA RAN].) To help address the question of whether CableLabs members can benefit from these ecosystem trends towards converged core networks, this document summarizes work within CableLabs and the MSOs on converged cores for wireline and wireless networks. It also identifies requirements for interworking between the 5G core (5GC) and hybrid fiber-coax (HFC) networks.

There are multiple potential motivations for the convergence of core networks supporting wireline and wireless access. Convergence can be a method to offer end-to-end network slices tailored to growing enterprise and vertical markets. Convergence may be a strategic initiative, in which the network evolves towards convergence over time in incremental steps. A converged core may be able to avoid overlapping functions within the network and therefore reduce long-term capital expenditures or operating expenses (CAPEX or OPEX). For example, operators may deploy a converged subscription store rather than a subscription store per access. Convergence may also enable operators to deliver services and execute policy more consistently. Operators have identified several use cases that a converged core must support, as described in Section 8 of this document.

1.2 Elements of Convergence

Motivations for convergence can lead to several initiatives:

- convergence of services and applications,
- convergence of policy, and
- convergence of core networking.

A convergence of services, applications, and policy is essential to the delivery of a consistent user experience regardless of access network. To this end, operators need to have methods to service each user device, including devices behind the residential gateway. Otherwise, convergence may be incomplete, with variable service and segmented policy. (Note that services to Internet of things [IoT] devices are identified for future work.)

3GPP, the BBF, and CableLabs are considering convergence aspects at the core networking layer, an important step towards a complete converged architecture. This level of convergence concerns topics such as subscriptions for network access and policy for traffic management within the mobile core network. 3GPP release 16 addresses this level of core convergence in support of a residential gateway (RG). The scope of this work is focused on linking the RG to the 5GC. It does not provide a complete solution for delivering services to individual devices in the home, but that may be a topic for future work.

Certain stakeholders are considering over-the-top approaches to deliver services and policies to subscriber devices regardless of wireline or wireless access network. This strategy may allow operators to deploy converged services and policy with less dependency upon standards initiatives oriented to specific access networks or without bias towards one access network over another. The Apple ecosystem might be considered an example of a non-standard over-the-top convergence play, achieving a consistent service policy and experience delivery regardless of access network (Wi-Fi vs LTE) serving the iPhone. A forum to develop over-the-top convergence has not yet emerged.

1.3 Scope of This Release

The present scope of this technical report is focused on core convergence leveraging the 3GPP R16 5G converged core network specifications, particularly the convergence requirements for interworking between the 3GPP R16 5G mobile core and the HFC access network.

- Section 5 identifies architectures for convergence.
- Sections 6 and 7 include focus areas and requirements for convergence.
- Section 8 describes member use cases for convergence, which are mapped to convergence requirements in Section 9.
- Section 9 maps use cases to requirements contained in 3GPP specifications and this document. Gaps in 3GPP specifications to support the use cases are also identified.
- Section 10 identifies areas for future work.
- Section 11 describes CableLabs engagement in the 3GPP wireless-wireline convergence work item.

2 REFERENCES

This report uses the following informative references. References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific. For a non-specific reference, the latest version applies.

[3GPP 23.316]	3GPP Technical Specification 23.316, Wireless and Wireline Convergence Access Support for the 5G System (5GS)
[3GPP 23.501]	3GPP Technical Specification 23.501, System Architecture for the 5G System (5GS)
[3GPP 23.502]	3GPP Technical Specification 23.502, Procedures for the 5G System (5GS)
[3GPP 23.503]	3GPP Technical Specification 23.503, Policy and Charging Control Framework for the 5G System (5GS); Stage 2
[3GPP 24.501]	3GPP Technical Specification 24.501, Non-Access-Stratum (NAS) Protocol for 5G System (5GS); Stage 3
[3GPP 26.441]	3GPP Technical Specification 26.441, Codec for Enhanced Voice Services (EVS); General overview
[3GPP 26.891]	3GPP Technical Report 26.891, 5G Enhanced Mobile Broadband; Media Distribution
[3GPP 29.500]	3GPP Technical Specification 29.500, 5G System; Technical Realization of Service Based Architecture; Stage 3
[3GPP 29.503]	3GPP Technical Specification 29.503, 5G System; Unified Data Management Services; Stage 3
[3GPP 29.507]	3GPP Technical Specification 29.507, 5G System; Access and Mobility Policy Control Service; Stage 3
[3GPP 29.512]	3GPP Technical Specification 29.512, 5G System; Session Management Policy Control Service; Stage 3
[3GPP 29.531]	3GPP Technical Specification 29.531, 5G System; Network Slice Selection Services; Stage 3
[3GPP 38.413]	3GPP Technical Specification 38.413, NG-RAN; NG Application Protocol (NGAP)
[3GPP 38.414]	3GPP Technical Specification 38.414, NG-RAN; NG Data Transport
[BBF 5GC]	BBF 5G Fixed Mobile Convergence White Paper, submitted to 3GPP and available for download here: https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_129BIS_West_Palm_Beach/Docs/S2-1811672.zip
[WBA 5G]	Wireless Broadband Alliance, Unlicensed Integration with 5G Networks, October 2018, https://wballiance.com/wp-content/uploads/2018/10/Unlicensed-Integration-with-5G-Networks.pdf
[WBA RAN]	Wireless Broadband Alliance, RAN Convergence, January 2019, https://wballiance.com/wp-content/uploads/2019/01/RAN-Convergence-Paper-2019.pdf
[MULPIv3.1]	DOCSIS® 3.1 MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.1-I20-200407, April 7, 2020, Cable Television Laboratories, Inc.
[PCMM]	PacketCable™ Multimedia Specification, PKT-SP-MM-C01-191120, November 20, 2019, Cable Television Laboratories, Inc.
[MANO]	ETSI Group Specification (GS) NFV-MAN 001, Network Functions Virtualisations (NFV); Management and Orchestration
[LLX]	Low Latency Mobile Xhaul over DOCSIS® Technology Specification, CM-SP-LLX-I01-190628, June 28, 2019, Cable Television Laboratories, Inc.
[SEC]	DOCSIS 3.1, Security Specification, CM-SP-SECv3.1-I09-200407, April 7, 2020, Cable Television Laboratories, Inc.

2.1 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; http://www.cablelabs.com
- Internet Engineering Task Force (IETF) Secretariat, 46000 Center Oak Plaza, Sterling, VA 20166, Phone +1-571-434-3500, Fax +1-571-434-3535, http://www.ietf.org
- 3GPP, www.3GPP.org
- Broadband Forum (BBF), https://www.broadband-forum.org/
- Wireless Broadband Alliance (WBA), https://www.wballiance.com/

3 TERMS AND DEFINITIONS

This document uses the following terms.

5G UE Mobile Device	5G User Equipment Mobile Device as defined in [3GPP 23.501].
Broadband User Device	User device in the home network with only broadband Internet connectivity via the HFC network.
Femtocell	Small low-power cellular base station connected to the service provider's network via a broadband Internet connection either in a home network or in a small business network. It does not typically support all of the mobility handover/handoff functions that a small cell supports.
HFC Node	[MULPIv3.1]defines the Fiber Node as a point of interface between a fiber trunk and the coaxial distribution in the HFC wireline network. The term HFC Node in [3GPP 23.316] refers to the Fiber Node used in HFC networks.
Integration Model	The wireline customer premises equipment (CPE) appears as a user-equipment signaling endpoint to the 5G mobile core, supporting the potential of a single core network to serve HFC, Wi-Fi, LTE, and 5G NR networks. See [3GPP 23.316]
Interworking Model	Interworking between the HFC network and 5G mobile core is placed within the network, allowing legacy customer premises equipment (CPE) to operate with a converged core network. See [3GPP 23.316]
Small Cell	Small low-power cellular radio access node that operates in licensed and unlicensed spectrum connected to service provider's network via broadband Internet connection in a home network or in a small business network.

4 ABBREVIATIONS AND ACRONYMS

This document uses the following abbreviations.

5G-CRG	5G Cable Residential Gateway
5GC	5G Core
5GCAN	5G Cable Access Network
5QI	5G QoS Identifier
AF	Application Function
AGF	Access Gateway Function
AKA	Authentication and Key Agreement
AMBR	Aggregate Maximum Bit Rate
AMF	Access and Mobility Management Function
AN	access network
AP	access point
ARP	Allocation and Retention Priority
ATSSS	Access Traffic Steering, Switching, and Splitting
BWR	Bandwidth Report
CCAP	Converged Cable Access Platform
CDN	content delivery network
CHF	charging function
CM	cable modem
CMTS	cable modem termination system
COPS	Common Open Policy Service [Protocol]
CP	control plane
CPE	customer premises equipment
CRG	Cable Residential Gateway
CS	circuit switched
DL	downlink
DNAI	Data Network Access Identifier
DNN	Data Network Name
EAP	Extensible Authentication Protocol
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunneled Transport Layer Security
eDVA	embedded digital voice adapter
eMBB	enhanced mobile broadband
eMTA	embedded multimedia terminal adaptor
FN-CRG	Fixed Network Cable Residential Gateway
FN-FRG	Fixed Network Fiber Residential Gateway
GBR	guaranteed bit rate
GCI	Global Cable Identifier
GFBR	guaranteed flow bit rate
GPRS	General Packet Radio Service
GPSI	Generic Public Subscription Identifier

GTP	GPRS Tunneling Protocol
HFC	hybrid fiber-coax
ID	identifier
IGMP	Internet Group Management Protocol
IMEI	International Mobile Equipment Identifier
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IoT	Internet of things
IP	Internet Protocol
IPTV	IP television
LAN	local area network
LTE	Long Term Evolution
MA PDU	Multi-Access PDU
MAC	Media Access Control
MIoT	massive Internet of things
MSO	multiple system operator
N5GC	Non-5G Capable
NAS	Non-Access Stratum
NFV	network function virtualization
NGAP	Next Generation Application Protocol
NR	New Radio
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
N3IWF	Non-3GPP InterWorking Function
ONU	Optical Network Unit
OLT	Optical Line Terminal
PCC	Policy and Charging Control
PCF	Policy and Control Function
PCMM	PacketCable Multimedia
PCRF	Policy and Charging Rules Function
PDB	Packet Delay Budget
PDU	Packet Data Unit
PEI	Permanent Equipment Identifier
PFCP	Packet Forwarding Control Protocol
PHY	physical
PLMN	Public Land Mobile Network
PS	packet switched
QNC	QoS Notification Control
QoS	quality of service
RAN	radio access network
RAT	Radio Access Technology
REST	Representational State Transfer

RFSP	Radio Frequency Selection Priority
RG	residential gateway
RG-LWAC	RG Level Wireline Access Characteristics
Rx	receiver
SBI	Service Based Interface
SCTP	Stream Control Transmission Protocol
SDN	software-defined networking
SIM	subscriber identity module
SIP	Session Initiation Protocol
SM	session management
SMF	Session Management Function
SSC	session and service continuity
SST	Slice Service Type
STB	set-top box
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TCP	Transmission Control Protocol
TDD	time-division duplex
TLS	Transport Layer Security
UDM	Unified Data Management
TR	Technical Report
UDP	User Datagram Protocol
UE	user equipment
UL	uplink
UP	user plane
UPF	User Plane Function
URLLC	ultra-reliable low-latency communications
URSP	UE Route Selection Policy
VLAN	virtual LAN
VOD	video on demand
VoLTE	Voice over LTE
Vo5G	Voice over 5G
VPN	virtual private network
vRAN	virtual RAN
vSRVCC	Single Radio Video Call Continuity
W-AGF	Wireline Access Gateway Function
W-CP	Wireline Control Protocol
WAG	wireline access gateway
WAN	wireline access network

5 CONVERGED ARCHITECTURE WITH THE 3GPP 5G CORE

Three 3GPP architectural models for convergence are considered in this document:

- 3GPP R16 interworking model of converged architecture as defined in [3GPP 23.316],
- 3GPP R16 integration model of converged architecture as defined in [3GPP 23.316], and
- Bridged residential gateway (RG) with convergence of services and policy to devices behind the RG.

3GPP has identified reference architecture diagrams for the interworking and integration models of convergence; they are shown in Figure 1 and Figure 2, respectively. The following hybrid fiber-coax (HFC) network components are portrayed in the 3GPP reference architectures.

The FN-CRG (Fixed Network Cable Residential Gateway) is, at minimum, the Cable Modem (CM) customer premises equipment (CPE). It may include a Wi-Fi Access Point (AP), a voice eMTA (embedded multimedia terminal adapter), or a video set-top box (STB), but the primary focus is to provide an HFC-based broadband Internet service. The FN-CRG, which is part of the home network, may include a Wi-Fi AP/Router. The home network may include a Next-Generation Radio Access Network (NG-RAN) unit to receive and transmit signals from and to 5G user devices.

The FN-FRG (Fixed Network Fiber Residential Gateway) is, at minimum, the Optical Network Unit (ONU). It may include a Wi-Fi AP, a Wi-Fi Router, or a voice eMTA with the primary focus to provide a Passive Optical Network (PON) broadband Internet service. The FN-FRG, which is part of the home network, may include a Wi-Fi AP/Router. The home network may include a NG-RAN unit to receive and transmit signals from and to 5G user devices.   The 3GPP specifications need to be updated to include the FN-FRG converged architecture in a future release.

The 5G-CRG (5G Cable Residential Gateway) adds the 3GPP 5G control plane to the 5G-CRG so that the 5G-CRG appears as both a 5G user equipment (UE) and an HFC FN-CRG. Certain operators may decide to integrate the 5G UE and FN-CRG into a single unit that can be configured by a unified management system. Other operators will be motivated to deploy 5G-CRGs where the 5G UE portion is implemented separately from the FN-CRG. In this case, the FN-CRG may be placed in bridged configuration. This modular implementation approach allows provisioning and management systems of the 5G UE and FN-CRG to remain separate and independent from each other.

The W-AGF (Wireline Access Gateway Function), as identified by 3GPP, is a layer of interworking capabilities between the HFC network and the 5G mobile core infrastructure.

5.1 3GPP R16 Interworking Model for 5G Converged Architecture

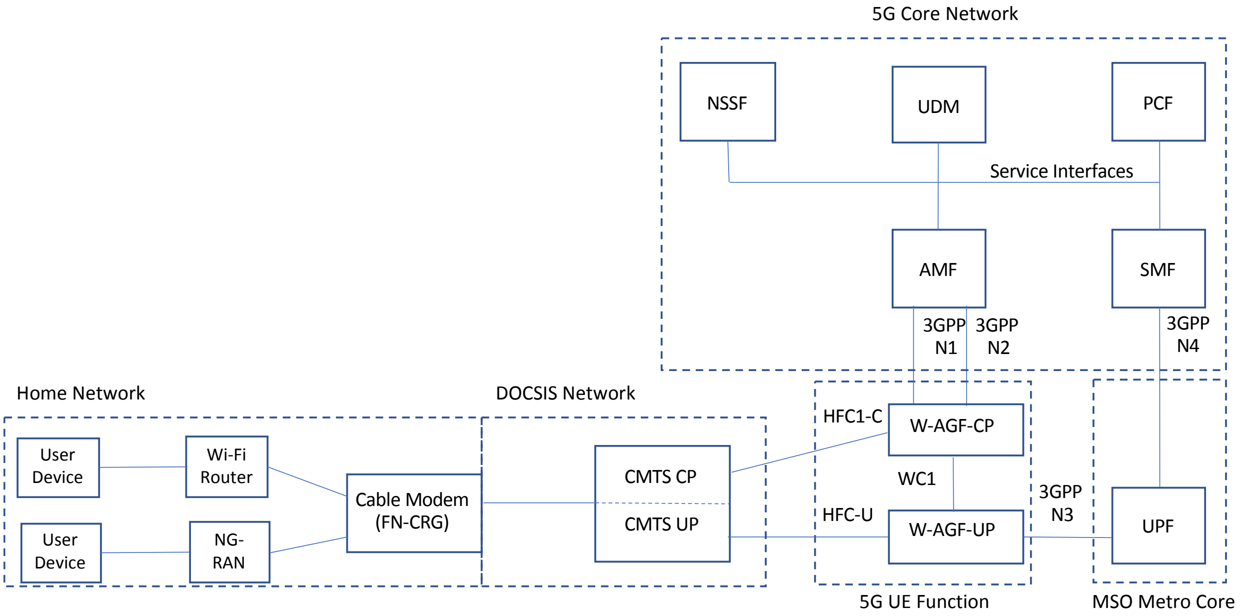


Figure 1 - Interworking Model Block Diagram of 5G Converged Architecture

The Interworking Model for legacy Cable Modems (i.e., FN-CRG) in the 5G converged network architecture is depicted in Figure 1. The 5G converged architecture is the convergence of three separate networks, namely, the 5G core network (5GC), the DOCSIS network, and the home network. This model places the interworking and translation functions, specifically the W-AGF-CP/UP, between the 5GC and the DOCSIS network. The FN-CRG, which is part of the home network, may include a Wi-Fi AP or Wi-Fi Router. A Next-Generation RAN (NG-RAN) unit, which is connected to the FN-CRG, is used to transmit and receive signals from and to the 5G user devices. There is no impact to deployed FN-CRGs, the CMTS, and there is no change to FN-CRG authentication and network admission. This method provides a means for operators who manage mobile networks to immediately realize benefits from a shared core while using legacy CMs and CMTSs. It also provides an orderly migration step towards the integrated model of convergence described in Section 5.2.

The W-AGF communicates to the Access and Mobility Management Function (AMF) over the 3GPP N1 and 3GPP N2 reference points per [3GPP 23.501]. The N1 reference point supports 5G UE Function authentication and network admission signaling, with the 3GPP Non-Access Stratum (NAS) protocol profiled for FN-CRGs. The N2 reference point to the AMF carries access network control messaging as specified by 3GPP. This control messaging is translated by the interfaces between the W-AGF in order to interoperate with existing interfaces on the CMTS. The W-AGF network also needs to support an N3 user plane (UP) reference point (also per [3GPP 23.501]) to the User Plane Function (UPF), which requires 3GPP-specified tunneling. The UPF is typically located at the MSO's core network. The user plane between the CMTS and W-AGF-UP uses an existing interface on the CMTS. Operators may configure the interface between CMTS and W-AGF-UP as a layer 2 path to switch traffic to CMs. The W-AGF acts as a 5G UE Function on behalf of the FN-CRG in the interworking model. It manages registration into the 5GC, data session management, and slice selection on behalf of the FN-CRG. Note that there is a 5G UE Function for every supported FN-CRG CPE.

The CMTS CP interfaces to the W-AGF-CP via an HFC1-C interface using existing high-speed WAN interface. To achieve interoperability among multiple CMTS vendors and the adoption by the MSOs, the HFC1-C interface requirements should be standardized, although it may include vendor-proprietary protocols and interfaces in initial deployments. This means the convergence interworking layer interface requirements between the W-AGF and the CMTS needs to be defined, standardized, and tested, whereas the interfaces to the 3GPP 5GC are open-standard interfaces capable of multi-vendor interoperability. Some of these requirements are placed upon the interworking layer interfaces throughout this document. References to 3GPP specifications are made for 5GC interfaces and capabilities.

5.2 3GPP R16 Integration Model for 5G Converged Architecture

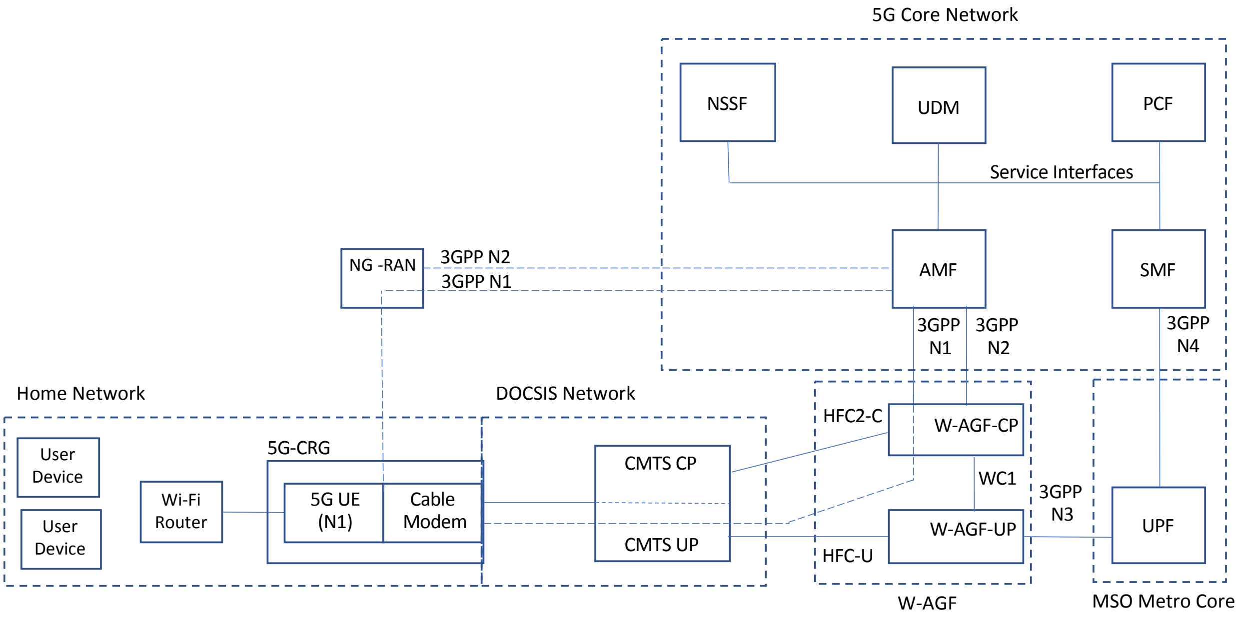


Figure 2 - Integration Model Block Diagram for 5G Converged Network Architecture

The Integration Model for 5G-CRG CPE in the 5G converged network architecture is depicted in Figure 2. The 5G converged architecture is the convergence of three separate networks, namely, the 5G core network (5GC), the DOCSIS network, and the home network. This model places 3GPP 5G network functions throughout the DOCSIS access network in order to support the promise of a single core across multiple access networks. The 5G-CRG appears as a 5G UE to the 5GC. The 5G-CRG CPE integrates the 5G UE and the CM functionality. A NG-RAN unit, which may be located either outside or inside the home, is used to transmit and receive signals from 5G user devices. The 5G UE functions may be implemented separately from the CM so that 5G and CM provisioning and management systems can remain separate. Alternatively, operators may choose to deploy 5G-CRGs that integrate the 5G UE and CM functionality.

In one use case, the Integration Model provides a hybrid access for the 5G-CRG to connect to the AMF via the NG-RAN using 3GPP N1 air interface, and via a wireline using the DOCSIS network as shown in Figure 2. The 5G-CRG can aggregate the bandwidth of both the wireless and wireline networks in a single multi-access PDU session, and transmit simultaneously PDUs to both networks using Multipath TCP (MPTCP). In another use case (not shown in Figure 2), the NG-RAN is connected to the 5G-CRG in the home network, and the 5G-CRG is using the wireline access for PDUs transmission. Although the integration model is better prepared to support a fuller range of 3GPP features, it is much more challenging to implement than the Interworking Model. The 5G control plane (CP) (the N1 interface per [3GPP 23.501]) is transported transparently through the wireline network to the 5GC. The UPF is typically located at the MSO's core network.

The CMTS CP interfaces to the W-AGF-CP via HFC2-C interface using existing high-speed WAN interface. To achieve interoperability among multiple CMTS vendors and the adoption by the MSOs, the HFC2-C interface should be standardized, although it may include vendor-proprietary protocols and interfaces in initial deployments. This means the convergence interworking layer interface requirements between the W-AGF and the CMTS needs to be defined, standardized, and tested, whereas the interfaces to the 3GPP 5GC are open-standard interfaces capable of multi-vendor interoperability. Some of these requirements are placed upon the interworking layer interfaces throughout this document. References to 3GPP specifications are made for 5GC interfaces and capabilities.

5.3 Protocol Stacks for 5G Converged Architecture

The goal of this section is to illustrate the control and user planes' protocol stacks with the 3GPP reference points for both the Interworking and Integration Models. Figure 3 illustrates the interworking model control plane's protocol stacks on the 3GPP reference points for 5G converged network architecture. DOCSIS protocol packets are transported over the HFC network from the FN-CRG to the CMTS. All the control plane traffic to the W-AGF is transmitted from the CMTS over IP layer, in compliance with the HFC1-C interface requirements. The 3GPP Non-Access Stratum (NAS) protocol is used to convey non-radio signaling between the W-AGF and the AMF. In this model, the W-AGF is required to support N2 reference point, which includes the 3GPP NGAP protocol.

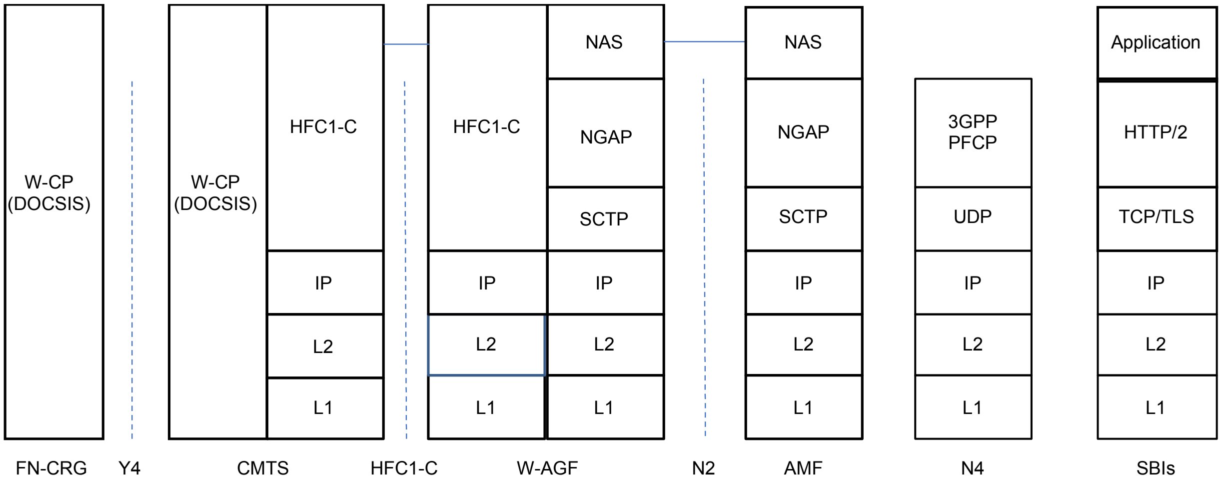


Figure 3 - Interworking Model Control Plane Protocol Stacks for 5G Converged Network Architecture

Figure 4 illustrates the Integration Model control plane's protocol stacks on 3GPP reference points for 5G converged network architecture. All the DOCSIS protocol packets are transported from the 5G-CRG over the HFC network to the CMTS similarly to the interworking model. The 3GPP NAS protocol is supported by the 5G-CRG CM and is transported through the HFC network to the W-AGF and the 3GPP AMF. The NAS protocol is encapsulated in EAP-5G (identified in [3GPP 23.501]) over the DOCSIS protocol until the 5G-CRG is authenticated. After a security association is established, the NAS protocol is carried over TLS between the 5G-CRG and the W-AGF. The combined use of EAP-5G over the DOCSIS protocol and TLS is depicted as the Wireline Control Protocol (W-CP) in Figure 4. See [3GPP 23.316] for a detailed message flow of the process and protocols. The N1 reference point includes the 3GPP NAS protocol. As in the Interworking Model, the Integration Model requires the W-AGF to support the N2 reference point that includes the 3GPP NGAP protocol. The N3 UP reference point employs 3GPP GTP tunneling between the W-AGF and the UPF. The N4 CP-to-UP interface employs 3GPP-defined Packet Forwarding Control Protocol (PFCP). The Service Based Interfaces (SBIs) in the 5GC are specified between the AMF, PCF (Policy and Control Function), and SMF (Session Management Function).

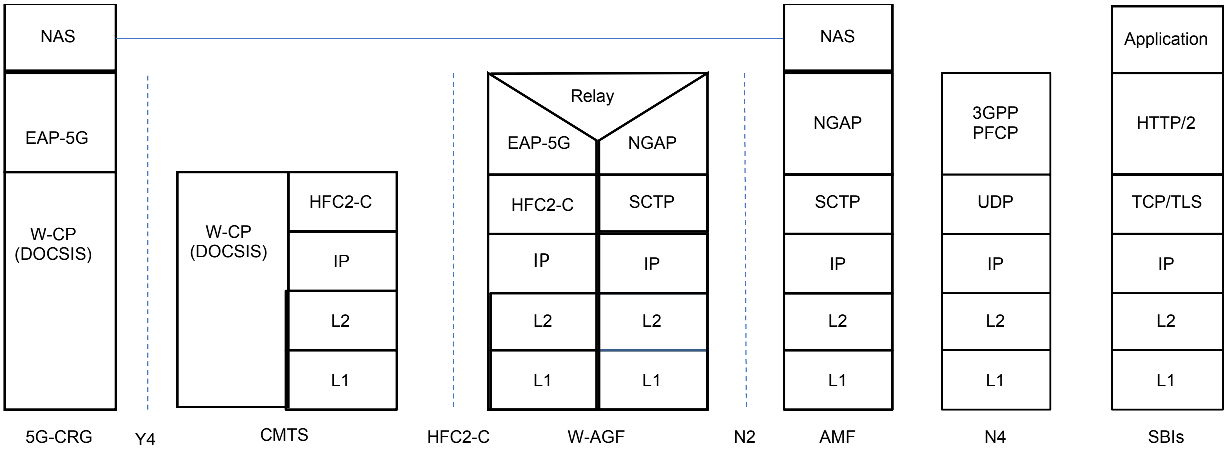


Figure 4 - Integration Model Control Plane Protocol Stacks for 5G Converged Network Architecture

Figure 5 illustrates the Interworking and Integration Models' user plane protocol stack on 3GPP reference points for the 5G converged network architecture. The most widely-deployed FN-CRG includes an IP layer to support voice applications. In addition, the 5G-CRG includes 3GPP UE IP layer that may be tunneled to the W-AGF. User plane traffic on the CMTS can be tunneled to the W-AGF using L3TP over the HFC-U interface.

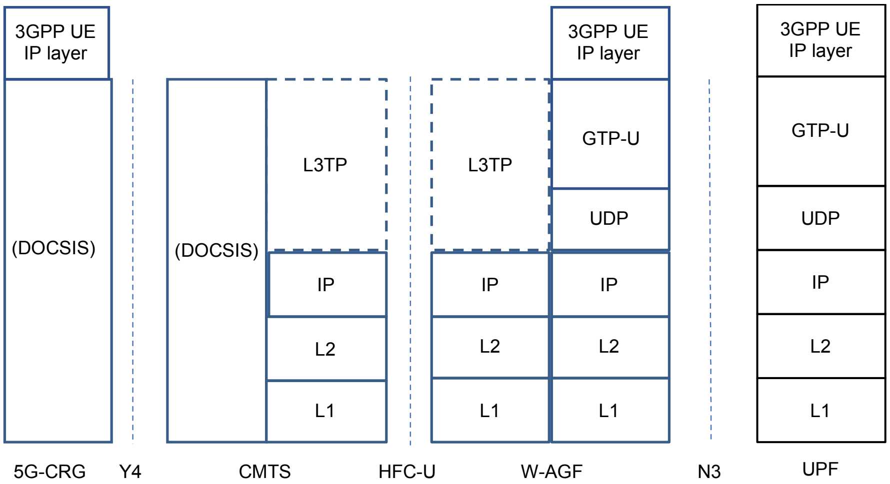


Figure 5 - User Plane Protocol Stacks for 5G Converged Network Architecture

5.4 Bridged CRG for Converged 5GC Network with DOCSIS Network

Figure 6 below illustrates the bridged CRG in the home network connected to a 5GC network via an HFC network architecture with DOCSIS protocol. This bridged CRG architecture provides converged services and policy for user devices located in the home network. Devices behind the bridged CRG that are served by the 5GC are referred to by 3GPP as N5GC devices. See section 4.10a of [3GPP 23.316]. The CRG, which may take the form of the FN-CRG or 5G-CRG, operates in bridged mode as part of a strategy to support the 5G converged core by applying policy, addressing, and services to individual devices. Layer 2 traffic is sent between the user devices in the home network and 5G UPF via the bridged CRG and HFC network. See [3GPP 23.316] for the registration of user devices into the 5G core. The CMTS as well can be configured for layer two traffic forwarding per operator configuration. The UPF, which is typically located at the MSO's core network, assists in providing visibility of user devices in the 5GC with access router functions. In this way, the 5GC can help assign IP addresses to the user devices. Policy can be applied to each user device via the PCF and SMF control at the UPF. Applications can also influence traffic management to the user devices via the SMF. Converged 5G CP and UP services to both mobile devices and local devices in the home network are delivered via the bridged CRG. It should be pointed out that there is a 5G UE Function for every supported bridged FN-CRG CPE.

Several enhancements to the R16 converged 5GC are needed to realize this architecture as follows:

1. Procedures to admit and connect widely available user devices that do not necessarily support 3GPP credentials or 3GPP signaling, such as Wi-Fi-only laptops, into the 5GC.
2. Procedures for traffic priority (QoS) and management for widely available user devices via the 5GC.
3. Procedures to apply converged policy to user devices with a common policy platform for mobile and fixed network user devices.

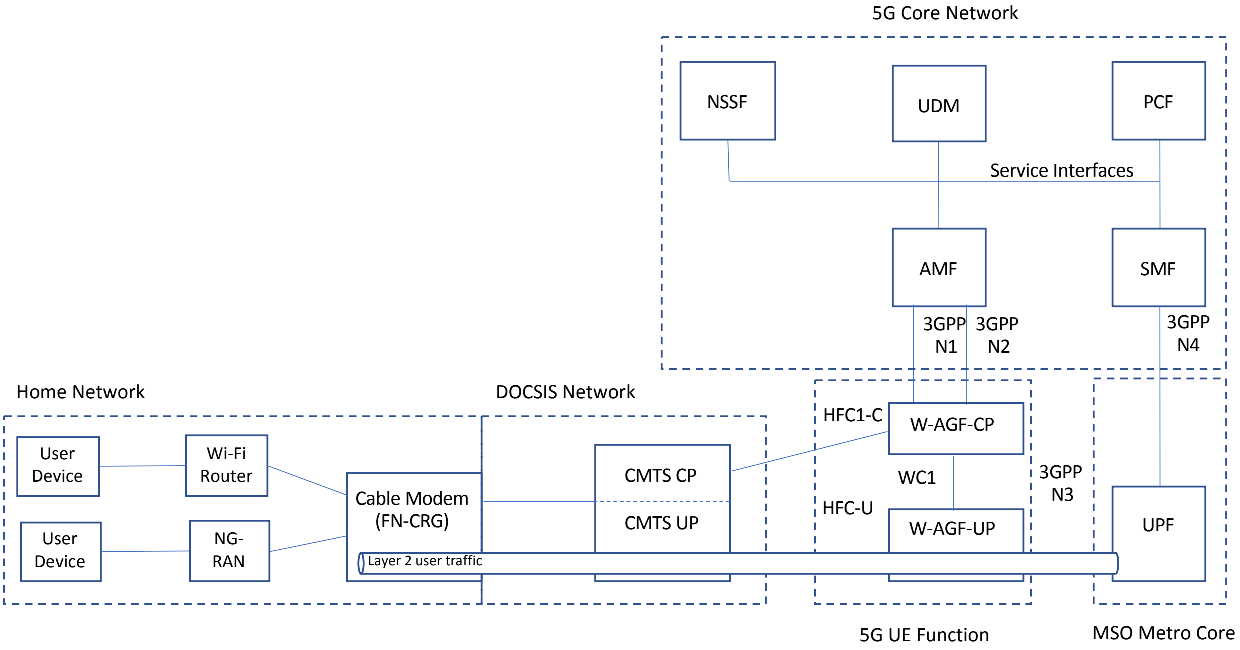


Figure 6 - Bridged CRG for Converged DOCSIS Network with 5GCore Network Architecture

5.5 Bridged CRG for Converged 5GC Network with PON Network

Figure 7 below illustrates the bridged RG in the home network connected to a 5GC network via a Passive Optical Network (PON) architecture. This bridged Fixed Network Fiber Residential Gateway, FN-FRG, architecture, which is missing from the [3GPP 23.316] v16.2.0 technical specification, provides converged services and policy for user devices located in the home network. The Optical Line Terminal (OLT), which is typically located at the MSOs headend, replaces the CMTS shown in Figure 6, and the Optical Network Unit (ONU) is located at the home network, which is at the edge of the PON network. The RG, which may take the form of an FN-FRG (i.e., ONU) or 5G Fiber Residential Gateway, 5G-FRG, operates in bridged mode as part of a strategy to support the 5G converged core by applying policy, addressing, and services to individual devices.

The PON architecture below supports both Ethernet PON (EPON) based on the IEEE 802.3av standard, and Gigabit-capable PON (GPON) based on the ITU-T G.984 set of standards. DOCSIS provisioning over Ethernet version 2 (DPoEv2) is used to provide DOCSIS provisioning and management for the bridged ONU in EPON architecture deployments. For GPON deployments, ITU-T G.984 based management and control system is used for the bridged ONU. Layer 2 traffic is sent from the user devices in the home network and 5G UPF, which is typically located at the MSO's core network, via the bridged FN-FRG using the Optical Node User 1 (ON1-U) interface for EPON architecture and ON2-U interface for GPON architecture at the OLT. The control and/or management messages from the bridged FN-FRG to the 5GC network are transmitted via ON1-C interface for EPON architecture, and ON2-C for GPON architecture as shown in Figure 7. The OLT can be configured for layer two traffic forwarding per operator configuration.

Several enhancements to the R16 converged 5GC are needed to realize this architecture as follows:

1. Procedures to admit and connect widely available user devices that do not necessarily support 3GPP credentials or 3GPP signaling, such as Wi-Fi-only laptops, into the 5GC.
2. Procedures for traffic priority (QoS) and management for widely available user devices via the 5GC.
3. Procedures to apply converged policy to user devices with a common policy platform for mobile and fixed network user devices.

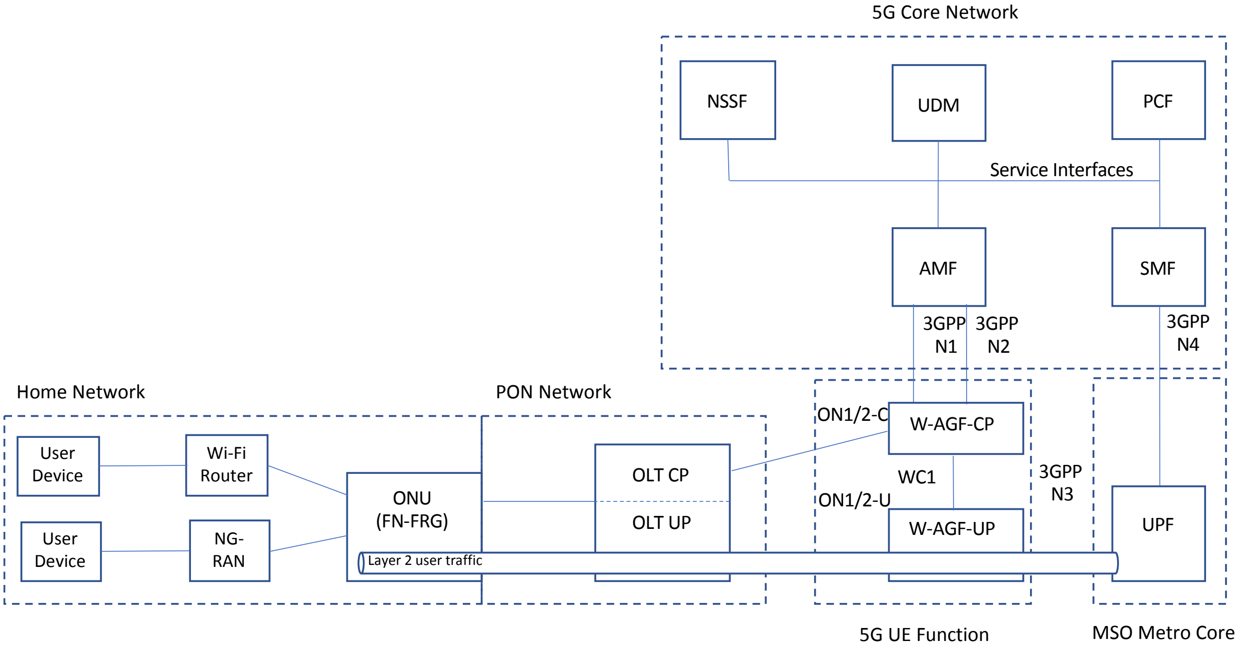


Figure 7 - Bridged FN-FRG for Converged PON Network with 5GC Network Architecture

6 CONVERGENCE FOCUS AREAS

6.1 Subscriptions, Authentication, and Admission

The following subsections describe converged subscriptions, which are held within the 5GC Unified Data Management (UDM) network element.

6.1.1 Integration Model Subscription

Wireline CPE appears as 3GPP UEs to the 5GC within the integration model of convergence. More specifically, a wireline CPE that also supports a 3GPP air interface is assigned an International Mobile Subscriber Identity (IMSI) subscription ID and subscription profile, supports Authentication and Key Agreement (AKA) authentication procedures, and is subject to network admission processes similar to the 3GPP UE. The combination of wireline and 3GPP air interfaces is known as a hybrid CPE configuration. A wireline-only CPE may support a variety of operator-determined EAP methods within 3GPP NAS signaling.

The service set reflected in the CPE subscription is relevant to wireline applications such as HFC broadband Internet. Fixed-line voice may leverage the same IP Multimedia Subsystem (IMS) and application subscription elements as Voice over 5G (Vo5G), but this will require eMTA and IMS application server updates from legacy PacketCable systems.

The detailed integrated model subscription profile for wireline CPE is contained within 3GPP R16 specifications.

6.1.2 Interworking Model Subscription

The converged subscription within the UDM for the interworking model links HFC legacy subscription parameters with 5G New Radio (NR) subscriptions. Whereas a mobile 5G NR subscription supports a single person or device, an HFC legacy subscription typically supports a household or enterprise. Therefore, a converged subscription for the interworking model may need to link multiple mobile subscriptions to a single HFC subscription to provide a consistent set of services and user experience across wireline and wireless access networks. Figure 8 illustrates a single HFC subscription being linked to multiple mobile device subscriptions. The wireline portion includes HFC broadband Internet and IPTV (IP television) portions. 3GPP specification [3GPP 23.316] refers to a Global Cable Identifier, which contains an HFC_Identifier. The HFC_Identifier is typically the CM MAC address per [MULPIv3.1], and is unique within an operator's network. The HFC_Identifier combined with the operator realm in Network Access Identifier format are used to construct the 3GPP Subscription Permanent Identity (SUPI) for wireline only CPE as defined in [3GPP 23.316]. When a CM is authenticated, initialized, and admitted for service using legacy methods, the CM MAC address is listed as registered in the UDM. Similarly, when an STB is authenticated, initialized, and admitted for service using legacy methods, the STB MAC address is listed as registered in the UDM.

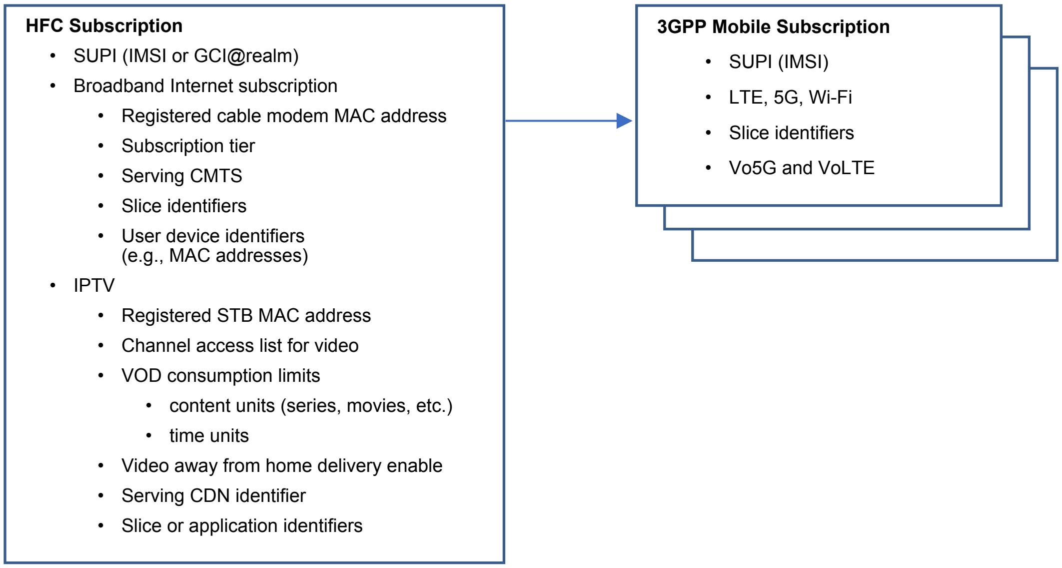


Figure 8 - Subscription Attributes for Convergence Interworking

User devices within the home may also be linked to an HFC subscription for their active registration period. Devices may be identified by MAC addresses or operator-determined credentials. These device identifiers persist across CM registrations only if they are registered into the 5GC by the operator or via a subscriber portal.

Profiles for 5G NR, LTE, and Wi-Fi are contained in the mobile subscription(s), which may be linked to an HFC subscription for the same account. The cellular subscription profile is defined in 3GPP specifications for the UDM and subscription data model.

Figure 9 provides a high-level illustration of the FN-CRG (i.e., CM) registration process with the 5GC network. Not all protocol message responses and error conditions are illustrated in the message sequence diagram. See [3GPP 23.316] section 7.2.1.3 and associated procedures in [3GPP 23.502] for a more detailed description of the messaging sequence in the mobile core. Legacy CM and CMTS processes are used to admit the CM onto the network. The high-level message sequence diagram is described below.

1. The CM reset configuration file is applied
2. The CM is authenticated and admitted onto the DOCSIS network using DOCSIS admission procedures.
3. A default DOCSIS service flow is established (i.e., SFID) and becomes active for the CM to support broadband Internet service.
4. The W-AGF detects that the CM is admitted onto the DOCSIS network (The W-AGF detection mechanism details are vendor specific, and haven’t been standardized yet).
5. The W-AGF sends a mobile core registration request to the AMF
6. The AMF posts the CM registration into the UDM using Nudm_UECM registration message with SUPI=HFC_ID and requests the CM subscription data
7. The CM subscription data is sent to the AMF using Nudm_SubscriptionData_UpdateNotify response message; it may include subscription tiers, network slice ID, or other HFC subscription info.
8. The AMF may optionally request policy information from the PCF using Npcf_request policy message.
9. If requested by the AMF, the PCF sends the requested policy information using Npcf_policy response message.
10. The AMF sends a registration accept to the W-AGF. Authorized network slice IDs may be included.

11. The W-AGF sends the DOCSIS service flow updates as needed to the CMTS based upon the information provided in the registration accept.
12. The CM receives the updates to its DOCSIS service flows from the CMTS.

The result of a successful CM registration is admission of the CM into the converged DOCSIS and 5GC network. A DOCSIS service flow is established for wireline user traffic.

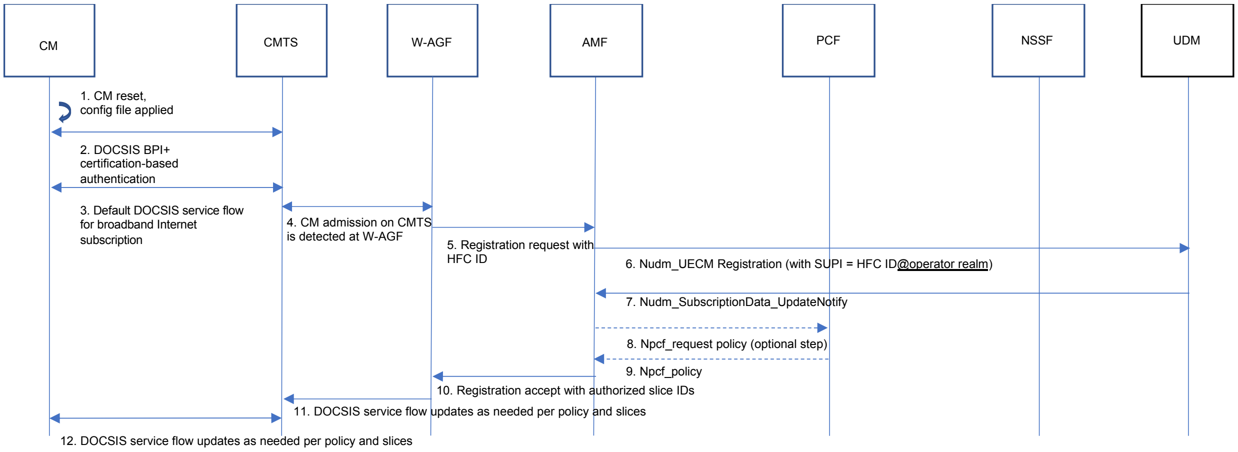


Figure 9 - High-Level Cable Modem Registration Message Flow

6.1.2.1 Voice Services and the Interworking Model

Legacy PacketCable 1.5 and PacketCable 2.0 (IMS) systems use call models and telephony feature sets that are different from those used in Voice over LTE (VoLTE) or Vo5G systems. The PacketCable 2.0 system leverages the 3GPP IMS core components with a PacketCable 2.0-specific Telephony Application Server and eMTA (eDVA, embedded digital voice adapter). Therefore, a single IMS set of core SIP proxies might be leveraged across Vo5G and PacketCable 2.0 systems. However, legacy PacketCable 2.0 CPE will still need to be supported with the PacketCable 2.0 application server. Certain vendor products may be able to execute both PacketCable 2.0 and Vo5G features on a single IMS platform.

6.2 Traffic Bonding and Traffic Switching

6.2.1 3GPP ATSSS, Hybrid Devices, and Hybrid CPE

This section describes the establishment of data sessions capable of supporting traffic bonding and traffic switching among access networks. This process can include scenarios in which traffic flows are delivered to the subscriber device over HFC and 5G NR network segments to a hybrid CPE that incorporates both a CM and 3GPP NR. Operators may also choose to use ATSSS (Access Traffic Steering, Switching, and Splitting) to aggregate 5G NR and Wi-Fi traffic flows on an ATSSS-capable mobile device and to use ATSSS traffic switching to provide highly available services to hybrid CPE. ATSSS, a 3GPP 5GC feature, is used as the basis for traffic flow management in these multi-segment scenarios. Per 3GPP specifications, the ATSSS feature is executed by a single SMF and UPF combination to manage the multiple traffic legs over wireless and wireline networks. The ATSSS feature will require the HFC access network to interface to an SMF and UPF that also interface to the 5G NR network. The ATSSS traffic management and bonding configuration for the UE is sent during multi-access data session establishment. Figure 9 is a high level illustration of the use of traffic bonding to a subscriber CPE that bonds, or aggregates, traffic flows over the HFC and 5G NR network. Not all protocol message responses and error conditions are illustrated in the message sequence diagram. See [3GPP 23.502] section 4.22.2 for a more detailed description of ATSSS message flows. 3GPP R17 plans to incorporate LTE into enhanced ATSSS services.

Each step shown in the message sequence diagram Figure 10 is described below. Note that the hybrid CPE registration to the 5G converged core over NR may occur before or after its registration to the core over a DOCSIS network. The message flow diagram below is an example of the hybrid CPE registration process.

1. A 5G UE registration sequence is completed for the hybrid CPE (i.e., 5G-CRG) over the NR radio air interface as specified in section 4.2.2.2 of [3GPP 23.502].
2. The hybrid CPE sends a multi-access (MA) PDU session request to the AMF.
3. The AMF requests a MA PDU session creation from the SMF (Session Management Context request with MA PDU session ID)
4. The SMF retrieves the requested subscription information related to session management with MA PDU session ID from the UDM.
5. The SMF may optionally request session management policy information from the PCF.
6. Session management policy information is sent from the PCF if requested.
7. The SMF creates the session user plane path at the UPF based upon the subscription information and policy. See section 4.3.2.2 of [3GPP 23.502].
8. The SMF sends an MA PDU session accept message with an MA PDU session ID to the AMF.
9. The AMF forwards the PDU Session accept message with an MA PDU session ID to the hybrid CPE.
10. The user plane for the 5G NR-RAN traffic is established. See section 4.3.2.2 of [3GPP 23.502].
11. The hybrid CPE is authenticated by the CMTS and admitted onto the HFC network. Note that the registration sequences for 5G NR shown in step 1 may occur before HFC registration sequence, as illustrated here, or after the HFC registration sequence.
12. The hybrid CPE sends a 5G wireline access registration request to the 5G core using 5G network registration procedures.
13. The 5G core network registration and admission sequence is completed. See section 7.2.1.1 of [3GPP 23.316]
14. The hybrid CPE sends an MA PDU session request to the AMF over the HFC network
15. The AMF sends the MA PDU session request to the SMF, executing the multi-access PDU session.
16. The SMF updates the PDU session user plane at the UPF for the wireline traffic. See section 4.3.3.2 of [3GPP 23.502].
17. A multi-access PDU session accept is sent from the SMF and is sent through to the CPE
18. The W-AGF may optionally request updated DOCSIS service flows at the CMTS if needed
19. The CMTS completes updated DOCSIS service flows if needed
20. The multi-access traffic paths are established and ready to be used. Downstream traffic may be split at the UPF and sent to the CPE over NR and HFC accesses. See section 4.22 of [3GPP 23.502].

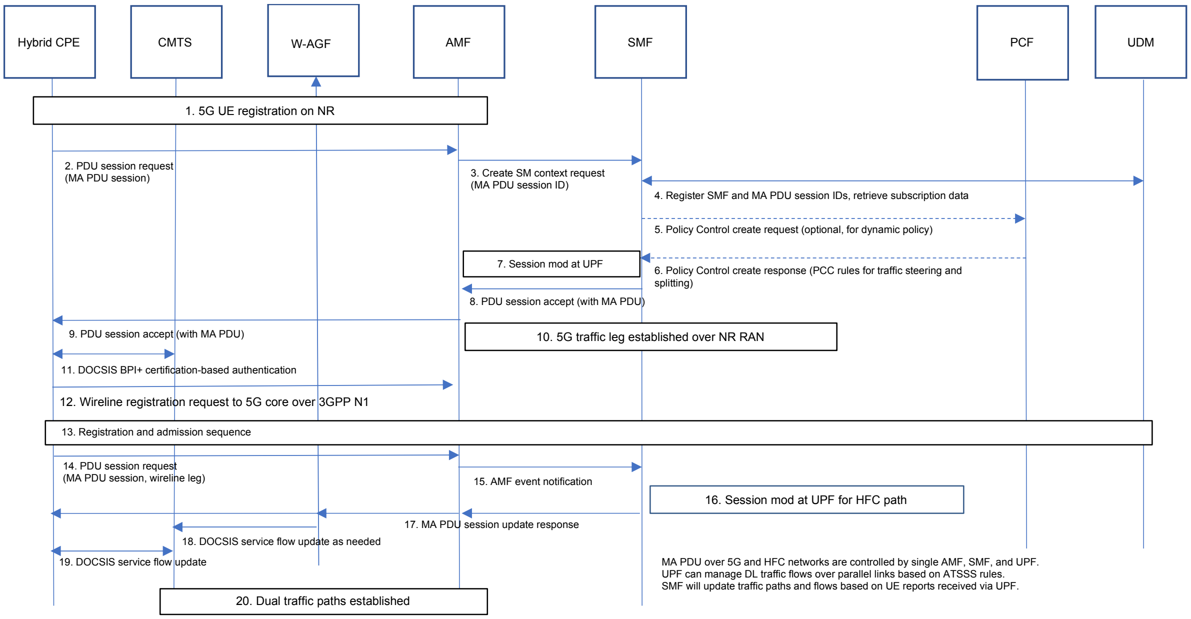


Figure 10 - Traffic Bonding over Wireline and Wireless with ATSSS for the Hybrid CPE

6.2.2 3GPP Session and Service Continuity (SSC)

3GPP R15 includes session and service continuity (SSC) capabilities in three modes of operations, listed below. The data service characteristics and SSC mode chosen for a data session depend on the application.

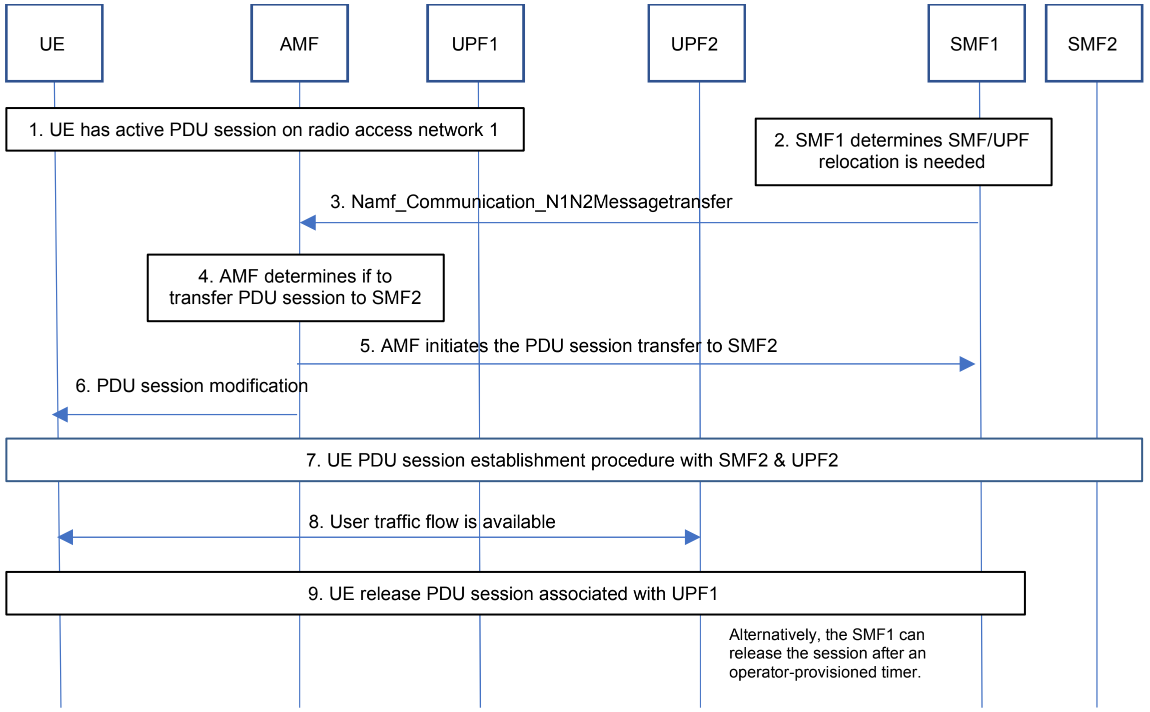
- SSC Mode 1 (SSC1): The network preserves the connectivity service provided to the UE, as well as the UE IP address assigned to the data session.
- SSC Mode 2 (SSC2): The network releases the connectivity service delivered to the UE as well as the data session(s) when the UE moves across networks. IP addresses are not preserved. Given this break in data sessions and connectivity, it is expected that the application layer will play a substantial role in maintaining continuous service.

SSC Mode 3 (SSC3): The changes to the user plane are visible to the UE, but connectivity to the UE is not lost. The UE IP address is not preserved, but the prior IP address/prefix is maintained for some time after the new IP address on the new access network is assigned. The timeframe for preserving the prior IP address is indicated to the UE via NAS signaling. Therefore, SSC3 can help provide a continuous user experience for applications capable of withstanding IP address changes. Figure 11 provides a high-level 3GPP SSC3 message flow diagram. Not all protocol message responses and error conditions are illustrated. See [3GPP 23.502] sections 4.3.5.2 and 4.3.5.3 for a more detailed description of the messaging flow.

Each of the steps in the SSC3 sequence flow diagram Figure 11 across two different radio air interfaces such as 5GC network (network 1) and public Wi-Fi network (network 2) is described below:

1. The SSC3 sequence begins with the UE connected to network 1 with an active PDU session served by SMF1 and UPF1. See section 4.3.2.2 of [3GPP 23.502].
2. SMF1 determines that an SMF/UPF relocation is needed. The sequence here assumes that a change in radio access triggers the change in SMF. See section 4.3.5.2 of [3GPP 23.502]
3. The SMF1 sends a SMF relocation message (Namf_Communication_N1N2Messagetransfer) to the AMF.
4. The AMF determines if to transfer the PDU session to SMF2 (network 2) per 3GPP procedures. See section 4.3.5.2 of [3GPP 23.502].

5. Based on step 4 decision, the AMF initiates the PDU session transfer to SMF2 per 3GPP procedures. See section 4.3.5.2 of [3GPP 23.502].
6. The AMF notifies the UE that a PDU Session Modification process is underway via PDU Session Modification message.
7. A PDU session is established among the UE, SMF2 and UPF2. A new IP address may be assigned to the UE. See section 4.3.2.2 of [3GPP 23.502]. Note the UE can start to release the PDU session with SMF1 and UPF1.
8. The user traffic path is now available between the UE and UPF2.
9. The UE releases the PDU session associated with UPF1. Alternatively, the SMF1 may release the PDU session based upon an operator provisioned timer if the UE does not initiate a release. See section 4.4 of [3GPP 23.502].



The triggers for SMF/UPF relocation and the way the triggers are detected by the SMF are not explicitly defined.
Change in RAN could be one trigger.
IP address is not preserved.

Figure 11 - 3GPP Session and Service Continuity Mode 3 Message Flow Diagram

6.3 UE Routing Selection Policy

Routing selection priorities for the UE as delivered from the 5GC are specified by 3GPP as UE Route Selection Policy (URSP). The policy rules are contained within the PCF and are initially transferred to the UE during network registration or Packet Data Unit (PDU) session establishment. Updates can be subsequently pushed by the network. The UE uses these policies to help determine which cellular or non-3GPP access to prefer when multiple options are available. As such, the URSP can assist in mobile data offload to Wi-Fi. The URSP can also help the UE select network slices and PDU sessions for user traffic. Therefore, URSP can play a role in routing fixed CPE traffic to specific network slices.

URSP is optional for wireline operation and is deployed per operator configuration. The URSP is delivered to the 5G-CRG or to the W-AGF in the case of the FN-CRG. The URSP is stored for the duration of a CRG registration to the 5GC. Operators may configure the W-AGF to store the URSP for a duration of time after the CRG deregisters and prior to its next registration.

6.4 Continuous Services

Continuous services, particularly real-time services, across access networks require fast transitions, often with IP address preservation. Transitions across cellular and Wi-Fi air interfaces are a primary example. Over-the-top traffic approaches employing tunneling or traffic aggregation can achieve continuous real-time services; however, these solutions may be largely proprietary. Therefore, this section considers 3GPP approaches that leverage the standardized 5G UE and 5GC. Although this use case may not primarily rely on convergence aspects, a successful converged architecture needs to support this use case.

Continuous real-time services with the 3GPP 5GC may combine the ATSSS traffic steering feature with UE URSP. URSP provides the overall network selection criteria, and ATSSS steers traffic flows to the UE over the available access networks. This combined solution provides an end-to-end network layer view of continuous service capabilities. It does not, however, address certain UE or access network aspects of continuous service requirements, i.e., mandated PHY layer UE air interface thresholds or actions needed for quality continuous service across networks. Therefore, operators may need to rely upon UE vendors and their chip suppliers to fill in potential gaps on UE behavior at the PHY layer.

It should be noted that 3GPP defines methods for the base stations to direct UEs to certain air interfaces, as an alternative to approaches similar to URSP or ATSSS. However, the interaction of these radio access network (RAN) direction methods and URSP with ATSSS for continuous service is not yet fully addressed in 3GPP. Careful network planning for feature interactions may be needed.

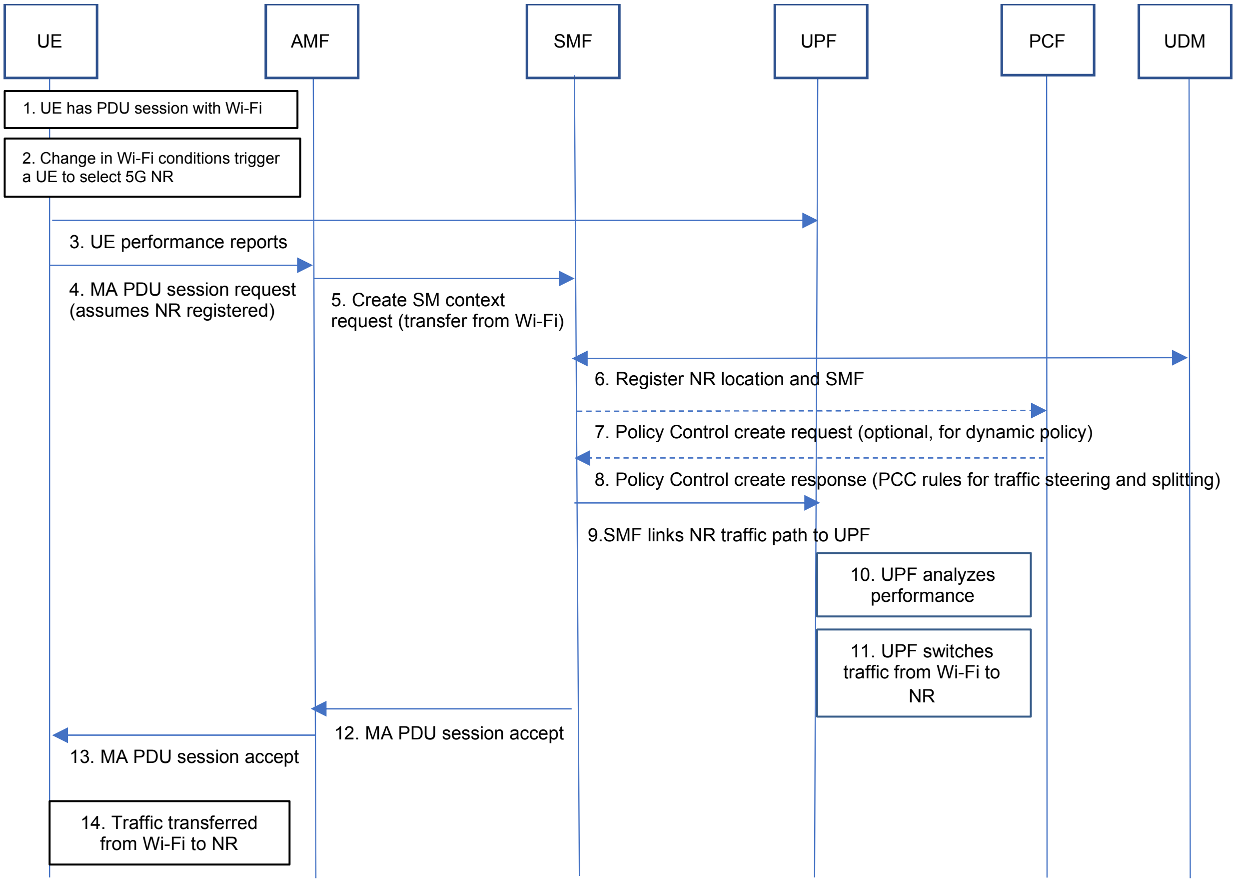
Figure 12 illustrates a high-level message flow for continuous services across NR and Wi-Fi implemented with 3GPP ATSSS. Not all protocol message responses and error conditions are illustrated. See [3GPP 23.502] section 4.22.2 for a more detailed description of ATSSS message flows used for continuous service with IP address preservation.

The high-level message flow illustrated in Figure 12 is described below.

1. The UE has established a Multi-Access (MA) PDU session over public Wi-Fi network per 3GPP procedures. See sections 4.12.2.2, 4.12.5 and 4.22.2 in [3GPP 23.502].
2. The UE detects a change in Wi-Fi performance threshold (i.e., increased round-trip latency or degraded SNR) that trigger the UE to transition to 5G NR-RAN. Performance thresholds used for triggers in this case are per vendor UE implementation, there is no 3GPP reference available.
3. UE performance reports may be sent to the UPF in the bearer plane per operator policy.
4. The UE sends a MA PDU session request to the AMF with the MA PDU session ID to include an NR-RAN traffic path.
5. The AMF requests the SMF to complete the traffic path switch from Wi-Fi to NR.
6. The SMF registers the UE status on NR into the UDM
7. The SMF may optionally request data session related operator policy for NR from the PCF
8. The PCF sends data session related operator policy to the SMF if requested
9. The SMF constructs the traffic path to the UE over NR.
10. The UPF analyzes the performance thresholds for the user traffic over Wi-Fi and NR networks.
11. Based on the UPF performance analysis, the UPF switches the user traffic from the Wi-Fi path to the NR path. See section 4.22.2 of [3GPP 23.502]
12. The MA PDU session accept is sent from the SMF to the AMF
13. The MA PDU session accept is sent from the AMF to the UE.

14. The UE traffic switching process from Wi-Fi to NR is completed. See section 4.22.2 of [3GPP 23.502].

The ATSSS feature can also be applied to hybrid CPE for which 5G NR or LTE is used to deliver highly available HFC broadband Internet.



N3IWF and WAG are not shown.
Multiple protocol alternatives are being considered for multipath and handovers.
UE reports to UPF are sent with an ATSSS-initiated data session.
In this example, UE applied ATSSS rules to the UL path.

Figure 12 - Continuous Services with ATSSS Traffic Steering

6.5 Converged Policy

6.5.1 Goals and Characteristics

Converged policy is foundational for operators to deliver the subscribed user experience across multiple devices and regardless of access network. The following are example considerations for converged policy:

- Traffic management, such as the proper quality of service (QoS) and traffic priority for applications
- Subscribed services, such as parental control to specific users
- Subscribed tiers of service and throughput limits based on billing or usage
- User identification

- Device identification within the home that can be linked to a subscription
- Addressing and packet filtering of data flows destined for devices.

To meet converged policy objectives, the 5G converged architecture needs to support the following:

1. Network authentication and admission of user devices in the home network behind a bridged CRG (see Figure 6 and Figure 7)
2. Access router functions for the bridged CRG and user devices in the home network behind a bridged CRG
3. Policy enforcement points for DOCSIS service flows and 5G data flows that may traverse wireline or wireless access, and
4. Operator-configurable policy rules that can apply to user devices with wireline and wireless access in the home network.

3GPP R16 supports many of the objectives and architectural aspects listed above, but a number of gaps remain that may be addressed in a future 3GPP release:

- Support for bridged CRGs and service to devices behind the bridged CRG,
- Router and traffic management functions for devices in the home, and
- Policy enforcement points that support the aspects above in addition to policy over wireless access networks.

6.5.2 QoS and the 3GPP PCC Architecture

The 3GPP Policy and Charging Control (PCC) architecture specified in [3GPP 23.503] provides a standardized method for the operator to set traffic priorities and QoS characteristics for individual traffic flows within mobile networks. Policy creation and enforcement points are defined. The operator may configure PCC rules held within the 5GC PCF. These rules can take information from applications, the AMF, and the SMF in order to determine traffic priorities specific to access networks. QoS for the converged core will consider how PCC rules can be applied and mapped to HFC QoS. HFC-specific parameters are identified as needed.

Policy creation and enforcement are defined in DOCSIS specifications but vary in practical deployments across vendor solutions. Figure 13 illustrates the following three common QoS architectures specified or used in HFC deployments:

A. This option is a vendor-proprietary use of DOCSIS QoS to support voice applications. It is presently deployed by some MSOs.

B. The second option uses PacketCable Multimedia 2.0 per [PCMM], which is well-specified and aligned with the 3GPP Policy and Charging Rules Function (PCRF), but it has fewer deployments. Common Open Policy Service (COPS) is used to dynamically create, modify, and delete service flows mainly for voice applications, although other applications such as real-time video conferencing or video streaming are supported.

C. The third option shown is to use a Software-Defined Networking (SDN) architecture to dynamically create, modify, and delete service flows for the different supported applications. The SDN Controller receives service provisioning information from the MSO's Operations Support Systems (OSS)/Business Support Systems (BSS), and creates a flow policy to switch the incoming packets for each specific service flow to the CM eMTA via the distributed CCAP platform. This option is not yet widely implemented.

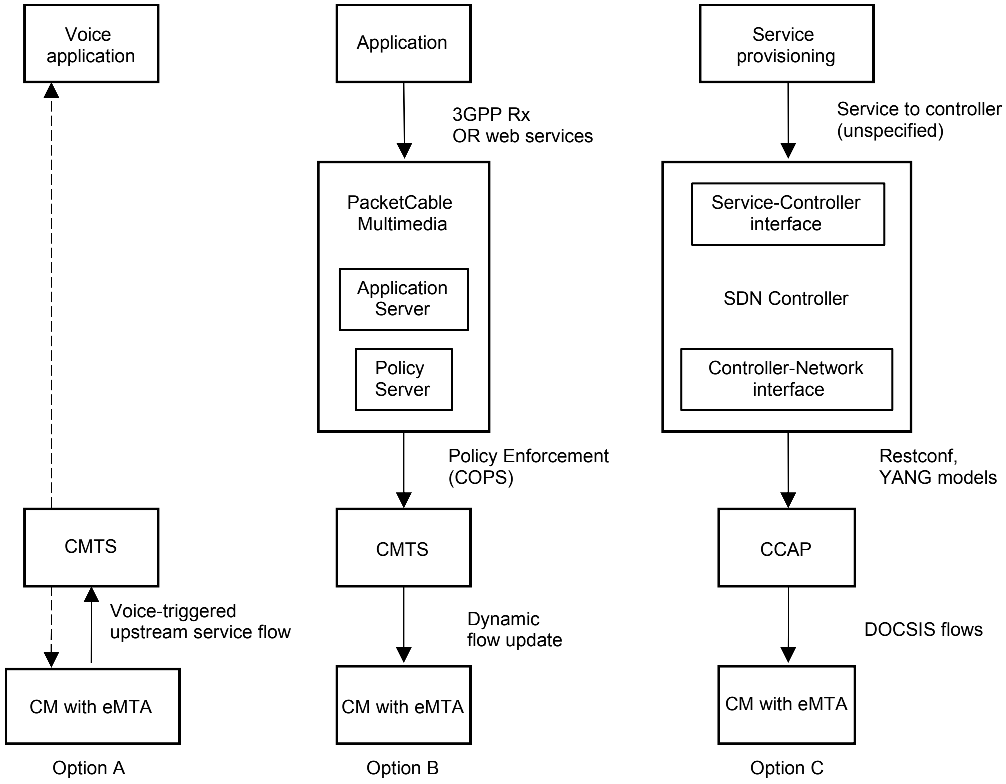


Figure 13 - HFC Architecture Alternatives for QoS

6.5.3 PCC Application to HFC QoS

Per [3GPP 23.503], sources of input into the PCC rules include

- operator-managed applications,
- AMF, and
- SMF.

The PCF accepts application requests for network resources and then uses the input list above within PCC rule sets to identify data flow qualities for the application. The following subsections list the parameters from each source and whether they need to carry HFC-specific information, as well as PCC rules and their HFC considerations.

6.5.4 Input from Operator-Managed Applications

Application media types and connection characteristics are input into the PCF via either the 3GPP Rx interface or a PCF web services interface. The PCF selects candidate QoS classes needed to support the application media types and connection characteristics.

The Rx interface used between the application and the PCF is brought forward from the 3GPP PCRF, which is also leveraged by [PCMM]. As such, 3GPP 5GC standards for the Application Function (AF)-to-PCF interface can be used without updates or parameter additions for HFC networks.

6.5.5 Input from the AMF

Table 1 lists the parameters made available from the AMF to the PCF for input into PCC rules in response to application requests for network resources. HFC-associated values for certain parameters are also listed. The HFC Node identified in [3GPP 23.316] refers to the Fiber Node defined in [MULPIv3.1] which describes the Node Number and Node Name.

Table 1 - Input from the AMF into the PCF for HFC Access Network

3GPP Parameter from AMF	Applied to HFC Network for Interworking	Applied to HFC Network for Integration
SUPI	Global Cable ID@operator realm. (see Section 7.2)	5G IMSI subscription ID, or Global Cable ID@operator realm for wireline-only CRGs
PEI	CM MAC address	CM MAC address
Location of subscriber	HFC Node ID[1], or MAC address + HFC Node ID	HFC Node ID, or MAC address + HFC Node ID
Service area restriction	Collection of Node IDs	Collection of Node IDs
RFSP index	Not applicable	Not applicable
RAT type	Wireline	Wireline
GPSI	External ID per 3GPP 23.008 (username@realm)	External ID per 3GPP 23.008 (username@realm)
Access type	non-3GPP	non-3GPP
Serving PLMN ID	Not applicable	PLMN ID

6.5.6 Input from the SMF

Table 2 lists the parameters made available from the SMF to the PCF for input into PCC rules in response to application requests for network resources. No additional parameter types are identified for use with HFC access networks, but the HFC-associated values for certain parameters are listed below.

Table 2 - Input from the SMF into the PCF for HFC Access Network

3GPP Parameter from SMF	Applied to HFC Network for Interworking	Applied to HFC Network for Integration
SUPI	Global Cable ID@operator realm. (see Section 7.2)	5G IMSI subscription ID, or Global Cable ID@operator realm for wireline-only CRGs
PEI	CM MAC address	CM MAC address
IPv4 address of UE	IPv4 address assigned to CM	IPv4 address assigned to CM
IPv6 network prefix of UE	IPv6 network prefix assigned to CM	IPv6 network prefix assigned to CM
Default 5QI and default ARP	Default DOCSIS service flow ID	Default DOCSIS service flow ID
Request type (initial, modification)	3GPP request type	3GPP request type
Type of PDU session	3GPP PDU session type	3GPP PDU session type
Access type	non-3GPP	non-3GPP
RAT type	Wireline	Wireline
GPSI	External ID per 3GPP 23.008 (username@realm)	External ID per 3GPP 23.008 (username@realm)
Internal-group identifier	Not applicable	Not applicable
Location of subscriber	HFC Node ID, or MAC address + HFC Node ID	HFC Node ID, or MAC address + HFC Node ID
DNN	3GPP DNN	3GPP DNN
PLMN ID	Not applicable	PLMN ID of operator
Application ID	3GPP Application ID	3GPP Application ID
Allocated application instance ID	3GPP Application ID instance	3GPP Application ID instance
Detected service data flow descriptions	Not supported	3GPP service flow descriptions
UE support of reflective QoS	Not supported	Not supported
3GPP PS data off status	Not applicable	Not applicable

6.5.7 PCC Rule Parameters

Table 3 indicates HFC-related values that can be applied within the 3GPP PCC rules parameters. 3GPP PCC rule parameters are defined in [3GPP 23.503] unless otherwise indicated in the table. HFC QoS class examples and DOCSIS service flow parameters are defined in [PCMM].

Table 3 - PCC Rules Parameters for HFC Access Network

Information name	Description	Interworking with HFC Network	Integrated with HFC Network
Rule identifier	Uniquely identifies the PCC rule within a PDU session. Used between PCF and SMF to reference PCC rules.	3GPP	3GPP
Service Data Flow Detection	*Method for detecting packets belonging to a service data flow*		
Precedence	Determines the order in which the service data flow templates are applied at service data flow detection, enforcement, and charging. (Application filter detection is not applicable.)	3GPP	3GPP
Service data flow template	For IP PDU traffic: Either a list of service data flow filters or an application ID that references the corresponding application detection filter for detecting the service data flow. For Ethernet PDU traffic: Combination of traffic patterns of the Ethernet PDU traffic. Defined in [3GPP 23.501], clause 5.7.6.3.	3GPP	3GPP
Mute for notification	Defines whether the application's start or stop notification is to be muted.	Not applicable	3GPP
Charging	*Identities and instructions for charging and accounting required for an access point where flow-based charging is configured*	*Conditional: if operator applies 3GPP charging to HFC network*	3GPP
Charging key	The charging function (CHF) uses the charging key to determine the tariff to apply to the service data flow.	Conditional	3GPP
Service identifier	Identity of the service or service component that the service data flow in a rule relates to.	3GPP	3GPP
Sponsor identifier	ID provided from the AF that identifies the sponsor, used for sponsored flows to correlate measurements from different users for accounting purposes.	Conditional	3GPP
Application service provider identifier	ID provided from the AF that identifies the application service provider, used for sponsored flows to correlate measurements from different users for accounting purposes.	Conditional	3GPP
Charging method	Indicates the required charging method for the PCC rule. Values: online, offline, or neither.	Not applicable	3GPP
Service data flow handling while requesting credit	Indicates whether the service data flow is allowed to start while the SMF is waiting for the response to the credit request. Only applicable for charging method online. Values: blocking or non-blocking	Not applicable	3GPP
Measurement method	Indicates whether the service data flow data volume, duration, combined volume/duration, or event shall be measured. Applicable to reporting if the charging method is online or offline. Note: Event-based charging is only applicable to predefined PCC rules and PCC rules used for application detection filter (i.e., with an application ID).	Not applicable	3GPP
Application function record information	ID provided from the AF that correlates the measurement for the charging key/service ID values in this PCC rule with application-level reports.	Not applicable	3GPP
Service identifier-level reporting	Indicates that separate usage reports shall be generated for this service ID. Values: mandated or not required	3GPP	3GPP

Information name	Description	Interworking with HFC Network	Integrated with HFC Network
Policy Control	*How to apply policy control for the service data flow*		
Gate status	Indicates whether the service data flow, detected by the service data flow template, may pass (Gate is open) or shall be discarded (Gate is closed).	Not applicable	3GPP
5QI	ID for the authorized QoS parameters for the service data flow.	3GPP values: 5G QoS to HFC QoS mapping in W-AGF	3GPP values: 5G QoS to HFC QoS mapping in W-AGF
QNC	Indicates whether notifications are requested from 3GPP RAN when the GFBR can no longer (or can again) be guaranteed for a QoS flow during the lifetime of the QoS flow.	Not applicable	Not applicable
Reflective QoS control	Indicates to apply reflective QoS for the service data flow.	Not applicable	Not applicable
UL-maximum bitrate	Uplink maximum bitrate authorized for the service data flow.	3GPP; mapped to service flows in W-AGF	3GPP; mapped to service flows in W-AGF
DL-maximum bitrate	Downlink maximum bitrate authorized for the service data flow.	3GPP; mapped to service flows in W-AGF	3GPP; mapped to service flows in W-AGF
UL-guaranteed bitrate	Uplink guaranteed bitrate authorized for the service data flow.	3GPP; mapped to service flows in W-AGF	3GPP; mapped to service flows in W-AGF
DL-guaranteed bitrate	Downlink guaranteed bitrate authorized for the service data flow.	3GPP; mapped to service flows in W-AGF	3GPP; mapped to service flows in W-AGF
UL sharing indication	Indicates resource sharing in uplink direction with service data flows having the same value in their PCC rule.	Not applicable	Not applicable
DL sharing indication	Indicates resource sharing in downlink direction with service data flows having the same value in their PCC rule.	Not applicable	Not applicable
Redirect	Redirect state of the service data flow (enabled/disabled).	Not applicable	Not applicable
Redirect destination	Controlled address to which the service data flow is redirected when redirect is enabled.	Not applicable	Not applicable
ARP	The Allocation and Retention Priority for the service data flow consisting of the priority level, the preemption capability, and the preemption vulnerability	3GPP	3GPP
Bind to QoS flow associated with the default QoS rule	Indicates that the dynamic PCC rule shall always be bound to the QoS flow associated with the default QoS rule.	Not applicable	3GPP
Bind to QoS flow associated with the default QoS rule and apply PCC rule parameters	Indicates that the dynamic PCC rule shall always be bound to the QoS flow associated with the default QoS rule. Also indicates that the QoS-related attributes of the PCC rule shall be applied to derive the QoS parameters of the QoS flow associated with the default QoS rule instead of the PDU-session-related parameters authorized default 5QI or ARP.	Not applicable	3GPP
PS-to-CS session continuity	Indicates whether the service data flow is a candidate for Single Radio Video Call Continuity (vSRVCC).	Not applicable	Not applicable
Priority level	Indicates a priority in scheduling resources among QoS Flows (optional).	3GPP	3GPP
Averaging window	Represents the duration over which the guaranteed and maximum bitrate shall be calculated (optional).	Not applicable	3GPP
Maximum data burst volume	Denotes the largest amount of data that is required to be transferred within a period of 5G-AN PDB (optional).	Not applicable	Not applicable
Access Network Information Reporting	*Access network information to be reported for the PCC rule when the corresponding bearer is established, modified, or terminated*		
User location report	Serving cell of the UE is to be reported. When the corresponding bearer is deactivated, information on when the UE was last known to be in that location is also to be reported. if available.	Not applicable	Not applicable
UE timezone report	Time zone of the UE is to be reported.	3GPP	3GPP

Information name	Description	Interworking with HFC Network	Integrated with HFC Network
Usage Monitoring Control	*Identities required for Usage Monitoring Control*		
Monitoring key	The PCF uses the monitoring key to group services that share a common allowed usage.	Not applicable	3GPP
Indication of exclusion from session-level monitoring	Indicates that the service data flow shall be excluded from PDU session usage monitoring.	3GPP	3GPP
Traffic Steering Enforcement Control	*Identities required for Traffic Steering Enforcement Control*		
Data network access identifier(s)	ID(s) of the target Data Network Access. Defined in [3GPP 23.501], clause 5.6.7.	3GPP	3GPP
Traffic steering policy identifier(s)	Reference to a preconfigured traffic steering policy at the SMF (UL and DL may have separate IDs).	3GPP	3GPP
N6 traffic routing information	Describes the information necessary for traffic steering to the DNAI. Described in [3GPP 23.501], clause 5.6.7.	3GPP	3GPP
Information on AF subscription to UP change events	Indicates whether notifications of change in user plane path are requested (as defined in [3GPP 23.501] clause 5.6.7).	3GPP	3GPP
RAN Support Information	*Information supporting the RAN for e.g. handover threshold decision*		
UL maximum packet loss rate	Maximum rate for lost packets that can be tolerated in the uplink direction for the service data flow. Defined in [3GPP 23.501], clause 5.7.2.8.	Not applicable	3GPP
DL maximum packet loss rate	Maximum rate for lost packets that can be tolerated in the downlink direction for the service data flow. Defined in [3GPP 23.501], clause 5.7.2.8.	Not applicable	3GPP

The PCC rules are envisioned to use 5G QoS service classes, indicated with standardized 5QI (5G QoS Identifier) values. These classes need to be mapped to applicable HFC QoS traffic management mechanisms. HFC QoS can be organized around HFC Service Class Names or around a set of HFC service flow parameters. Both Service Class Names and groupings of HFC service flow parameters are operator deployment settings in HFC systems. A minimum common set of HFC service classes is not identified. The mapping is placed within the interworking layer for the interworking model or within the HFC infrastructure for the integration model.

Charging with the interworking model will follow existing DOCSIS models. Online charging is not required for the interworking model and may optionally apply to the integrated model.

6.5.8 5GC and PCMM for the Interworking Model

This section considers how an HFC PCMM system may link into the 5GC within the interworking model. The 5G SMF interfaces to the 5G UPF, which is the bearer policy enforcement point. The UPF (using policy from the PCF via SMF) conveys 5G QoS to the W-AGF. The W-AGF maps the 5G QoS to HFC QoS and manages the HFC service flows at the CMTS accordingly. See Table 5.7.4-1 of [3GPP 23.501] for listing of standardized 5G QoS classes. The classes are implemented in the 5G system per [3GPP 23.503] and 3GPP stage 3 specifications. The W-AGF maps the 5G QoS classes to DOCSIS QoS as configured by the operator. As described in [MULPIv3.1] and [PCMM], operator can define and build DOCSIS QoS classes using DOCSIS layer two scheduling techniques as part of the CMTS configuration. The W-AGF can then map the DOCSIS QoS to the 3GPP standard 5G QoS classes. For the interworking model, in scenarios for which a UPF is not required, an interworking function is needed between the SMF and the CMTS Common Open Policy Service (COPS) Protocol interface as shown in Figure 14. The W-AGF as identified in [3GPP 23.316] provides the interworking between the 3GPP N4 interface and the CMTS. The CMTS pkt-mm-2 COPS interface, as defined in the CableLabs [PCMM] specification, provides the HFC bearer enforcement point in HFC systems. Higher levels of combination, including placing an HFCdedicated SMF in the interworking function, is not precluded. As seen in Figure 14, the PCF and SMF replace the PCMM platform for the interworking model. PCC rules within the PCF will need to accommodate HFC parameters as described in the subsections above.

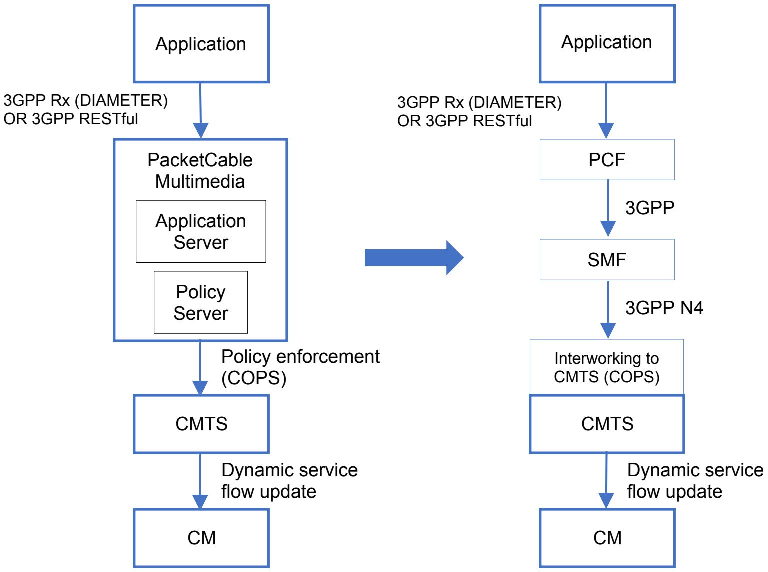


Figure 14 - Use of PCF with PCMM CMTS Interface

6.6 Network Slicing

Network slicing allocates and configures a portion of network resources to support a specific set of characteristics for an application or a subscriber set. 3GPP has standardized the slice types shown in Table 4. See section 5.15.2.2 of [3GPP 23.501]. The 3GPP slicing architecture is extensible. The Slice Service Type (SST) values 128–256 are reserved for operator- or vendor-defined slice types. That is, an MSO-defined slice type that includes HFC characteristics may be assigned an SST value of 128 or greater. Table 5 illustrates hypothetical examples of MSO-defined network slice service types for mobile Xhaul, IPTV and other services. The SST values for operator defined slices may be set by the operator as a network specific configuration, or they may be specified by CableLabs as common values used for the cable industry. CableLabs and operator assigned SST values, as illustrated in Table 5 are taken from the range of 128 to 256.

Table 4 - 3GPP Standard Slice Service Types

SST	SST Value	Characteristics
eMBB	1	Suitable for 5G enhanced mobile broadband
URLLC	2	Suitable for ultra-reliable low-latency communications
MIoT	3	Suitable for massive IoT

Table 5 - Proposed MSO-Defined Network Slice Service Types

SST	SST Value	Characteristics
Mobile Xhaul	To be assigned	Suitable for traffic transport from 5G core to small cells
IPTV	To be assigned	Suitable for transport of linear video and VoD
Traffic Bonding	To be assigned	Suitable for traffic bonding to either 5G mobile device or Broadband Internet user device to increase service availability
Subscription Tiers	To be assigned	Suitable for providing different service subscription tiers to 5G mobile and broadband Internet customers

SST	SST Value	Characteristics
Business Services	To be assigned	Suitable for providing private networking services to SMB and Enterprise customers

Network SSTs are linked to subscriptions in the UDM and are initially authorized for use by the UE at network registration. UE traffic flows are placed into a network slice as part of PDU session establishment. The UE requests a data session with a slice ID suitable for the application requested by the subscriber. In response to a data session request, the AMF selects an SMF that manages the data session within a slice instance and completes the user data path for the session within the network slice. QoS for the flow may be applied per PCC rules contained in the PCF. The HFC link to the CM can form part of the user data path within a slice that includes the wireline network. The interworking function in the HFC network can invoke HFC configuration or DOCSIS traffic flow characteristics based on the slice ID received from the UDM via the AMF.

The 3GPP URLLC standard network slice supports a performance goal of 1msec one-way latency from the UE to the DNN side of the UPF. Therefore, the URLLC network slice should not be applied to CM subscriptions, or whenever the HFC is the path of a user plane, since current HFC systems cannot typically meet this latency objective.

6.7 Virtualization and SDN

3GPP specifications recommend the ETSI specification on network function virtualization (NFV) management and orchestration, [MANO], although vendors go further to customize NFV methodologies in their implementations. The HFC ecosystem has not yet converged towards a common NFV approach. Furthermore, initial virtualization efforts in the HFC network and, separately, in mobile cores have not always resulted in cost savings for operators. As such, a common NFV and software-defined networking (SDN) methodology is not within the scope of this document. A converged and mature NFV and SDN methodology across wireless and wireline networks may ultimately result in more efficient networks in the longer term.

6.8 5G Core Delivery of Media and IPTV

A goal of the 5GC support of IPTV is to ensure quality delivery of high-definition media over the 5GC without impact to the content delivery network (CDN) system. The 5GC should be agnostic to the CDN architecture. Therefore, the architecture of the CDN system is not addressed, and impact to the CDN system is minimized.

This subsection considers how the 5GC can be part of an overall solution to deliver high-quality media to support IPTV services. 3GPP has completed study items that provide a vision of IPTV support within the 5GC (see [3GPP 26.891]). The converged core further defines 5GC support of IPTV. This subsection first describes how high-quality media delivery for IPTV can be supported by the 5GC per 3GPP specifications.

A subset of IPTV subscription parameters is held within the UDM (see Section 7.2). The subscription parameters placed within the UDM support the 5GC capability to deliver IPTV with mobility and location considerations and to organize multicast groups within the 5GC for the sake of linear TV delivery. The UDM holds the following information:

- IPTV account ID or STB MAC address;
- channel access list;
- service authorized only within the home, within the MSO footprint, or while roaming; and
- content caps per month per account regardless of device.

The STB MAC address network admission should be indicated in the UDM when the STB is admitted to the network. This requires an interworking function to note the registration in the UDM. No impact to STB authentication or network admission procedures is required.

Figure 15 illustrates the establishment 5GC PDU session suitable to deliver IPTV via unicast, such as video on demand (VOD). Not all protocol message responses and error conditions are illustrated. See [3GPP 23.316] for a more detailed description of IPTV support by the 5G converged core.

A description of the high-level message from in Figure 15 is provided below.

1. The sequence begins with the registration of a STB MAC address into the 5G core per 3GPP specifications. See section 7.7.1 of [3GPP 23.316].
2. The IPTVSTB requests a PDU session for IPTV with a DNN assigned for IPTV.
3. The AMF selects an SMF enabled for IPTV services. See section 7.7.1 of [3GPP 23.316]
4. The AMF sends create data session for IPTV to the SMF
5. The SMF retrieves IPTV related subscription parameters, which can include a channel access list from the UDM.
6. The SMF optionally may request policy for the IPTV data session from the PCF.
7. The PCF provides policy for IPTV to the SMF if requested.
8. The SMF selects an IPTV capable UPF for the data session. See section 7.7.1 of [3GPP 23.316]
9. The SMF send user plane IPTV parameters to the UPF including access lists, multicast groups and QoS
10. The UPF confirms the session user plane establishment to the SMF
11. The SMF sends a PDU session accept to the AMF
12. The AMF sends a PDU session accept to the IPTV STB
13. The IPTV STB receives and acknowledges the PDU session accept message to the AMF.
14. The IPTV STB PDU session is established, and the IPTV STB starts to receive unicast IPTV media packets.

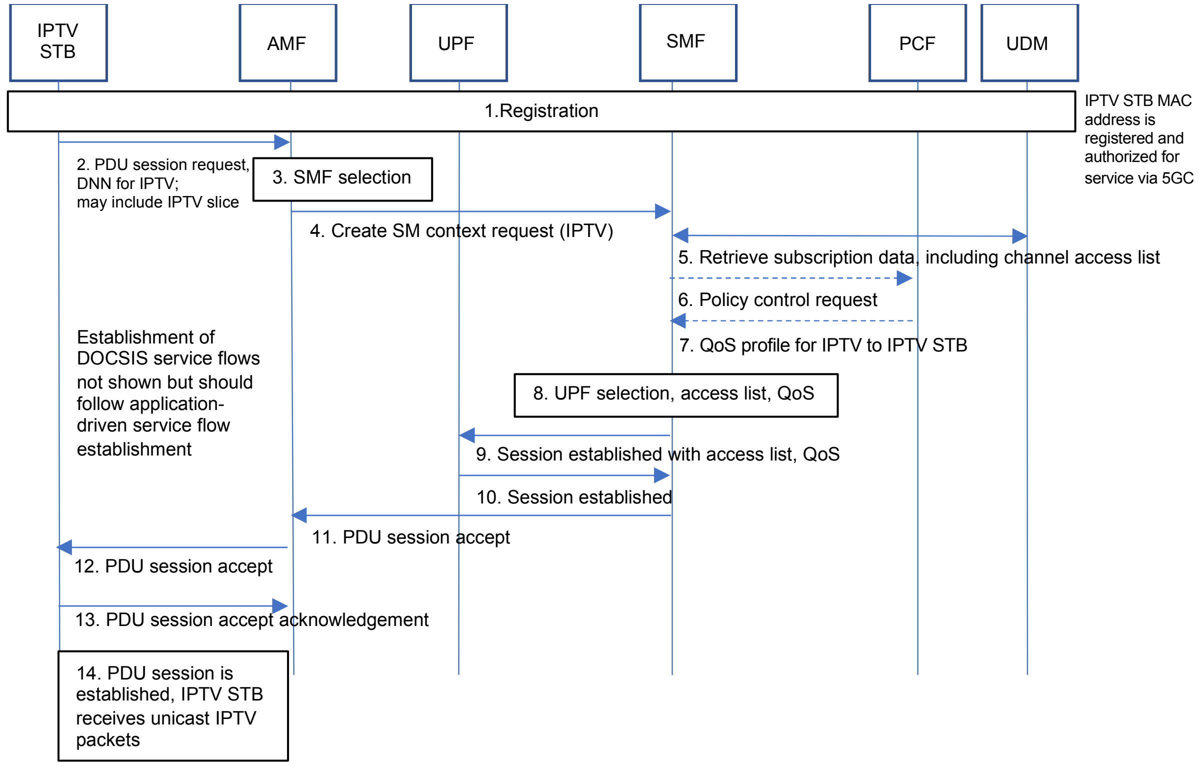


Figure 15 - PDU Session Establishment for IPTV

Figure 15 is a high-level message flow that illustrates the use of multicast groups in the 5GC to deliver linear TV. In this case, a multicast group transports a specific IPTV linear channel. Not all protocol message responses and error conditions are illustrated.

A description of the high-level message flow in Figure 15 is provided below.

1. The IPTV STB requests a channel via an IGMP version 3 (IGMPv3) Join request message on the user plane.
2. The UPF compares the IGMP Join request with its the authorized channel access list. If allowed, the IPTV multicast packets on the channel multicast group will be sent to the IPTV STB. See section 7.7.1.1.3 of [3GPP 23.316].
3. The IPTV server sends multicast packets with media content to the UPF
4. The UPF directs the media packets to the PDU session for the IPTV STB based upon the channel requested and the channel access list assigned to the IPTV STB. See section 7.7.1.1.3 of [3GPP 23.316].
5. IPTV media packets are forwarded from the UPF to the IPTV STB.

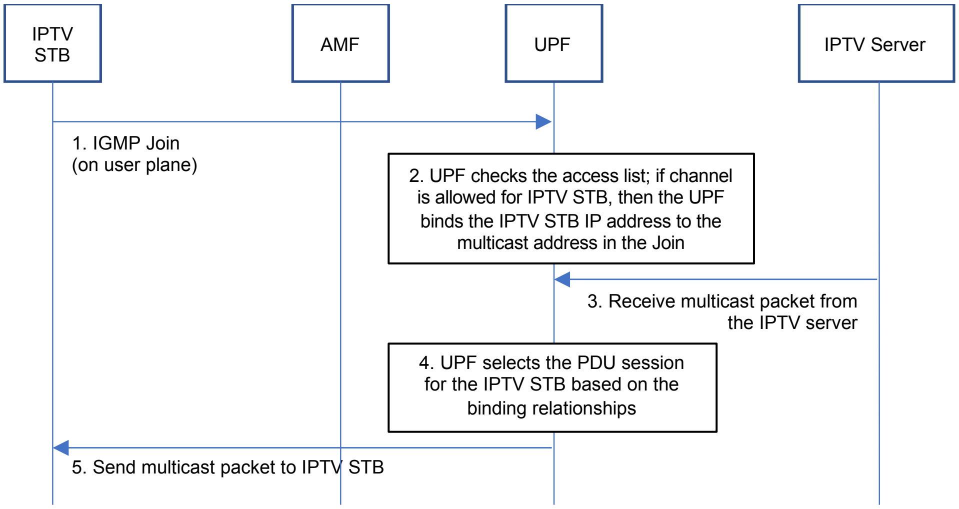


Figure 16 - IP Multicast Within the 5GC for Linear IPTV

The IPTV STB maps an IPTV channel to a multicast group (according to mechanisms that are outside the scope of this report) and requests to join the appropriate multicast group per the channel requested by the subscriber. The UPF binds the IPTV STB to the multicast group then directs multicast group packets to flow from the IPTV server to the CPE.

6.9 HFC Network and System Evolution

Legacy HFC network architectures are rapidly evolving into a Distributed Access Architecture (DAA). The primary concept behind DAA is to distribute some or all of the functionality of the CMTS/CCAP down to a remote location, like the Fiber Node. The key driver for the distributed architecture is the shift from analog to digital optics, which essentially makes the link between the cable headend and the fiber node a Layer 2 Ethernet connection. In a digital HFC plant, the fiber portion utilizes a baseband network transmission technology such as Ethernet, EPON (Ethernet over Passive Optical Networks), GPON (Gigabit Passive Optical Network), or any layer 2 technology that would support a fiber-based PHY layer. There are 3 main distributed architectures as follows:

- Remote PHY architecture
- Remote MAC-PHY architecture
- Split-MAC variation architecture

In the Remote PHY architecture, the integrated CCAP is separated into two distinct components. The first component is the CCAP Core and the second component is the R-PHY Device (RPD). The CCAP Core contains both a CMTS Core for DOCSIS networking and an Edge QAM Core for Video. The RPD contains mainly PHY related circuitry, such as downstream QAM modulators, upstream QAM demodulators, together with pseudo-wire logic to connect to the CCAP Core.

In the Remote MAC-PHY architecture, both the DOCSIS MAC and PHY layers are moved down to the Fiber Node with Layer 2 Ethernet connectivity between the cable headend and the Fiber Node. There are two different options based on how video is handled. In both cases, the data forwarding CMTS functionality is at the remote Fiber Node. A compact CMTS is deployed at the fiber node and the CMTS Network Side Interface (NSI) is connected to the cable headend via the digital optical network. There are two options for handing video distribution, namely Remote CCAP or Remote CMTS and Divided Edge QAM.

The Split-MAC architecture is in between the Remote PHY and Remote MAC-PHY architectures, where some of the MAC functionality is defined and reside at the headend and the remaining MAC and PHY functionalities are moved to the Fiber Node. Specifications efforts for the split-MAC architecture are presently suspended.

In order to operate and manage these access architectures at a higher capacity and at a lower cost, the MSOs are exploring virtualized hardware platforms. For example, in the Remote PHY architecture, the main PHY layer functionality, which modulates the bits onto the wire, need to remain in the Fiber Node. However, essentially all other functionality can be virtualized. The transition to virtualization for the DAA may have an impact on both the integration and interworking models of the 5G converged network architecture in terms of HFC1/2-C and HFC-U interface requirements to the 5GC network.

7 REQUIREMENTS

7.1 Introduction

Convergence requirements within the 5GC are specified in the 3GPP specifications referenced in this document. Additional requirements placed upon the W-AGF and other network elements to support HFC requirements are documented in the following subsections.

7.2 UDM Requirements

5G network admission, slice authorization, and the application of policy are all enabled by the pre-provisioned subscription in the UDM. Registration status is also held within the UDM. The UDM must support the requirements defined in [3GPP 29.500] and [3GPP 29.503]. In addition, the UDM must support the subscription parameters in Table 6 that link:

- Multiple Broadband User Devices (excluding 5G UE mobile devices) to a residential HFC Internet broadband account, and
- Multiple 5G UE Mobile Devices to an HFC Internet broadband account - See [3GPP 23.501] for the definition of the 5G UE Mobile Device.

Table 6 - Subscription Parameters

Subscription Parameter	Format	Normative	Syntax
HFC Subscription			
Global Cable ID (HFC Identifier) @operator realm or IMSI	CM MAC address @ operator realm, or IMSI	Mandatory	See [3GPP 23.316]
Subscription tier (in Mbps)	Integer, 3GPP AMBR or RG-LWAC	Optional	Integer, [3GPP 23.316]
Slice identifiers	NSSAI per 3GPP specifications	Optional	See [3GPP 23.501]
User device identifiers	MAC address	Optional	Per [MULPIv3.1] specification
User device identifiers	Application indicator or credentials as specified by the operator	Optional	Operator defined
3GPP Mobile Subscriptions			
per IMSI	See 3GPP specifications	Mandatory	See 3GPP specifications
IPTV Support in 5G Core			
Registered STB ID	See [3GPP 23.316]	Optional	See [3GPP 23.316]
Channel access list	See [3GPP 23.316]	Optional	See [3GPP 23.316]
VOD consumption limits	See [3GPP 23.316]	Optional	See [3GPP 23.316]
Video away from home delivery	See [3GPP 23.316]	Optional	See [3GPP 23.316]
Serving CDN	See [3GPP 23.316]	Optional	See [3GPP 23.316]
Slice identifiers	See [3GPP 23.316]	Optional	See [3GPP 23.316]

The UDM may support the IPTV parameters in Table 6.

As described in [3GPP 23.316], the CM MAC address, per [MULPIv3.1], appended with the operator realm is registered into the UDM when the W-AGF detects a legacy CM authorization by the CMTS. The 3GPP IMSI is used for registration for CPE that support 3GPP air interfaces. Subscription tiers are applied at the time of registration per 3GPP specifications. A subscription tier or throughput maximum under operator-identified conditions may determine the value of the Aggregate Maximum Bit Rate (AMBR) parameter or the Residential Gateway Level Wireline Access Characteristics parameter in the UDM. See [3GPP 23.316]. The 3GPP Network Slice Selection Assistance Information (NSSAI) parameters indicate the slices authorized for use to an authenticated CM by their assignment in the subscription. User device IDs are registered at the time of their detection on the HFC-enabled local-area network (LAN).

HFC Node IDs as described in [3GPP 23.316] are used to construct location information and to indicate service areas and service area restrictions. The HFC Node ID is the Fiber Node as defined in [MULPIv3.1]. For the sake of convergence, HFC Node IDs are limited to a string of six characters maximum in length.

7.3 CPE Requirements

7.3.1 5G-CRG

A wireline-only 5G-CRG combines the 3GPP UE control plane with an HFC cable modem. The 5G-CRG CPE must comply with the following requirements:

1. The 5G-CRG (wireline only) **shall** support the 3GPP 5G N1 protocol as specified in [3GPP 23.316].
2. The 5G-CRG (wireline only) **shall** populate the 3GPP Permanent Equipment Identifier (PEI) reported with the CM MAC address.
3. The 5G-CRG (wireline only) **shall** a CM MAC address for the HFC_Identifier. The HFC_Identifer with operator realm is used for the wireline only CRG SUPI as described in [3GPP 23.316]. The CM MAC address is specified in [MULPIv3.1].
4. The 5G-CRG that supports 3GPP NR or 3GPP LTE **shall** comply with [3GPP 23.316], which includes requirements for the Subscription Concealed Identifier (SUCI) and SUPI based upon IMSI, and the PEI is populated with the International Mobile Equipment Identifier (IMEI).

7.3.2 FN-CRG

The FN-CRG is a legacy cable modem, which in most cases operates as bridged CRG device as described in Section 5.4. In this case, no convergence requirements are placed on the FN-CRG. Within the interworking model for convergence, the W-AGF provides convergence functions on behalf of legacy cable modems.

7.3.3 Bridged CRG and Devices on the Subscriber LAN

The bridged CRG must comply with the following requirements:

1. The bridged CRG **shall** support layer 2 traffic forwarding between the subscriber LAN and the 5GC user plane as specified in [3GPP 23.316].
2. The bridged CRG **shall** identify the subscriber LAN with an appropriate identifier such as a virtual LAN (VLAN) ID.
3. The bridged CRG **shall** preserve user device MAC addresses as a source address when traffic forwarding so that the 5GC is able to apply services to each user device individually.

7.4 CMTS Requirements

The HFC1-C and HFC2-C interfaces between the CMTS and W-AGF are not presently standardized. These interfaces are expected to be specified and implemented by CMTS vendors for multi-vendor interoperability. Otherwise, the W-AGF needs to be customized on a per CMTS basis in order to support the interactions between the CMTS and W-AGF as described in this document. Operators may also select to integrate W-AGF capabilities including the N1, N2 and N3 interfaces into virtualized HFC infrastructure.

7.5 High Level W-AGF Requirements

The W-AGF must support the following requirements:

1. The W-AGF **shall** support the 3GPP N1 reference point as specified in [3GPP 23.316].
2. The W-AGF **shall** support the 3GPP N2 reference point as specified in [3GPP 23.316].
3. The W-AGF **shall** support the 3GPP N3 reference point as specified in [3GPP 23.316].
4. The W-AGF **shall** support the W-AGF requirements specified in [3GPP 23.316].

5. The W-AGF **shall** support individual VLANs per residential gateway as received via the CMTS.

Each residential gateway in the home network may be assigned its own VLAN between the CMTS and the W-AGF to complete the user plane traffic flow between the DOCSIS access network and the W-AGF.

7.6 Registration, Authentication, and CPE Status

The FN-CRG, 5G-CRG, and W-AGF requirements to support registration, authentication, and status are specified as follows:

1. The FN-CRG **shall** support DOCSIS Baseline Privacy Plus Interface (BPI+) per [SEC] security for authentication with the CMTS to provide a service into the 3GPP 5G Core network.
2. The W-AGF **shall** detect the CM (i.e., FN-CRG) registration into the CMTS.
3. The W-AGF **shall** report CM registrations and de-registrations per FN-CRG requirements specified in [3GPP 23.316].
4. The W-AGF **shall** be able to detect CM unreachability by the CMTS and report the idle status to the 5GC per [3GPP 23.316]. The method by which the W-AGF detects CM registration and reachability status from the CMTS is per vendor implementation. See the CableLabs [MULPIv3.1] specification for how the CMTS detects CM reachability.
5. The 5G-CRG **shall** support 3GPP N1 NAS encapsulated in EAP-5G for initial registration procedures via the DOCSIS network.
6. When the EAP-5G registration is complete and a security association is established between the 5G-CRG and the W-AGF, then the 5G-CRG **shall** support NAS over TLS to the W-AGF for the balance of registration. See [3GPP 23.316] for a message diagram sequence that illustrates the use of EAP-5G and TLS.

7.7 Network Slicing

The 5G-CRG, FN-CRG, and W-AGF requirements to support network slicing are as follows:

1. The 5G-CRG **shall** support network slicing and NSSAI as specified in [3GPP 23.316].
2. The W-AGF **shall** support network slicing and NSSAI on behalf of individual FN-CRGs.
3. The W-AGF **shall** allow the operator to configure the way in which the W-AGF selects slices for the FN-CRG/FN-FRG based on slice IDs received during FN-CRG/FN-FRG registrations, DOCSIS flows initiated by the FN-CRG/FN-FRG, or an FN-CRG/FN-FN-FRG application.
4. Upon FN-CRG/FN-FRG registration, when no other information is available for network slice selection, the W-AGF **shall** select either the enhanced mobile broadband (eMBB) network slice specified by 3GPP for the 5GC to connect to default DOCSIS service flows or an operator-provisioned default slice in the W-AGF for the FN-CRG/FN-FRG.
5. The W-AGF **shall** support operator configuration of slice types to FN-CRGs/FN-FNGs and DOCSIS service flow settings.

7.8 Session Management

The requirements to support session management are summarizes as follows:

1. The 5G-CRG **shall** support the session management procedures specified in [3GPP 23.316].
2. The W-AGF **shall** support session management procedures for each FN-CRG as specified in [3GPP 23.316].
3. The W-AGF **shall** establish an IP PDU data session within the eMBB slice per operator configuration upon the CMTS completing default DOCSIS service flows for the FN-CRG.
4. The W-AGF **shall** establish an Ethernet PDU data session within the eMBB slice if the operator has configured the FN-CRG to be a bridged gateway.

5. The W-AGF **shall** execute a PDU session modification when the FN-CRG or the CMTS completes a dynamic DOCSIS service flow update. The method by which the W-AGF detects the CMTS service flows and service flow updates for an FN-CRG is per vendor implementation.
6. The W-AGF **shall** be able to support multiple PDU sessions for the FN-CRG and to map an individual PDU session to a specific DOCSIS service flow.
7. The W-AGF **may** use the CMTS COPS PCMM interface to manage network-initiated DOCSIS service flow updates on behalf of the FN-CRG.

7.9 Policy

The W-AGF must support mapping of DOCSIS service flow QoS classifiers to 5GC 5QI values as configured by the operator. The mapping is flexible and determined by the operator, but Table 7 provides a few examples. See [3GPP 23.501], table 5.7.4-1, for 3GPP standardized 5QI values mapped to 5G QoS characteristics.

Table 7 - Examples of 3GPP 5QI Mapped to DOCSIS QoS

Application (*Example*)	DOCSIS Scheduling Type	Flow Spec Service Number	DOCSIS Service Class Name (*Example*)	3GPP 5QI Standard Value	3GPP Resource Type	3GPP Priority Level
Real-time voice	Unsolicited Grant	2 (guaranteed)	"Real time voice"	1	GBR with 100 ms delay budget	20
VPN	Real-Time Polling Service	2 (guaranteed)	"Guaranteed delay and throughput"	2 or 4 (*example*)	GBR with 150 or 300 ms delay	40 or 50
General data service	Best Effort	5 (controlled load)	"Best Effort Data"	9 (*example*)	Non-GBR	90

Table 8 shows the most supported voice codecs by the MSOs listed according to their popularity, and their performance parameters for real-time voice application. DOCSIS Real-Time Polling Service (RTPS) is suitable for real-time traffic that generates variable-size data packets on a periodic basis, including real-time video conferencing applications that utilize the VPN connectivity. In this case, the DOCSIS GBR has a variable bandwidth, depending on the broadband connectivity of the FN-CRG, and the assigned DOCSIS QoS to the service flow. The GBR values in the table below are examples and may differ from deployed values configured by operators. The EVS codec requirements are specified in 3GPP 26.441.

Table 8 - Performance Parameters for Real-Time Voice Application

Supported Voice Codec	Access Network	Guaranteed BW (GBR)	Maximum RT Latency	Maximum Jitter	Voice Payload Size
G.711µ-law	Wireline	500 kb/s	< 100 ms	< 30 ms	20 ms
G.729 Annex A	Wireline	500 kb/s	< 100 ms	< 30 ms	20 ms
G.722.1	Wireline	500 kb/s	< 100 ms	< 30 ms	20 ms
Adaptive Multi-Rate Narrow Band	Cellular	500 kb/s	< 100 ms	< 30 ms	20 ms
Enhanced Voice Service[2]	Cellular	500 kb/s	< 100 ms	< 30 ms	20 ms

The W-AGF must be able to receive 5GC 5QI indicators and, as mapped by the operator, set the DOCSIS service flow QoS. The W-AGF may use the CMTS COPS PCMM interface, per the CableLabs [PCMM] specification, to set the QoS of DOCSIS service flows. (See the [MULPIv3.1]and [PCMM] specifications for how HFC QoS may be defined and applied to DOCSIS service flows by the CMTS.) Otherwise, the W-AGF may use vendor solutions to update

---

DOCSIS service flow QoS. The W-AGF must be able to detect DOCSIS service flow QoS updates initiated by the FN-CRG and use PDU session modification procedures per [3GPP 23.316] to update the QoS used within the 5GC.

HFC subscription service tiers may be provisioned in the UDM assigned to HFC subscription. Upon receiving subscription parameters for a CM registration into the 5GC, the W-AGF updates the DOCSIS service flows to the CM to regulate the delivered throughput to the CM per the subscribed HFC service tier.

8 USE CASES AND CAPABILITIES

The exemplary use cases and priority network capabilities described below illustrate the potential value of 5G converged network architecture to the delivery of subscriber services. The subsections below include an explanation of how each use case may be executed with the 5G converged network architecture, and an assessment of the value and implications of applying the 5G converged network architecture to the use case.

8.1 Use Case 1: Consistent User Experience Across Access Networks

A successful 5G converged network architecture is capable of delivering a consistent user service set and consistent operator policy across wireless and HFC access networks. For example, users can set parental controls once and expect them to be executed consistently on mobile devices over 5G or Wi-Fi or on in-home LAN devices for a given user. Video content selection with operator-managed volume limits applicable across access networks is another example service. The goal is to deliver the same user experience and applications on wireless and wireline networks.

8.2 Use Case 2: Continuous Real-Time Services

With continuous real-time service, transitions across 5G, 4G, Wi-Fi, and other access networks are transparent to the user experience. Real time services as referred to in this section envision interactive video conferencing and voice services. These services require low latency transport with minimum re-transmissions. In fact, one-way latency is expected to be less than 50 ms for these real-time services. The 5G URLLC network slice is typically not required. It requires PHY and MAC layer procedures during transitions to be rapid and reliable, and real-time applications often require a persistent IP address. Although this use case may not necessarily rely upon wireless-wireline convergence features, it remains a high-priority use case for operators that need to be supported by the RAN and by core networks.

Mobile devices also play an essential role in continuous services, including actions triggered by PHY parameter thresholds. Although the converged core does not assist in UE PHY procedures, it contributes to continuous real-time service across RANs for mobile devices through its use of 3GPP ATSSS and its support for access network priority selection per operator policy, QoS, and IP address preservation. Section 6.4 describes the use of ATSSS for transitions across 5G NR and Wi-Fi radio networks.

Three specific use cases in this use case category to consider:

Use Case 2A: Wi-Fi Data Off-Loading with Single Service Flow

A wireless user is consuming its real-time services outside his home network via his 5G NR UE mobile device. When the user's 5G NR UE mobile device joins his Wi-Fi home network, it offloads all the 5G NR traffic to the in-home Wi-Fi network using a single service flow to support both the 5G NR UE mobile traffic and the in-home Wi-Fi traffic.

If the 5G NR UE mobile device is a roamer, and connects to a visited Wi-Fi home network, the 5G mobile traffic must be transported via an encrypted L2 tunneling protocol (L2TP) to ensure traffic isolation between the visited Wi-Fi home network and the roamer. Since there is only a single service flow, both the roamer traffic and the visited Wi-Fi home network traffic receive the same treatment unless other techniques to prioritize, police, and rate shape traffic are used.

The use of a single common service flow to conserve the consumption of service flows may be beneficial to some MSOs to provision and support the required service flows for each user.

Use Case 2B: Wi-Fi Data Off-Loading with Two Service Flows

Similar to use case 2A except when the user's 5G NR UE mobile device joins its Wi-Fi home network, it offloads all the 5G NR traffic to the in-home Wi-Fi network using a separately allocated service flow from the in-home Wi-Fi traffic service flow. This use case allows the service provider to optimize each service flow attributes to the type of traffic, depending if it is from a 5G NR UE mobile device or from another device in the home network. Note that the 5G NR traffic is typically routed to the 5G core network, and the user is unable to communicate with in-home Wi-Fi network devices unless the service provider is able to hairpin route the 5G NR traffic back to the home network. If this user roams to a visited network, then its 5G NR traffic can be hairpin routed to its home network from the visited service provider's network.

If the 5G NR traffic belongs to a roamer, the 5G NR traffic is routed to the 5G core network, and the roamer is not able to communicate with the devices on his home network. This means that the in-home traffic and the roamer's traffic are isolated from each other. In addition, because this traffic is on a separate service flow, different attributes can be applied to distinguish the service of a roamer from the service of the owner of the home network. The use of multiple service flows may be beneficial to some MSOs to prioritize, police, and rate shape traffic.

Use Case 2C: NG-RAN Data Off-Loading with Two Service Flows

Similar to use case 2A except there is no offloading of the 5G NR traffic to the in-home Wi-Fi network. Rather, the 5G NR traffic is offloaded to the NG-RAN in the home network. Thus, two service data flows, one for the 5G NR traffic, and one for the in-home Wi-Fi traffic must be established and maintained.

It should be pointed out for use cases 2B and 2C that the CMTS may have a limited number of service flows that can be allocated to support various types of user traffic. The availability of the CMTS service flows to support various types of user traffic is an MSO-specific capability, and depends on many factors such as the number of supported users, traffic load, etc.

8.3 Use Case 3: Traffic Bonding

Traffic bonding is the aggregation of two data flows across separate access networks. It can deliver greater bandwidth to the subscriber device. It can also increase service availability because it allows one data flow to deliver user traffic while the second is impaired or diminished. Traffic bonding is executed by UE and core network capabilities. The 3GPP ATSSS feature, per [3GPP 23.501], supports the 5G version of traffic bonding. Section 6.2.1 describes the use of 3GPP ATSSS for traffic bonding. The bonded traffic's priority and QoS parameters are Cable MSOs configurable.

8.3.1 Traffic Bonding to the 5G NR Mobile Device

User traffic is delivered to the 5G NR mobile device through parallel data flows over 5G NR and Wi-Fi. The traffic flows are aggregated at the mobile device for use by applications. Though this use case may not necessarily rely on wireless-wireline convergence features, it remains a high-priority use case for operators that need to be supported by the RAN and by core networks

8.3.2 Traffic Bonding to 5G-CRG Device

User traffic is delivered to the broadband Internet 5G-CRG through parallel data flows over 5G NR and the HFC network. The traffic flows are aggregated at the 5G-CRG for use by applications. This use case leverages the converged core with the 3GPP ATSSS feature as specified in [3GPP 23.501]. It is referred to as the hybrid use case within the 3GPP study item.

8.4 Use Case 4: Ultra-Low Latency

3GPP has identified the performance goal of 1milisecond (ms) latency for URLCC communications between the UE and UPF DNN interface. A standardized network slice ID has been reserved for URLCC in order to link the URLCC network configuration to applications that demand low latency. 5G vendors are working on 5G RAN and core solutions to achieve this performance goal.

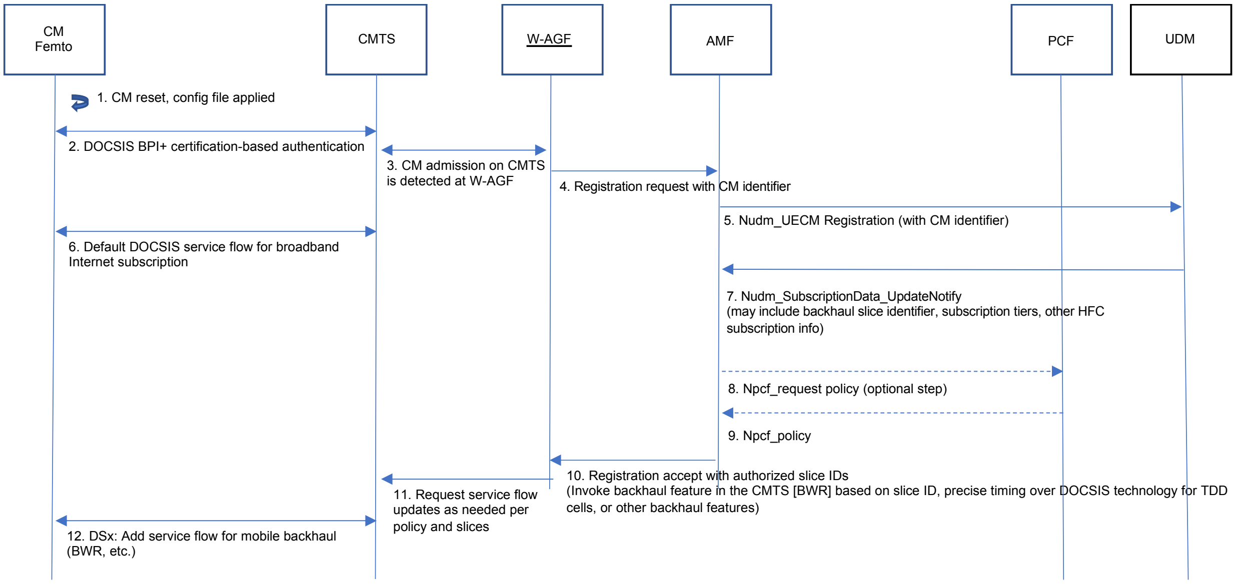
Current HFC networks may not typically achieve the latencies required to meet URLCC performance objectives, particularly on upstream data flows. Therefore, the standard URLCC network slice does not apply to wireline access and should not be assigned to wireline subscriptions in the UDM. The URLCC user plane should not be transported over HFC access as currently deployed.

8.5 Use Case 5: Mobile Xhaul

The mobile Xhaul use case considers using the HFC network as transport from the core network to small cells in the home, in the enterprise, or distributed in metro areas (such as strand units). Mobile Xhaul may also consider the use case of HFC transport between remote radio heads and virtualized baseband units. The CM in the residential or enterprise use case may simultaneously serve both subscriber broadband Internet services and mobile backhaul between small cells and the mobile core. In this case, the CM supports two different CMTS service flows, one suitable for the residential/enterprise subscriber, and a second suitable for either Small Cell or Femtocell subscriber. It should be pointed out, that CMTS may have a limited number of service flows that can be allocated to support various types of user traffic. Traffic routing and uplink/downlink (UL/DL) symmetry to support the small cell need to be enforced on the HFC service flow used as backhaul. This second HFC service flow can be invoked by one of two alternative methods.

Network slice: In this case, an operator network slice type for Xhaul is defined. The slice type is authorized for the CM when the CM registration is indicated to the UDM. The slice type is sent from the UDM to the AMF, where it is then sent to the HFC network. The HFC interworking layer then invokes the Xhaul service flow with the proper policy for the small cell. Figure 17 illustrates the concept of a network slice type used for backhaul with the following high message flow. Not all protocol message responses and error conditions are illustrated. The message sequence assumes that a femto cell is added to an existing CM deployment.

1. The CM configuration is updated to accommodate the femto cell in the customer premise network. The CM configuration is applied with a CM reset.
2. The CM is authenticated and admitted by the CMTS using DOCSIS procedures.
3. The W-AGF detects that the CM is admitted by the CMTS. The W-AGF then sends a registration request to the AMF.
4. The AMF registers the CM into the UDM and requests subscription information.
5. The UDM provides the subscription information that includes network sliced identifiers.
6. The CMTS provides a default DOCSIS service flow to the CM for broadband internet service. This step may occur any time after the admission by the CMTS shown in step 2.
7. The UDM provides subscription information to the AMF. In this case, a slide ID that supports femto transport services with the DOCSIS BWR feature is included in the subscription information. The subscription information also includes broadband internet and femto cell services parameters.
8. The AMF may optionally request policy from the PCF to apply to the services delivered to the subscriber.
9. The PCF sends policy to the AMF if requested by the AMF to do so.
10. The AMF sends a registration accept with the slice ID and any applicable policy to the W-AGF.
11. The W-AGF then indicates to the CMTS to add a service flow for the femto cell with the BWR feature invoked.
12. The CMTS adds the DOCSIS service flow to the CM for the femtocell service. BWR is active on the DOCSIS link.



Assumptions:
A simplified AMF is part of the HFC network.
An external SMF or UPF is not needed for this use case; may be incorporated into the HFC network.
Backhaul slice ID is an MSO value assignment.

Figure 17 - CPE for Broadband Internet and Small-Cell Backhaul

Subscribed feature: Alternatively, a backhaul feature could be defined that is assigned to the HFC subscription in the UDM. The UDM profile links the backhaul feature to the CM MAC address. The subscriber feature parameters are sent to the AMF, which then initiates a network-pushed secondary PDU session per the backhaul feature to the CM with a policy suitable for backhaul.

The mobile fronthaul use case considers using the HFC network as transport between radio heads in the enterprise or metro areas and virtualized baseband units. Mobile fronthaul is implemented with a converged core methodology similar to that of mobile backhaul, with two primary differences:

- location of the HFC transport between the mobile network components and
- differences between fronthaul and backhaul throughput and latency performance requirements. (Note that variations of virtual RAN [vRAN] architectures may have specific fronthaul performance needs.)

8.6 Use Case 6: IPTV

The IPTV use case considers the delivery of linear video over IP and VoD to fixed and mobile clients. The scope of the use case focuses on converged IPTV subscriptions and converged traffic management policy capable of delivering high-definition video. The characteristics of the video content delivery system are not within the scope of this use case given the numerous video architectures employed in the cable industry. The implementation of 5GC support for media delivery of IPTV is described in Section 6.8.

8.7 Use Case 7: Broadband Internet Portability (Nomadic CM)

Broadband Internet portability supports a subscriber moving from one residence to another within the same MSO service area without the need for subscriber or MSO intervention. That is, the subscriber is able to relocate their CM and expect it to be operational and online upon power-up. Procedures for this so-called nomadic CPE are not yet specified by 3GPP but may be anticipated for the future.

8.8 Use Case 8: Subscription Tiers

Subscription tiers are often included in broadband Internet product lines. A subscription tier for mobile may include advertised speeds that depend on the total traffic volume consumed by the user in a given time period. The mobile subscriber would receive full cellular speeds until reaching a volume limit, which would trigger a lower maximum delivered throughput for the remainder of the time period.

A converged subscription tier would support a set of speed targets and traffic volume thresholds for a given subscriber regardless of access network or device.

A subscription tier is directly reflected in the existing 3GPP PCC rules described in Sections 6.5.3 and 6.5.8 and can be enforced at the UPF.

8.9 Use Case 9: Business Services

Business services may provide private networking for the enterprise. In support of private networking, a converged core enables private IP addressing space, traffic segregation, and enterprise-level security. The 5GC natively supports private addressing for properly configured DNNs. In this case, businesses may want to control the subscription and authentication used for network admission, which may motivate non-SIM solutions for private isolated networks. The EAP-over-NAS authentication option described in [3GPP 23.501] can be used to carry EAP-TLS for certificate-based authentication or EAP-TTLS for username and password authentication.

9 USE CASES MAPPED TO REQUIREMENTS

Operator use cases are addressed by several requirements contained in this technical report and in the referenced 3GPP specifications. Table 9 identifies how the identified service provider's use cases in Section 8 are supported by the 3GPP specifications and this CableLabs report. Gaps in either 3GPP specifications or CableLabs documents are identified.

Table 9 - Requirements Mapped to Use Cases

Use Case #	Use Case Name	3GPP Specifications	CableLabs Technical Report	Gaps
1	Consistent user experience	Partially in 23.316	Sections on subscription, bridged RG, and policy	Support for bridged CRG and user devices in 3GPP
2A	Continuous real-time services: Wi-Fi data offloading with single service flow	23.501, 23.502	Sections 6.4 and 8.2 in this TR	Support for Wi-Fi data offloading with single service flow isn't addressed in this TR
2B	Continuous real-time services: Wi-Fi data offloading with two service flows	23.501, 23.502	Sections 6.4 and 8.2 in this TR	Support for Wi-Fi data offloading with two service flows isn't addressed in this TR
2C	Continuous real-time services: NG-RAN data offloading with two service flows	23.501, 23.502	Sections 6.4 and 8.2 in this TR	Support for NG-RAN data offloading with two service flows isn't addressed in this TR
3.1	Traffic bonding: 5G NR mobile devices	ATSSS specified in 23.501 and 23.502	Sections 6.2.1 and 8.3.2 in this TR on 5G NR mobile devices	Support for UDP traffic needs further detail
3.2	Traffic bonding: 5G-CRG device	ATSSS specified in 23.501, 23.502, and 23.316	Sections on ATSSS and W-AGF	
4	Ultra-low latency	23.501 on slicing	HFC slices, slice ID identified	HFC networks and systems need further development work
5	Mobile Xhaul	Not applicable	HFC configurations include mobile backhaul with BWR	New 5G service flows need to be added with policy control and management
6	IPTV	23.316	Sections 6.8 and 8.6 in this TR	
7	Nomadic CM	To be determined	To be determined	Not addressed in this TR
8	Subscription tiers	UDM specs	Sections on UDM and policy mapping	
9	Business services	Similar to residential LAN case	Similar to residential LAN case	Support for bridged RG and user devices is not addressed in this TR

10 FUTURE WORK

Areas of future work anticipated for the 5G converged core include:

- 3GPP 5G core support for bridged CRGs in which each user device is served by the core with a consistent set of services and policy,
- convergence with MSO-operated optical networks,
- converged security appliances, and
- requirements for converged fixed and mobile IoT devices.

11 3GPP ENGAGEMENT

CableLabs is participating directly in the 3GPP Study Item and Work Item for R16 of [3GPP 23.316]. CableLabs has submitted or actively cosigned and supported contributions on the following topics within 3GPP technical working groups.

- Architecture block diagrams and protocol stacks for the FN-CRG
- Registration procedures for the 5G-CRG and FN-CRG
- Authentication and network admission for MSO-subscriber CPE and devices
- Identifiers for the HFC network, including SUPI, SUCI, PEI, and service areas
- Solutions to support bridged CRGs
- ATSSS applied to the hybrid use case
- Distribution of policy on and configuration updates to the 5G-CRG and FN-CRG
- QoS mapping between the 5G core and DOCSIS service flows
- PDU session management linked to DOCSIS service flows

* * *