Technical Report

TR-466
Metro Compute Networking: Use Cases and High Level Requirements

Issue 1
Issue Date: September 2021

Issue History

Issue Number	Approval Date	Release Date	Issue Editor	Changes
1	28 September 2021	28 September 2021	Ruobin Zheng, Huawei Technologies Bo Lei, China Telecom	Original

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editor: Ruobin Zheng, Huawei Technologies
Bo Lei, China Telecom

Work Area Director(s): George Dobrowski, Morriscreek Consulting
Bruno Cornaglia, Vodafone

Table of Contents

Table of Figures

Executive Summary

This project document provides a list of use cases with related high level requirements that provides a framework defining a new metro-compute networking architecture with in-depth integration of computing and network on top of the Cloud-based broadband networks, with the purpose of connecting isolated edge sites (e.g., Cloud CO) as one cloud to serve edge computing services, supporting the edge to edge collaboration, the edge to cloud collaboration, and load balancing among edge sites at network level. It includes recommendations for BBF Work Projects.

1 Purpose and Scope

1.1 Purpose

There are many views in the industry about the “edge” and this project investigates the role of the “edge” in relation to the Metro Computing Network. With edge computing, service providers can help improve their customer's quality of experience by moving applications or content toward the lower edge tiers in the network hierarchy, providing a better user experience.

It is predicted by Gartner that by 2025, more than 75% of the computing data needs to be analyzed, processed, and stored at the edges. In this trend, the industry faces a strategic transformation from "device, PIPE, and cloud" to” device, EDGE, and cloud". The "EDGE" becomes the key to this transformation, in which the biggest network transformation is in the MAN (metro area network), where the traffic direction changes from “the cloud to the terminal” to “the terminal to the cloud”, and the traffic pattern changes from the north-south traffic to including east-west traffic. Thus, a third network--Computing Network-- is emerging.

Evolution of the network eras illustrated in Figure 1 is as follows:

- The first network-- Infrastructure Network, is a network connecting physical devices to physical devices. It deals with port-level interconnection.
- The second network-- Cloud-based telecom network, which is SDN/NFV enabled. It deals with tenant-level interconnection, connecting Tenants/Subscribers to Virtualized Network.
- The third network-- Computing Network, is a network connecting Computation to Data. It deals with service-level interconnection. Computing Network can be considered as the next step of SDN/NFV.

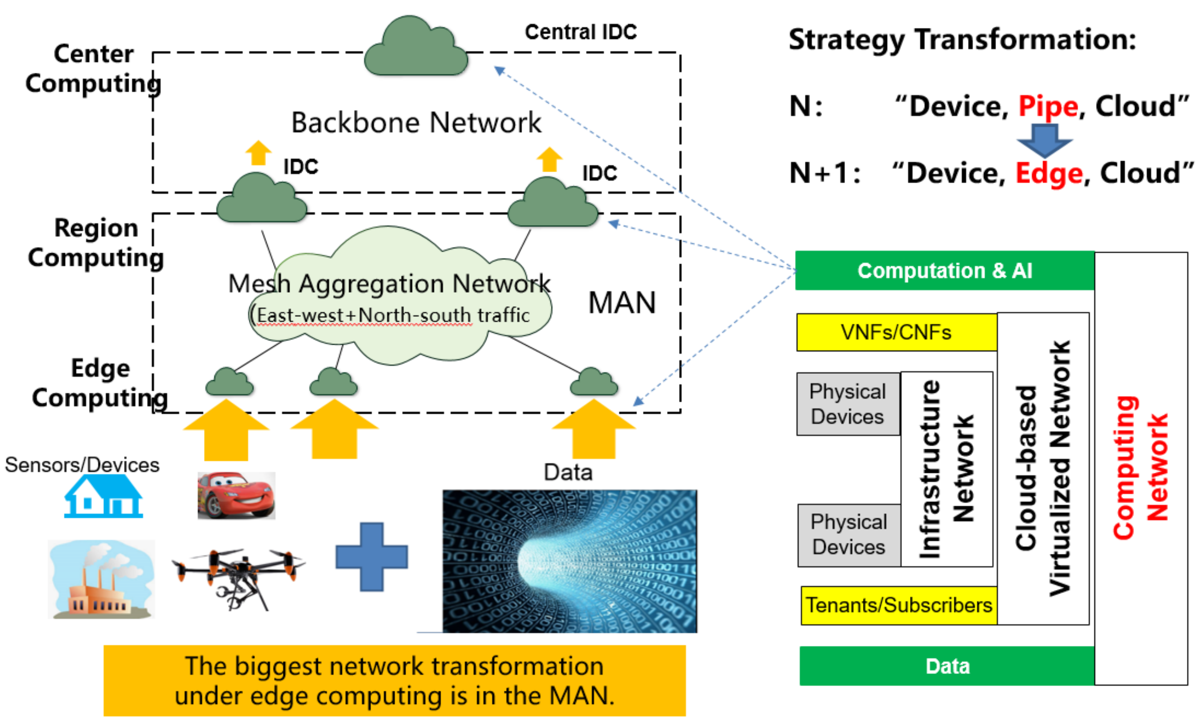


Figure 1 Evolution of the network eras

Carrier Edge Cloud is considered as the next growth point for cloud computing innovation. Beyond SDN/NFV, in the wave of edge computing, new business opportunity for Telco ICT transformation is emerging. The existing edge computing devices are deployed on the user side. However, this kind of solution is not based on standard and is provided exclusively by cloud providers. Small ICPs and even large cloud providers cannot afford the wide deployment and high edge costs of massive edge sites.

There is a unique value for operators, in that only operators have already owned a large number of edge sites. For Telco, operators will be able to transform to ICT service provider and transform business offering from bandwidth towards network connection and related computing and storage. For OTT, internet companies will be able to shift to light asset mode through edge sharing from Telco, save Asset Investment and O&M Costs of massive distributed edge nodes, e.g., CloudCO/MSBNG/BSG.

There are some edge computing-related SDO and industry organizations, such as the ETSI MEC ISG etc. However, there is no industry organization talking about the possible impacts on multi-service broadband networks under the trend of edge computing. Moreover, there are several issues associated with edge computing not addressed in the existing edge computing related organizations; for example, scalability at the edge, the low statistical multiplexing issue, “cloud island” issue, and the routing challenge for edge computing.

The BBF focus is on the broadband network covering CPE, CO, and PoP, which are exactly the Edge Cloud related area. The BBF’s CloudCO [2] has become a basis to further enable a dramatically faster and more efficient provisioning of edge computing services that requiring low latency and high bandwidth and are able to be enhanced to provide a high availability of new revenue-generating services. Further considering that the business growth and commercial deployment of NFV is far behind expectation, it represents an opportunity for BBF to involve in Edge computing and to utilize the virtualized network infrastructure to enable carriers to increase revenue via Edge Cloud services.

This project proposes exploring a new metro compute networking architecture with in-depth integration of computing and network on top of the Cloud-based broadband networks, with the purpose of connecting isolated edge sites (e.g., Cloud CO) as one cloud to serve edge computing services, supporting the edge to edge collaboration, the edge to cloud collaboration, and load balancing among edge sites at network level. The concept of metro compute networking is illustrated in Figure 2. It proposes exploring the network protocols to correlate computing power information of edge sites (e.g., Cloud CO) and network topology information. It provides customers with optimal computing power selection, allocation, and network connection, and schedules user computational requests to the optimal computing site.

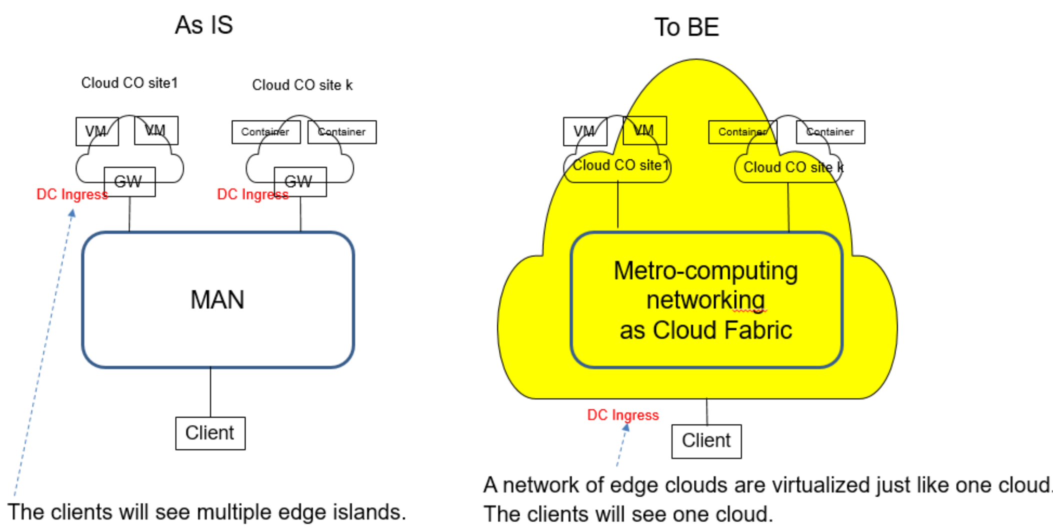


Figure 2 Concept of Metro Compute networking

1.2 Scope

This project looks at Cloud computing, potential Edge compute locations, and investigates how the compute locations can be networked together such that resources (VNF/CNFs) for edge cloud services can be deployed and scale. It will define the reference architecture with functional and nodal requirements to support metro compute networking in cloud-based broadband networks [2] [3] [4] [5]. The project has the following objectives:

- Describe the framework of metro compute networking
- Study the high level requirements and potential techniques of metro compute networking
- Provide use cases of metro compute networking when necessary
- Identify the gaps in Cloud CO specifications in order to implement a metro compute networking

Generally speaking, the scope of edge computing includes edge cloud, and the Ultra-reliable low-latency communication (URLLC) Edge are the interests of this project stream, while the IoT edge is beyond the scope.

1) Edge Cloud: It is an extension deployment of cloud (including public and private cloud) to network edge nodes. Carriers can use physical resources, such as equipment rooms and power distribution, to develop edge clouds and provide high-bandwidth and low-latency service experience for users. It can support smart campus, smart city, MEC, and CDN scenarios. By providing infrastructure services such as connectivity and computing, carriers can improve their network connection monetization capabilities. It is the next step of innovation breakthrough of cloud computing.
2) URLLC Edge: MEC that provides computing and storage resources for services that require low bounded latency and almost zero packet loss.
3) IoT Edge: It is an aggregation node for enterprise and industry data. It is an evolution gateway device based on cloud computing technologies. It provides key capabilities, such as heterogeneous connections, real-time processing, cloud-based management, and artificial intelligence, to enable industry digitalization.

The following topics are considered to be out of the scope of this work, such as:

- The interface between MEC and CloudCO, which may be accomplished in ETSI MEC ISG or the BBF CloudCO PS.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [1].

MUST	This word, or the term "REQUIRED", means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the term "RECOMMENDED", means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the term "OPTIONAL", means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document	Title	Source	Year
[1] RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[2] TR-384	Cloud Central Office Reference Architectural Framework	BBF	2018
[3] TR-101 Issue 2	Migration to Ethernet-Based Broadband Aggregation	BBF	2011
[4] TR-178 Issue 2	Multi-service Broadband Network Architecture and Nodal Requirements	BBF	2017
[5] TR-370 Issue 2	Fixed Access Network Sharing – Architecture and Nodal Requirements	BBF	2020

2.3 Definitions

The following terminology is used throughout this Technical Report.

Computing Host	A computing host is a physical amount of CPU, memory and hardware resources.
Computing Instance	A computing instance is a logical allocation of some or all of a computing host. Examples of computing instance can be containers or VMs or servers etc.
Computing Power	Computing power is the necessary capability required by applications and provided by computing instance in order to applications to fulfil their computational service operations. Computing power is the key core ability of a device or platform to process computational information to complete a certain computational task. It involves the computing capabilities of the device or platform, including logic computing capabilities, parallel computing capabilities, neural network acceleration and other computing capabilities.
Edge Site	A edge site is a collection of computing hosts and networking equipment. Typically it can be a CO site, a PoP site or a central DC.
Metro-Compute Networking	The Metro-Compute Networking is a new type of edge-cloud fabric in the broadband networks which distributes the computing power, storage, algorithm and other resource information of the edge (e.g., Cloud CO) sites through the network control plane (including centralized controllers, distributed routing protocols, etc.), and combines them with network information and user needs to provides the best distribution, association, transaction and deployment of resources such as computing, storage, and network, so as to realize the optimal configuration and use of the entire cloud-based broadband network resources.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

AI	Artificial Intelligence
AN	Access Node
BBF	Broadband Forum
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
BSG	Broadband Service Gateway
CDN	Content Delivery Network
CO	Central Office
CPE	Customer Premises Equipment
DC	Data Center
FIB	Forwarding Information Base
ICT	Information and Communication Technology
ID	Identifier
IGP	Interior Gateway Protocol

IoT	Internet of Things
IP	Internet Protocol
MCN	Metro Compute Networking
MEC	Multi-Access Edge Computing
MPLS	Multiprotocol Label Switching
MSBNG	Multi-service BNG
NFV	Network Function Virtualization
PoP	Point of Present
PS	Project Stream (BBF)
RIB	Routing Information Base
SLA	Service Level Agreement
SR	Segment Routing
TR	Technical Report
URLLC	Ultra-Reliable Low-Latency Communication
VM	Virtual Machine
VR	Virtual Reality

3 Technical Report Impact

3.1 Energy Efficiency

Typically external load balancers have to be deployed to distribute traffic between servers in a data center. The number of load balancers is proportional to the numbers of edge sites, which are expensive in the scenario of edge computing. In addition, it is difficult to load balance across multiple sites. The compute-aware routing in the Metro Compute Networking can alleviate the need for large numbers of hardware load balancers depending on application use cases and thus saving energy.

3.2 Security

Sharing information related to computing power of edge sites between IT provider (e.g., computing provider) and Network Infrastructure Provider can create issues on security. It is highly recommended to define proper methods between IT provider and Network Infrastructure Provider to address potential security issues.

3.3 Privacy

Sharing information related to computing power and tenants of edge sites between IT provider (e.g., computing provider) and Network Infrastructure Provider can create issues on customer privacy. It is highly recommended to define proper methods between IT provider and Network Infrastructure Provider to address potential privacy issues.

4 Business Drivers or Issues Being Addressed

In an intelligent society, tens of thousands of Internet companies obtain traffic and require computing power. Carriers have a large number of edge equipment rooms and edge computing power after network cloudification evolution. They are the owners of computing power and traffic guiders.

To adapt to the development of an intelligent society, a new business model that dynamically and quickly matches the preceding supply-demand relationship is as follows: Internet companies rent edge computing power from carriers on demand, and traffic is obtained from carriers' MCN, thereby saving a large amount of investment in heavy assets of edge computing and traffic acquisition costs. Carriers release edge equipment rooms and network cloudification advantages to monetize network connections and edge digital assets (computing and storage).

There are several issues associated with edge computing in multi-service broadband network.

- Scalability at edge

  As the chosen edge location gets closer to the user, the processing power and storage capacity becomes limited due to space and other environmental constraints. Operators hesitate to deploy cloud services at edge, since the edge cloud service in fixed network has high computing dynamism and randomization challenges. Generally, a cloud-based telco network (NFV) is relatively static, and traffic can be predicted. However, cloud services and computing resource requirements cannot be predicted. Especially in discount seasons and unpredictable hot spots, the edge computing consumption increases dramatically. For instance, CloudVR/CloudPC traffic has transient large pulses, which cannot ensure good delay experience for all users. For a 50Mb/s video stream, pulse height can reach up to 750Kb/ms (i.e., 750Mbps). It is difficult for a single one edge site to bear this kind of traffic impact.

- Low statistical multiplexing of computing resources at edge

  The hardware cost per user is high. The GPU resource per user is excessive. The power consumption per user is high. And the tidal effect of edge computing is even more serious than cloud computing.

- Cloud networking issue at edge

  After the telecom network is cloudified, if simply copying DC technology to edge, the "cloud isolated island" problem occurs. Different cloud islands can only be connected through heterogeneous technologies such as VXLAN, Ethernet, or MPLS/IP. In such multi-cloud networking scenarios, pipe stitching increases the number of operational points operations. During the deployment of new services, the technical boundary is frequently configured and even VLAN planning is performed. In addition, hop-by-hop OAM/ protection combination is required. The OPEX is hard to reduce.

- Routing challenge for edge computing

  Typically, OTT providers use application-layer DHT routing for edge computing. DHT is effective for some services such as web services, but is challenging for edge computing services. It is a tradeoff between good load balancing and good locality. To expect uniform distribution of computing function/data storage in the hash ring, we have to face the poor locality/delay issue because we cannot expect the edge computing site is nearest . If optimizing DHT routing for edge computing, the load balancing might be sacrificed. Network Infrastructure Providers are also facing routing challenges under edge computing. For the traditional DNS and IP routing, it only ensures that IP Addresses are reachable, but cannot ensure the availability and QoS of edge-computing power.

- Digital assets monetization issue at edge

  Core Competitiveness of Internet Industry is traffic. At present, the top pain point of Internet companies is that the cost of obtaining traffic accounts for up to 30% of the total enterprise cost. Traditional Internet traffic-obtaining methods include search engines, aggregation websites, and portal websites, such as Google, App stores, etc. How to obtain traffic at low cost is always a big problem for Internet enterprises. However, in the trend of edge computing, the top pain point of

Internet companies is even worse. Due to the high distribution degree of edge computing, the statistical multiplexing ratio of computation power is lower, and the traffic obtaining is more difficult. In addition, it even introduces another pain point: The cost of edge-site assets is very high. Therefore, the Internet industry needs a low-cost sharing economic solution to address this pain point. There are business opportunities as well as challenges in the wave of edge computing deployment.

- For carriers: How can the advantages of edge equipment rooms and NFV be released? How to monetize “edge digital assets (computing and storage)"?
- For Internet companies: How can the digital assets be shared and the traffic be driven from carriers to OTTs on demand, so that both traffic obtaining costs and heavy assets cost can be saved?

5 Use Cases

5.1 Edge to Edge Collaboration

Title	Edge to Edge Collaboration
Story Highlights	There is a high probability that a single one edge site becomes hot spots. However, there is a low probability that all the edge sites become hot spots at the same time. Therefore, one idea is to build a "Network of Edge cloud" for the support of edge to edge collaboration in order to solve the scalability issue and low statistical multiplexing of computing resources under cloud computing.
Business Drivers or Issues Being Addressed	One issue of Edge Computing is scalability at edge. As the chosen edge location gets closer to the user, the processing power and storage capacity becomes limited due to space and other environmental constraints. Operators hesitate to deploy cloud services at edge, since the edge cloud service in fixed network has high computing dynamism and randomization challenges. Generally, a cloud-based telco network (NFV) is relatively static, and traffic can be predicted. However, cloud services and computing resource requirements cannot be predicted. Especially, in discount seasons and unpredictable hot spots, the edge computing consumption increases dramatically. For instance, CloudVR/CloudPC traffic has transient large pulses, which cannot ensure good delay experience for all users. For a 50Mb/s video stream, pulse height can reach up to 750Kb/ms (i.e., 750Mbps). It is difficult for a single one edge site to bear this kind of traffic impact. Another issue is the low statistical multiplexing of computing resources at edge. The hardware cost per user is high. The GPU resource per user is excessive. The power consumption per user is high. And the tidal effect of edge computing is even more serious than cloud computing.
Actors	Network Infrastructure Provider Computing Consumer Computing Provider

High-level architectural context

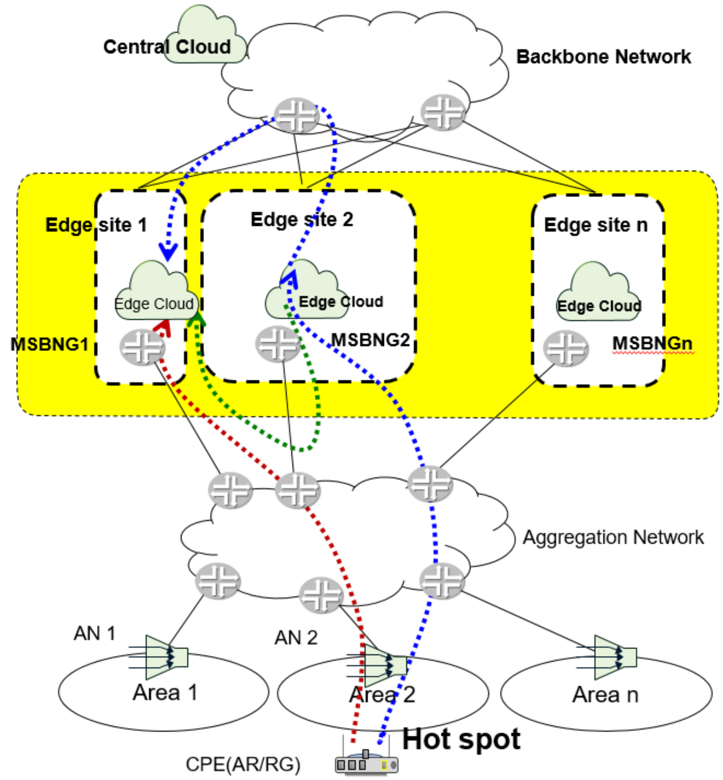


Figure 3 Edge to Edge Collaboration

A proper location of the edge cloud is, for example, the BNG/CloudCO site provided by a Network Infrastructure Provider who is also a Computing Provider. A high-level architecture of the Edge to Edge Collaboration is depicted in Figure 3. In order to address scalability issue, the edge clouds become a pool shared by Computing Consumers, the aggregation network becomes an edge cloud fabric or the backbone network becomes a fabric between edges and central cloud. The Metro-compute network can be defined as the edge cloud fabric in the multi-service broadband network, which directs traffic between different edge sites in the pool of edge clouds.

The Edge to Edge Collaboration means that a computing task of one site can be offloaded to other sites in the edge cloud pool. For example, when the green area becomes a hot spot, and the green edge site 2 unloads the computing task to the site 1 through the aggregation network. The aggregation network has to deal with not only north-south traffic, but also new east-west traffic. The topology of the aggregation network should be able to change from a tree to a new mesh. The edge cloud fabric can direct traffic between different edge sites.

A proper edge can be selected through this fabric for edge computing during subscriber session establishment. During the subscriber session duration phase, computing tasks can be offloaded to other sites through the aggregation network or backbone network. The subscribers can initiates multiple sessions to different edge sites.

From the perspective of Computing Consumers, there can be two kinds of implementation:

- The first one is a distributed control solution with which the multiple edge sites are virtualized like one cloud but with work-load distribution methods that do NOT require centralized control. It relies on the Metro-compute network (i.e., edge cloud fabric) to select the suitable edge sites for computing tasks on

	demand based on distributed protocols. • The second one is that the multiple edge sites are virtualized just like one cloud relying on a centralized control and management solution in order to support Edge to Edge Collaboration.
Related and Derivative Use Cases	-
Inputs to high level requirements	• The edge clouds provided by a Network Infrastructure Provider should be able to become a pool shared by Computing Consumers for the support of Edge to Edge Collaboration. • The aggregation network should be able to become an edge cloud fabric that can direct traffic between different edge sites. • The backbone network may be able be become an edge cloud fabric that can direct traffic between different edge sites. • Computing task can be offloaded from one edge site to other edge sites through the edge cloud fabric.

5.2 Abstracted Edge Cloud with a Centralized Controller

Title	Abstracted edge cloud with a centralized controller
Story Highlights	The multiple edge sites are virtualized just like one cloud. It relies on a centralized control and management solution in order to support Edge to Edge Collaboration with an assumption that the Network Infrastructure Provider provides both the access network and edge-computing nodes.
Business Drivers or Issues Being Addressed	One issue of Edge Computing is scalability at edge. As the chosen edge location gets closer to the user, the processing power and storage capacity becomes limited due to space and other environmental constraints. Operators hesitate to deploy cloud services at edge, since the edge cloud service in fixed network has high computing dynamism and randomization challenges. Generally, a cloud-based telco network (NFV) is relatively static, and traffic can be predicted. However, cloud services and computing resource requirements cannot be predicted. Especially in discount seasons and unpredictable hot spots, the edge computing consumption increases dramatically. For instance, CloudVR/CloudPC traffic has transient large pulses, which cannot ensure good delay experience for all users. For a 50Mb/s video stream, pulse height can reach up to 750Kb/ms (i.e., 750Mbps). It is difficult for a single one edge site to bear this kind of traffic impact. Another issue is the low statistical multiplexing of computing resources at edge. The hardware cost per user is high. The GPU resource per user is excessive. The power consumption per user is high. And the tidal effect of edge computing is even more serious than cloud computing.
Actors	Network Infrastructure Provider Computing Consumer Computing Provider

High-level architectural context

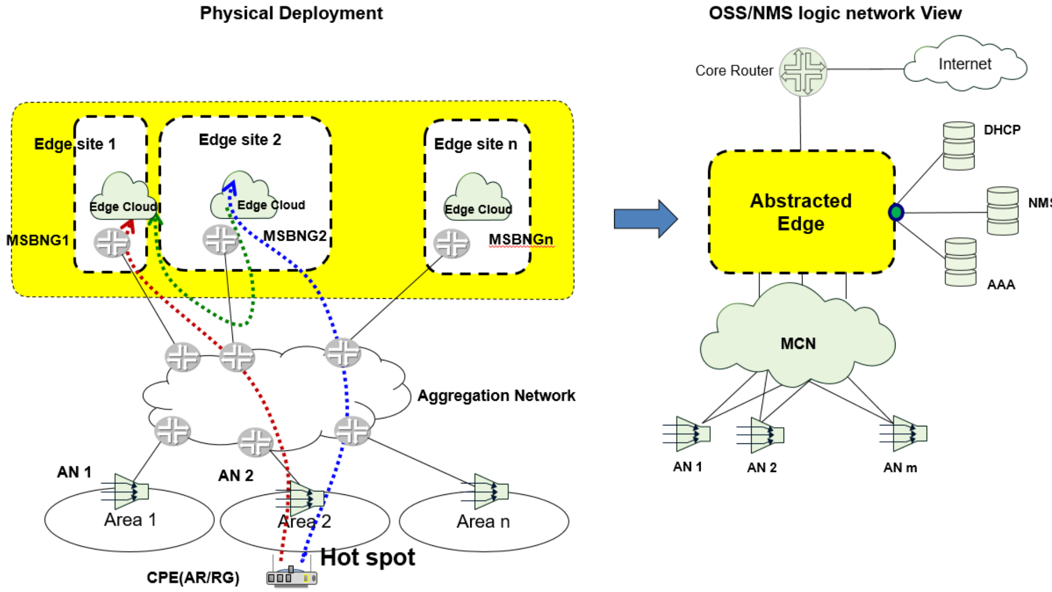


Figure 4 Logic network View of edge clouds

As shown in Figure 4, a couple of edge-computing nodes are abstracted, by an Edge Node controller, into a single network element being an abstracted EN, which acts just like one cloud with single one cloud address towards customers or network managers. In this way, the NMS, the DHCP server, and the AAA server etc. will view the abstracted EN as a single network element and each edge node is equivalent to a remote module of the abstracted EN.

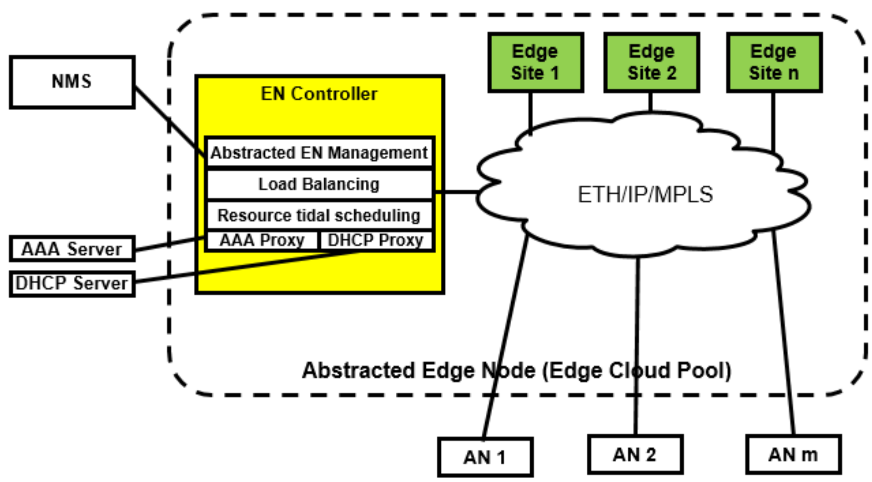


Figure 5 Abstracted edge cloud with a centralized controller

The EN controller can support automatic decomposition from an SLA of the subscriber (i.e., Computing Consumer) to the configurations of the edge nodes, so as to hide the complexity of distributed deployment details of the edge-computing nodes from high level management and to avoid increase of the operation and maintenance costs of distributed edge computing.

The EN controller support resource tidal scheduling and load balancing function for the support of allocating a proper edge node for edge computing.

To present multiple edge node as one network element, the abstracted EN management function of the controller maintains a mapping between physical access loop identifier and

	logic access loop identifier. The logic access loop identifier indicates a logical access loop on a virtual EN device in terms of control and management. For example, during load balancing, a physical access loop identifier carried in AAA/DHCP request message from Computing Consumer to the servers will be replaced with a logical access loop identifier. The logical access loop identifier in the AAA/DHCP response message from the servers to Computing Consumer will be replaced with a physical access loop identifier. Thus it hides the complexity of edge computing details out of high level management from the network managers. To support load balancing, the controller can select a proper edge node for edge computing. Based on a mapping policy between the physical access loop identifier and an edge node address, for example, it can select a proper address of an edge-computing node by adding the edge node address into the AAA/DHCP response message during subscriber session establishment according to the physical access loop identifier.
Related and Derivative Use Cases	Use case of Edge to Edge Collaboration
Inputs to high level requirements	• The multiple edge sites are abstracted by an Edge Node controller just like one cloud. • The EN controller support resource tidal scheduling and load balancing function for the support of allocating a proper edge node for edge computing.

5.3 Compute-aware Routing

Title	Compute-aware routing
Story Highlights	The computing capability of edge sites can be aware by network via routing protocol, so that the computing tasks or data can be dynamically routed to the most appropriate computing nodes to achieve best edge-computing experience.
Business Drivers or Issues Being Addressed	One challenge of Edge Computing is brought by Service Replication. The computing power of a single edge site is very limited (for example, 10 servers). The reliability of an edge-computing site is very much lower than that of a DC. Generally, multiple service replication needs to be provided across multiple edge sites to ensure better performance and reliability. However, one technical issue is how to direct computing requests or data towards which edge sites for the purpose of load balancing and QoS guarantee.

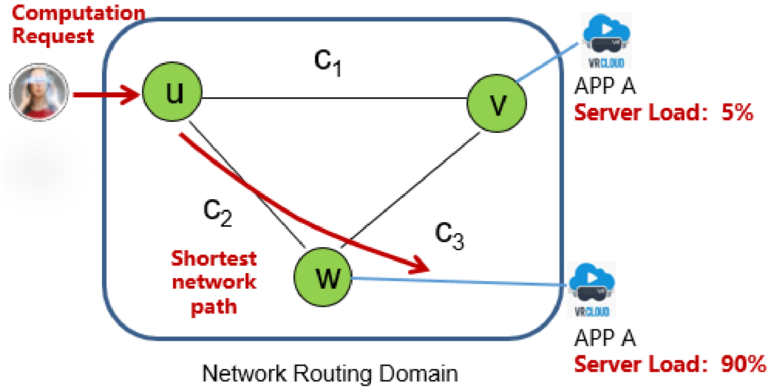
<table>
<tr>
<td></td>
<td>


Figure 6 Path towards overloaded computing site

In Figure 6, it shows that the current IP router typically selects the shortest path. However, for instance, when the computation request data arrives at router W, it is found that the edge computing site happens to be overloaded and even is down. Then the computation request may have to be discarded by the edge. Otherwise, it may have to be redirected along another path, shown in Figure 7, from router U to router W and then to router V. But this temporary redirected path usually is not able to guarantee QoS (e.g., delay).

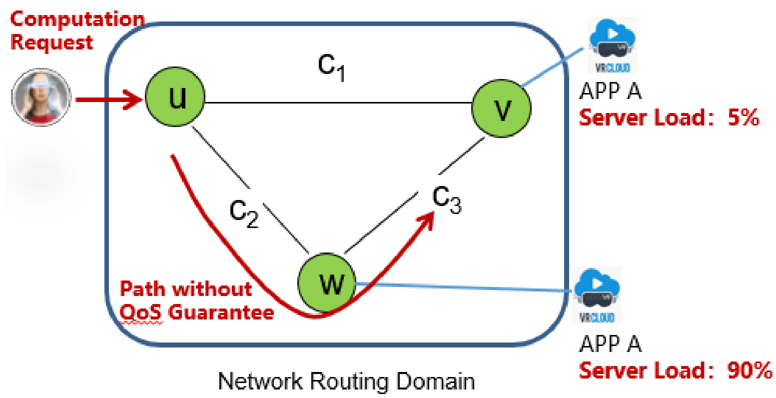


Figure 7 Redirected path without QoS Guarantee

Typically, computing providers use application-layer DHT routing for edge computing. DHT is effective for some services such as web services, but is challenging for edge computing services. It is a tradeoff between good load balancing and good locality. To expect uniform distribution of computing function/data storage in the hash ring, computing providers cannot expect the edge computing site is nearest at the same time. That occurs poor locality/delay issue. If optimizing DHT routing for edge computing, the load balancing might be sacrificed.

Network Infrastructure Providers are also facing routing challenges under edge computing. For the traditional DNS and IP routing, it only ensures that IP Addresses are reachable, but cannot ensure the availability and QoS of computing power.
</td>
</tr>
<tr>
<td>Actors</td>
<td>
Network Infrastructure Provider

Computing Consumer

Computing Provider
</td>
</tr>
</table>

High-level architectural context

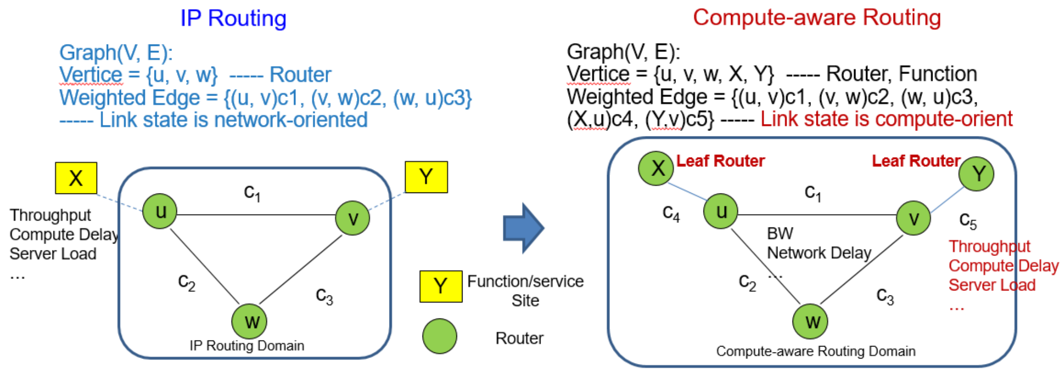


Figure 8 Extension of routing domain into computing domain

It is proposed to extend the routing domain into computing domain shown in Figure 8. It adds the computing nodes (e.g., X or Y in Figure 8) into the routing domain as leaf routers. And the computing capability of a leaf router (i.e., a computing container) can be added into the route calculation as a cost. Traditionally, the routing domain performs routing only based on the bandwidth as a cost. With the compute-aware routing, the computing capability, such as throughput, compute delay, and server load etc., can be handled as a kind of virtual link state and be added as a kind of cost into route calculation by routers.

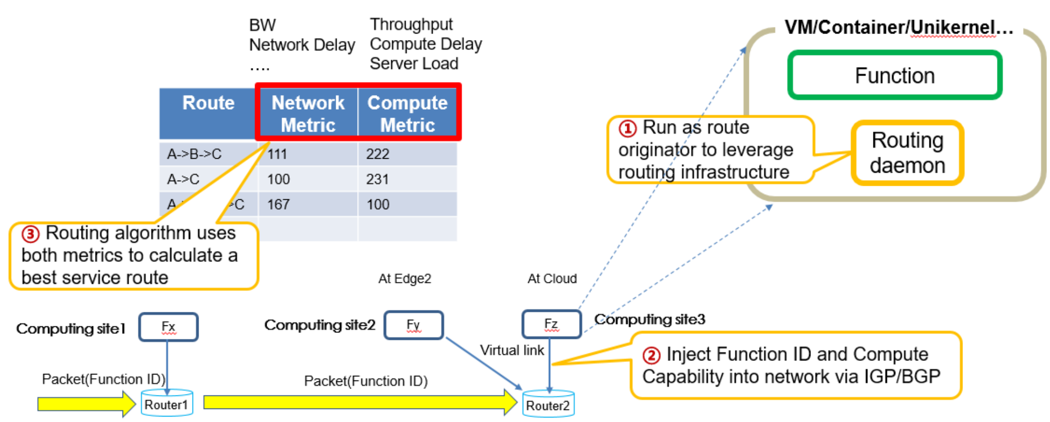


Figure 9 Proposed Compute-aware routing mechanism

The compute-aware routing mechanism is depicted in Figure 9. A computing function or service is identified by a function ID which maps to a group of instances that are functionally equivalent. The function ID can be an anycast address. The computing container should be able to run the routing protocol and advertises the computing capability and the function IDs which it support as routing information to the routers in the metro-compute network. A router computes a route based on both the computing capabilities and the network capabilities. The path cost value of a service route is a composite of both network metric and compute metric derivative from network capabilities and computing capabilities respectively. The routing protocol (e.g., IGP/BGP) is used in the distributed control plane in order to automatically select a proper edge-computing node or site for the processing of the computation tasks or data according to function ID sent from Computing Consumers.

The routers in the IP routing domain are provided by Network Infrastructure Providers. The computing containers at the edge site in the compute-aware routing domain are provided by Computing Providers or Network Infrastructure Providers. A computing container can be a site, a server, a VM, or a container.

There are some advantages of the compute-aware routing as follows:

1) It addresses service replication challenges in Edge Computing

Compared with traditional DNS and IP routing, it not only ensures that IP Addresses are reachable, but also guarantees the availability (e.g., Figure 10) and QoS (e.g., Figure 11) of edge-computing power.

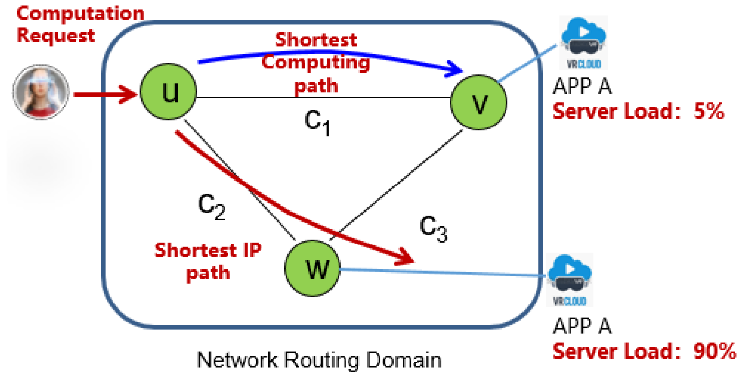


Figure 10 availability insurance of computing power through routing

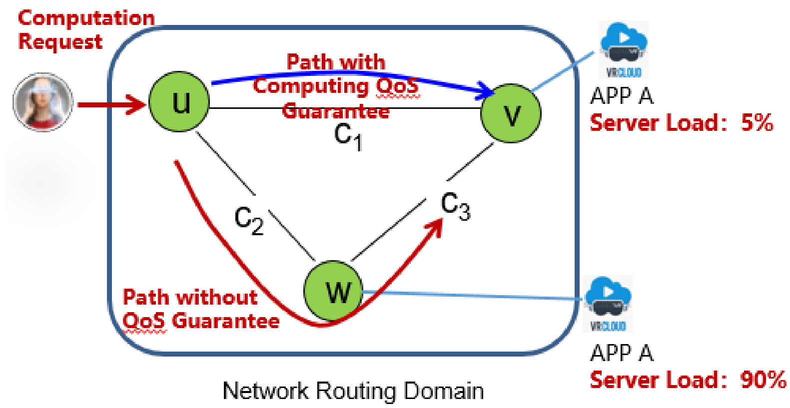


Figure 11 Path with computing QoS guarantee

2) No expensive load balancer within or across edge sites.

Typically, external load balancers have to be deployed to distribute traffic between servers in a data center. The number of load balancers is proportional to the number of edge sites, which are expensive in the scenario of edge computing. In addition, it is difficult to load balance across multiple sites. In comparison, the compute-aware routing takes charge of load balancing function which is distributed within the network routers. Thus it saves the deployment cost of external load balancers.

3) The computing network solution is more suitable than a traditional IT solution.

<table>
<tr>
<td></td>
<td>
<table>
<tr><th>Cloud Computing</th><th>Edge Computing</th></tr>
<tr><td>+Small number of cloud providers
+Small number of DC sites
+Cloud services have low requirements on networks</td><td>+Large number of computing power providers
+Large number of EC sites
+New services (e.g., AI) have high requirements on networks</td></tr>
</table>
The above table shows different feature comparison between cloud computing and edge computing.
As for a traditional IT solution, network information is open to cloud service providers. App-layer central controller selects the computing location and path for consumer. It relies on a central controller or its equivalence at the application layer acting as an intermediary between the client and the computing application service, and collecting global information with network topology, computing instances, and host context. All information needs to be remotely collected to the central controller at a higher location through the network, and the response is relatively slow. In a traditional Web service scenario, the service must be registered in the centralized service registry by the Web service provider, and the client must look up a location on a specific server before invoking the service. There are significant limitations in scalability, cost and latency of controlling traffic, single points of failure, and vulnerability to DDOS attacks.
In comparison, the central controller is replaced by compute-aware routers in the computing network. Network and computing resource information are aggregated to the distributed control plane of routers for unified scheduling and load balancing. All information is transmitted only between adjacent routers, instead of being collected by the central controller at a high location through the network. This reduces the global control traffic and control delay. The service registration is replaced by declaring function availability in the router. There is no service registration center, and no extra registry center component is required. No service location query is required, reducing the service delay. When a service is invoked, the FIB addressing is directly performed without addressing a specific server. Thus, it improves scalability, prevents single points of failure, and provides strong anti-DDoS capabilities.
4) It is based on standardized protocol (e.g., IGP/BGP) interface instead of proprietary interface between IT provider (e.g., computing provider) and Network Infrastructure Provider. And thus it can prevent vendor lock-in issue.
</td>
</tr>
<tr>
<td>Related and Derivative Use Cases</td>
<td>Edge to Edge Collaboration
Computing power transaction</td>
</tr>
<tr>
<td>Inputs to high level requirements</td>
<td>

The computing container should be able to run the routing protocol and advertises the computing capability and the function IDs, which it supports as routing information to the routers in the MCN. A computing container can be a site, server, VM, or container.
The routing protocol (e.g., IGP/BGP) is used in the distributed MCN control plane in order to automatically select a proper edge-computing node or site for computation tasks or data sent from Computing Consumers.
A router computes a route for computation tasks or data based on both the

</td>
</tr>
</table>

	computing capabilities and the network capabilities.

5.4 Seamless Edge Cloud Networking

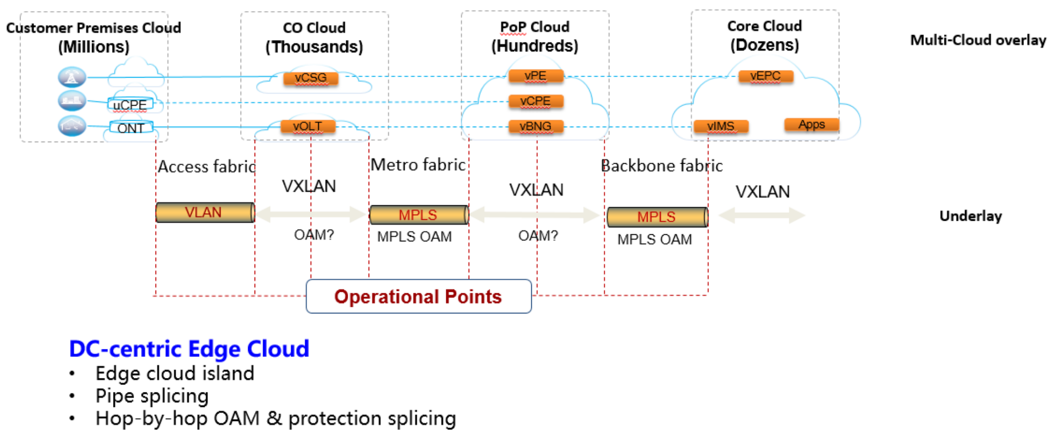
<table>
<tr><td>Title</td><td>Seamless Edge Cloud Networking</td></tr>
<tr><td>Story Highlights</td><td>In order to address "cloud isolated island", the approach of seamless edge cloud networking from CPE/AN to Edge Cloud is proposed based on the extension of segment routing technology for the support of not only network programming but also computing programming. It changes edge clouds from DC-centric to network-centric for the purpose of reduction of the number of operational points and OPEX.</td></tr>
<tr><td>Business Drivers or Issues Being Addressed</td><td>


Figure 12 Cloud isolated island issues at Edge

After the telecom network is cloudified, if simply copying DC technologies to edge, a "cloud isolated island" problem will occur, which is illustrated in Figure 12. Different cloud islands can only be connected through heterogeneous technologies such as VXLAN, Ethernet, or MPLS/IP. In such multi-cloud networking scenarios, pipe stitching increases the number of operational points operations. During the deployment of new services, the technical boundary is frequently configured and even VLAN planning is performed. In addition, hop-by-hop OAM/ protection combination is required. The OPEX is hard to reduce.</td></tr>
<tr><td>Actors</td><td>Network Infrastructure Provider
Computing Consumer
Computing Provider</td></tr>
</table>

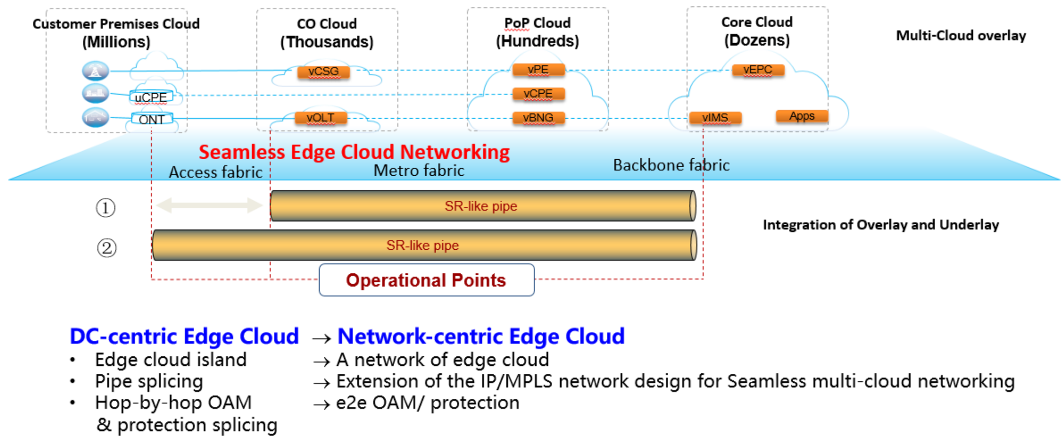
<table>
<tr>
<td>High-level architectural context</td>
<td>


Figure 13 Seamless Edge Cloud Networking

An approach of seamless edge cloud networking is introduced in Figure 13 through the e2e SR-like computing pipe from CPE/AN to Edge Cloud. The endpoint of the computing pipe can be a router or a CPE device of a computing consumer. The segment routing v6 can be extended into the edge cloud to support not only network programming but also computing programming.

In order to support computing programming, a functional program consisting of an order set of function IDs is used to indicate an order set of computation processing instructions. Each function ID identifies a computation processing instruction or instance. The functional program should be obtained by the endpoints of the computing pipe and be carried within the computation packets, which can be based on segment routing technology.

Based on the sequence of the functional program, the computation packets are forwarded and processed by the ingress, intermediate, and egress node in the computing path. These nodes can be CO Cloud nodes or PoP Cloud nodes which hold or connect to the computing containers for computing function processing according to the function ID.

Usually, the first function ID in the functional program is the defaulted index used by FIB/RIB lookup for the corresponding output port. The function ID should be removed from the functional program after corresponding function processing. Or a segments left field in the segment routing sub-header can be used as a function ID pointer.

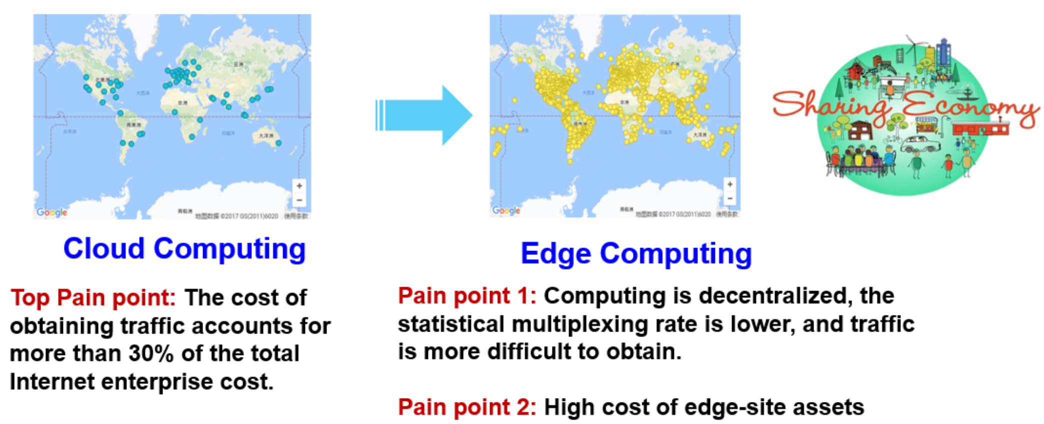
In this way, an edge cloud can be changed from DC-centric to network-centric; i.e., it is proposed to extend the legacy IP/MPLS technologies in the MAN into the edge cloud, rather than 100% copy DC technologies to the edge cloud. It turns the “edge cloud isolated islands” into a “network of edge cloud”. It changes the pipe splicing among islands to seamless multi-cloud networking through extension of the IP/MPLS network design into edge cloud. It replaces Hop-by-hop OAM and protection splicing with e2e OAM/ protection. Thus, the Device-Edge-Cloud convergence become possible.
</td>
</tr>
<tr>
<td>Related and Derivative Use Cases</td>
<td>
Edge to Edge Collaboration
Compute-aware routing
Computing power transaction
</td>
</tr>
<tr>
<td>Inputs to high level requirements</td>
<td>

A seamless edge cloud networking should be implemented through the end-to-end SR-like computing pipe from CPE/AN to Edge Cloud.
The endpoints of the SR-like pipe may be router-based ANs or Aggregation Nodes or CPE devices of computing consumers.

</td>
</tr>
</table>

	• The SRv6 should be extended into the edge cloud to support not only network programming but also computing programming.

5.5 Computing Power Transaction

Title	Computing power transaction through computing token
Story Highlights	To adapt to the development of an intelligent society, a new business model that dynamically and quickly matches the preceding supply-demand relationship is as follows: Internet companies rent edge computing power from carriers on demand, and traffic is obtained from carriers' MCN, thereby saving a large amount of investment in heavy assets of edge computing and traffic acquisition costs. Carriers release edge equipment rooms and network cloudification advantages to monetize network connections and edge digital assets (computing and storage).
Business Drivers or Issues Being Addressed	 **Figure 14 Pain point of Internet companies** Core Competitiveness of Internet Industry is traffic. At present, the Top Pain point of Internet company is that the cost of obtaining traffic accounts for up to 30% of the total enterprise cost. Traditional Internet traffic obtaining methods include search engines, aggregation websites, and portal websites, such as Google, App stores etc. How to obtain traffic at low cost is always a big problem for Internet enterprises. However, in the trend of edge computing, the top pain point of Internet companies is even worse. Due to the high distribution degree of edge computing, the statistical multiplexing ratio of computation power is lower, and the traffic obtaining is more difficult. In addition, it even introduces another pain point: The cost of edge-site assets is very high. Therefore, the Internet industry needs a low-cost sharing economic solution to address this pain point. There are business opportunities as well as challenges in the wave of edge computing deployment. • For carriers: How can the advantages of edge equipment rooms and NFV be released? How to monetize “edge digital assets (computing and storage)"? • For Internet companies: How can the digital assets be shared and the traffic be driven from carriers to OTTs on demand, so that both traffic obtaining costs and heavy assets cost can be saved?
Actors	Network Infrastructure Provider

<table>
<tr><td></td><td>Computing Consumer
Computing Provider</td></tr>
<tr><td>High-level architectural context</td><td>

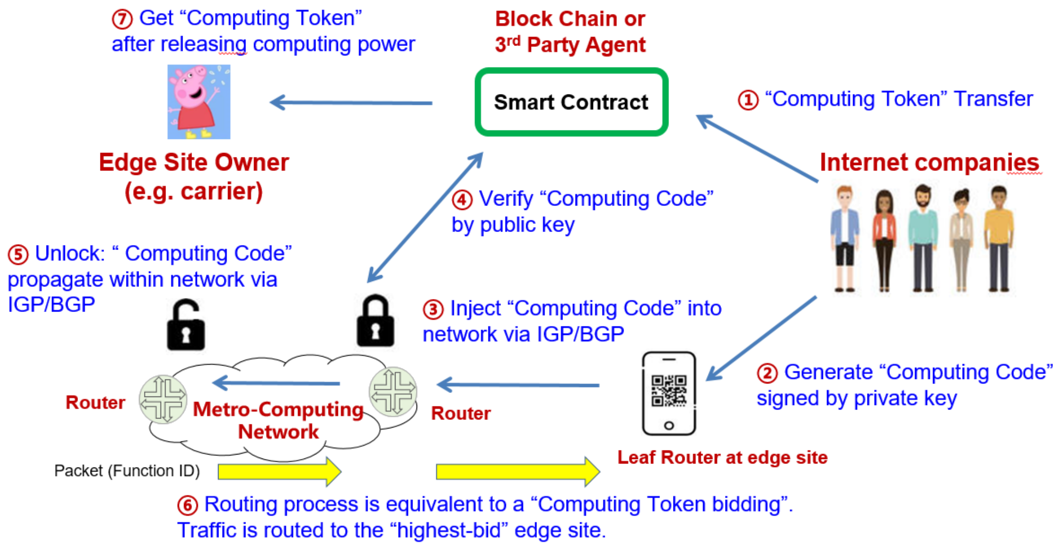


Figure 15 Computing power transaction through computing token

The concept of "Computing Token" is introduced for a new business model between carriers and Internet companies. Internet companies are the consumer of edge computing power. Carriers have a large number of edge sites and are the owner of edge computing power. The computing power of edge sites becomes an independent service for the Internet. Carriers' edge computing resources are priced based on certain rules for example "computing token". And the accounting and settlement are performed based on the blockchain.

A computing power transaction through computing token is proposed in Figure 15.

1) Internet companies and carriers agree on the rent of computing power through Smart Contract. Based on the computing capability provided by carriers at edge site, the Internet Company transfers the corresponding amount of "computing token" to the Smart Contract.

2) The Internet company generates the "Computing Code" according to the "computing token" transfer, signed by its private key.

1) The leaf router at edge site obtains the signed "Computing Code" from the Internet company and injects compute-aware routing information, including "Computing Code", into the routers in the metro-compute network via IGP/BGP. Each computing container can run as a leaf router as explained in the use case of compute-aware routing.

2) The routers in the metro-compute network verify "Computing Code" by public key and inform the Smart Contract of the verification information;

3) If the "Computing Code" is valid, the computing network will unlock: "Computing Code" propagate within routers in the metro-compute network via IGP/BGP and generate the corresponding entries in RIB which includes network metrics, computing metrics, and function ID；

4) The routing process is equivalent to a "Computing Token bidding". The compute-aware routers use both network metrics and computing metrics derivative from Computing Code in RIB to calculate and select a best computing service route toward an appropriate computing container. Thus, generate the corresponding forwarding

</td></tr>
</table>

	entries in FIB which includes function ID and its output port. Traffic carrying the function ID from the computing consumer will be routed to the "highest-bid" edge site of the Internet company for the computing function processing accordingly. 5) After guiding the calculation traffic and releasing computing power, the carriers will get the corresponding amount of "Computing Token" from Smart Contract. Under the new business model, the "Computing Token" is the business abstraction of computing capability provided by a carrier. And the "Computing Code" is the technical abstraction of computing capability of a carriers' edge site. The "Computing Token" is used in the network in the form of "Computing Code". The computing capability level, server load, machine type, the delay evaluation value and function ID which is supported by the computing container etc. can be encoded as "Computing Code". The routers will generate computing metric according to computing code. A function ID can be a hash value of URI or an IP address prefix or a network address. A function identified by a function ID can be a computing program, a function program, a service software, or a microservice deployed in the computing container.
Related and Derivative Use Cases	Edge to Edge Collaboration Compute-aware routing Seamless Edge Cloud Networking
Inputs to high level requirements	• The "Computing Token" is a business abstraction of edge computing capability provided by a carrier. • The "Computing Code" is a technical abstraction of computing capability of a carriers' edge site, which encodes computing capability level, machine type, server load, or computing latency etc. • A router in the metro-compute network obtains "Computing Code" from edge site via IGP/BGP and uses both network metrics and computing metrics derivative from Computing Code to calculate a computing service route. • The computing token transfer, the accounting and settlement should be performed based on the blockchain or 3rd party agent between owners of edge computing power (e.g., carriers) and consumers of edge computing power (e.g., Internet companies).

5.6 Edge-Computing Overlay Network

Title	Edge-Computing Overlay Network
Story Highlights	A metro-compute network architecture is proposed. It consists of two layers: the underlay network and the edge-computing overlay network. Four edge-computing network functions at overlay layer are introduced in order to support incremental deployment and protect operator's legacy investment. This use case is intended to be built and supported over the existing network and user plane which is distributed over multiple edge (e.g., Cloud CO) sites and is very difficult to have a centralized control. It has to rely on the Metro-compute network (i.e., edge cloud fabric) to select the suitable edge sites for computing tasks on demand based on distributed protocols. However, the edge-computing network functions at overlay layer are typically deployed as VNFs in the Cloud CO sites and thus are constrained by the control plane of CloudCO reference architecture in TR-384.

<table>
<tr><td>Business Drivers or Issues Being Addressed</td><td>To be aware of edge-computing service, each router in the aggregation network or backbone network may have to be upgraded. Whether or not the compute-aware routing function can be incrementally deployed is one of the key aspects to protect an operator’s legacy investment.

When the end-host information from the edge clouds propagate into the aggregation network or backbone network for optimizing edge-computing routing, the underlying infrastructure address space will tightly couple with the end-host address space. The large scale of address space will lead to FIB explosion and slow convergence of routing table.</td></tr>
<tr><td>Actors</td><td>Network Infrastructure Provider

Computing Consumer

Computing Provider</td></tr>
<tr><td>High-level architectural context</td><td>

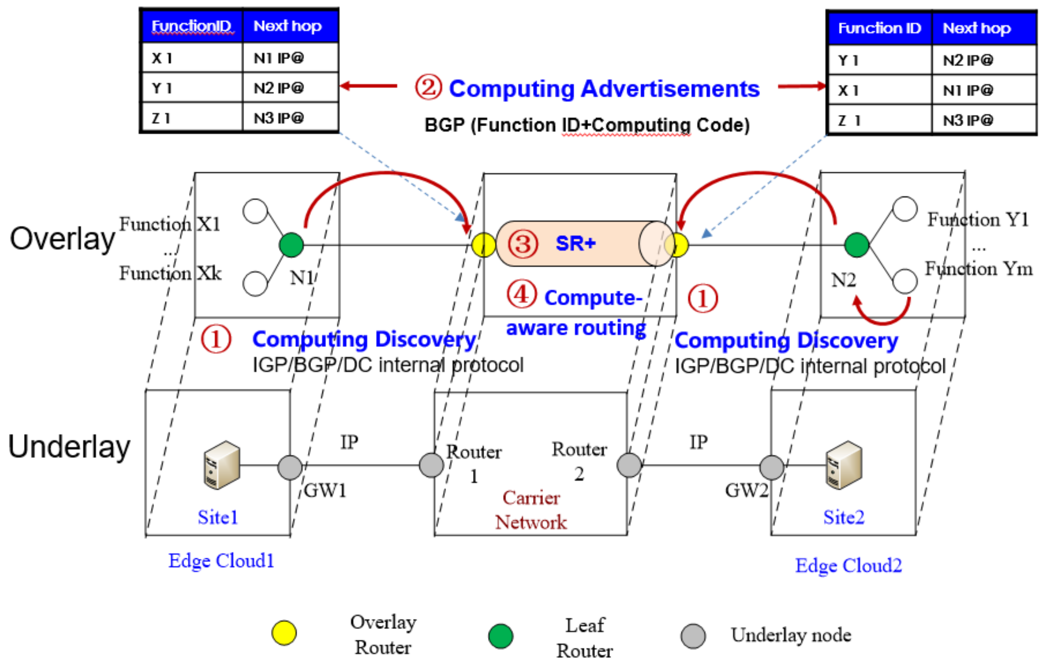


Figure 16 Metro-compute network Architecture1

A metro-compute network architecture consists of edge cloud sites being interconnecting through a cloud fabric, shown as a carrier network in Figure 16, provided by a Network Infrastructure Provider. The MCN is divided into two layers: the underlay network and the edge-computing overlay network.

The underlay network is the aggregation network or backbone network which is typically based on IP/MPLS technologies according to TR-101 [3] or TR-178 [4]. The edge-computing overlay network are virtual networks of interconnected nodes that share an underlying physical network, allowing deployment of edge-computing service functions or network functions such as compute-aware routing functions etc. that require specific network topologies without the need to modify the underlying network. The compute-aware routing functions, shown as an overlay router function in Figure 16, are typically deployed at the edge nodes of the underlay network. These edge nodes are ingress or egress compute-aware routers.

Leaf routers at computing containers are external extensions of the computing network for sensing the computing capability and services at edge cloud sites. Functional programs, service software, or micro-services can be deployed at edge sites, that is,

</td></tr>
</table>

Function X1...Function Xk or Function Y1...Function Ym in Figure 16.

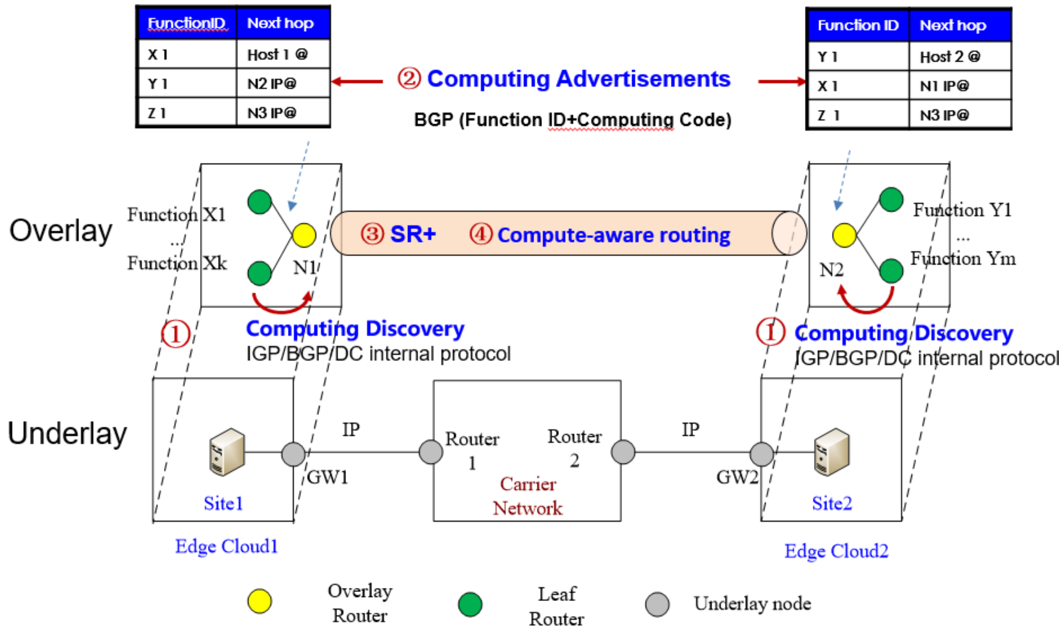


Figure 17 Metro-compute network Architecture2

The differences between the network in Figure 17 and that in Figure 16 is that the overlay router function implement within the edge sites instead of within the carrier network. Thus operators only need to upgrade the devices at edge sites and can protect the legacy investment at the carrier network.

There are four edge-computing network functions at the overlay layer:

1) Computing power and function discovery:

This function, which is supported by the leaf routers at edges, is responsible for discovery and aggregation of the compute-aware routing information, including the computing capability of the computing container, the identifier of the functions or services served by the computing container and/or the IP address or prefix of the computing container, and the advertisement of this routing information into the compute-aware routers in the MCN. This in-site advertisement should be implemented by extending IGP/BGP, i.e., propagating virtual link state to indicate a computing capability of the computing container and the function identifier from the computing container to the compute-aware routers.

2) Compute-aware routing information advertisements:

This function, which is supported by the compute-aware routers in the MCN, is responsible for the propagation of the compute-aware routing information within routers in the metro-compute network via IGP/BGP and the generation of the corresponding entries in RIB which includes the network metrics, the computing metrics and the function identifier. This inter-site advertisement should be implemented by extending routing protocols such as IGP/BGP.

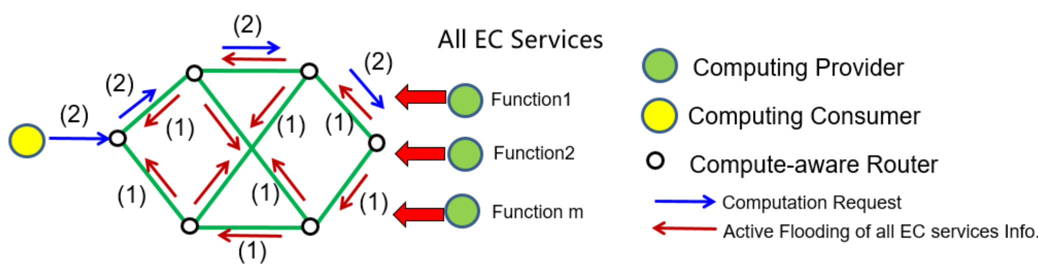
3) Compute-aware forwarding:

Nodes in the edge-computing overlay network can be thought of as being connected by virtual links, each of which corresponds to a computing path or tunnel, perhaps through many physical links, in the underlying network. The FIB lookup and forwarding at the routers in the computing path towards the corresponding egress router address or output port should be implemented by extending segment routing or other technologies according to the identifier of computing function.

	4) Compute-aware route calculation: This function, which is supported by the compute-aware routers in the MCN, is responsible for route calculation based on both the computing metric and the network metric, which are derivative respectively from computing capabilities (e.g., throughput, server load and computing delay) and the network capabilities (e.g., BW and network delay) so that it will automatically load balance the computation tasks or data from ingress routers to egress routers and proper edge-computing nodes/sites. Benefits of the edge-computing overlay network include the following: • Optimized device functions: Edge-computing overlay networks allow the separation (and specialization) of device functions based on where a device is being used in the network. An edge node or leaf router device can optimize its edge-computing functions and all its relevant routing protocols based on end-state information and scale, and an intermediate node or underlay device can optimize its functions and protocols based on link-state updates, optimizing with fast convergence. • Fabric scalability and flexibility: Overlay technologies allow the network to scale by focusing scaling on the overlay edge nodes. With overlays used at the fabric edge, the intermediate nodes or underlay devices are freed from the need to add end-host information to their forwarding tables. • Overlapping addressing: The overlay technologies used in the MCN allow virtual network IDs or network slicing to uniquely scope and identify individual private networks. This scoping allows potential overlap in function IDs and IP addresses between tenants. The overlay encapsulation also allows the underlying infrastructure address space to be administered separately from the tenant address space.
Related and Derivative Use Cases	Compute-aware routing Seamless Edge Cloud Networking Computing power transaction through computing token
Inputs to high level requirements	• A metro-compute network architecture should be divided into two layers: the underlay network and the edge-computing overlay network. • An overlay function of computing power and function discovery should be supported by the leaf routers at edges responsible for discovery and advertisement of the computing capability and the identifier of the functions or services served by the computing container to the compute-aware routers via IGP/BGP. • An overlay function of compute-aware routing information advertisements should be supported by the compute-aware routers to propagate the compute-aware routing information within compute-aware routers via IGP/BGP and generate the corresponding entries in RIB/FIB. • An overlay function of compute-aware forwarding should be supported by the ingress routers or egress routers in the computing path by extending segment routing based on function IDs. • An overlay function of compute-aware route calculation should be supported by the

	ingress routers or egress routers in the computing path for the support of inter-site load balancing or in-site load balancing for edge-computing services.

5.7 Popularity-based Overlay Routing

Title	Popularity-based Overlay Routing
Story Highlights	An overlay routing network use case is proposed which is composed of an underlay layer maintaining the full MCN topology and calculates the shortest-path trees, and an overlay layer providing edge-computing services in two ways: active publishing and passive serving. The overlay routing is based on a popularity-based routing policy which can reach a compromise between the active and passive methods and overcome the problem of traffic and RIB/FIB explosion.
Business Drivers or Issues Being Addressed	A traditional host is passively assigned an IP address by an ISP, and it uses the IP address to communicate with other hosts via address-based IP routing. In order to be aware of edge computing service, the compute-aware routing is proposed. However, compute-aware routing is Function-ID-based, instead of passive address assignment, a computing container should actively advertise/publish its computing capability and all the function IDs of edge computing services it wants to serve to the routers in the MCN via routing protocols.  **Figure 18 Active Flooding of all EC services Info.** These advertisement packets are propagated throughout the entire MCN domain, and every compute-aware router builds its RIB/FIB based on received announcements. Edge computing requests or data are routed to the computing containers by looking up the RIB/FIBs. Naively flooding these advertisements may lead to tremendous traffic. Moreover, each advertisement will be recorded in the RIB/FIB of each compute-aware router, thus publishing all edge computing functions or services will result in an RIB/FIB with numerous entries, i.e., RIB/FIB explosion.
Actors	Network Infrastructure Provider Computing Consumer Computing Provider
High-level architectural context	As proposed in the use case of Edge-Computing Overlay Network, each compute-aware router in the MCN has both underlay routing network functions and overlay network functions of compute-aware routing. The underlay routing network function is basically engaged in topology discovering, node/link failure handling, and shortest-path tree calculating, shown in Figure 19, which resembles link state information exchange functionality. The shortest-path tree comprises the shortest paths from the calculating router to each other router in the network.

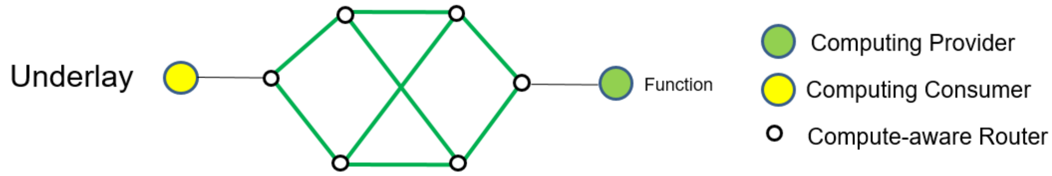


Figure 19 Shortest-path tree calculating at underlay layer

The overlay network functions of compute-aware routing is responsible for providing edge-computing services in both active publishing mode and passive serving mode.

In active publishing mode shown in Figure 20, the overlay network functions conducts efficient compute-aware routing information advertisements and RIB/FIB building. Firstly, when each computing container of a computing provider actively publishes/advertises the compute-aware routing information of edge-computing services or functions it can serve to an edge router, this compute-aware router ONLY disseminates the compute-aware routing information of hot services or functions to all other compute-aware routers in the MCN via the shortest-path trees obtained by the underlay routing network function instead of flooding. Each router generates or updates its RIB/FIB entry based on the received compute-aware routing information and the corresponding output port or next hop address. Secondly, when a computing consumer initiates a computing request for a hot service or function, the compute-aware routers forward the computing request towards the proper computing container serving this hot service or function. Finally, the computing provider replies the computation result/response to the computing consumer.

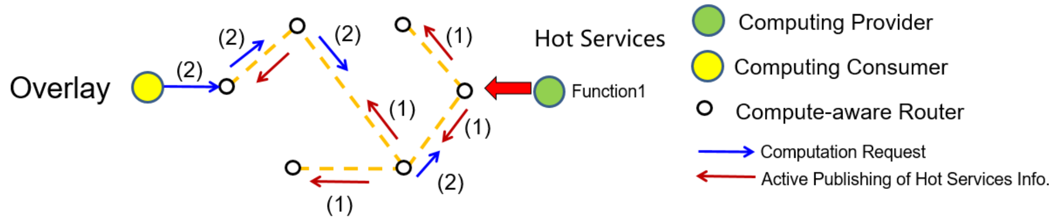


Figure 20 Active Publishing of Hot Services at overlay layer

In passive serving mode shown in Figure 21, the overlay network functions conducts efficient computing power and function subscription and RIB/FIB building. Firstly, when a cold service or function is requested for the first time by a computing consumer, the corresponding computation request packet will be forwarded through the shortest-path trees obtained by the underlay routing network function instead of flooding. The computation request packet will become a subscription packet propagating over the shortest-path trees to all other compute-aware routers in order to subscribe a function code or a computation result. Each compute-aware router generates or updates the function ID and output port in its RIB/FIB entry based on the function identifier carried in the computation request/subscription packet and the input port of this packet. Secondly, the computing provider publishes the functions code or computation result to the computing consumers according to the computation request/subscription. The compute-aware routers forward the corresponding packets based on the function identifier lookup in the FIB via the output port towards the computing consumer.

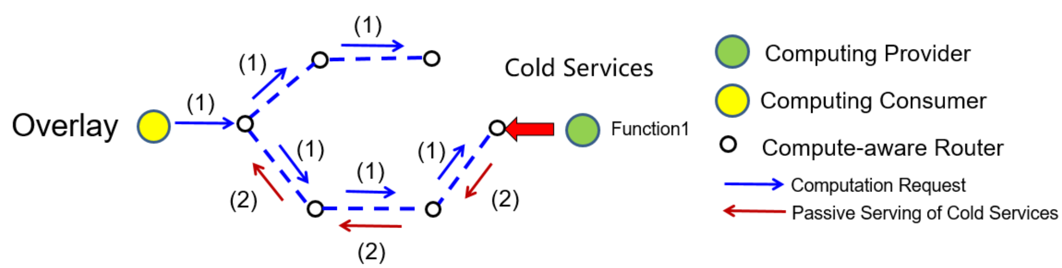


Figure 21 Passive Serving of Cold Services at overlay layer

In order to find a compromise between active publishing and passive serving, we propose that the computing provider actively announce the popular/hot EC services or functions, and the unpopular/cold EC services or functions be passively served. We define the access frequency as the popularity property of an EC service or function. The popularity value is used to indicate whether or not it is a popular service or function. When the popularity exceeds a threshold, it becomes a popular EC service or function and the compute-aware routing information gets published by the compute-aware router to all other routers in the MCN via the shortest-path trees.

A compute-aware router can suppress its RIB/FIB size by adopting a popularity threshold, as illustrated in Figure 22. And this requires computing providers add popularity property in its advertisement of compute-aware routing information. Once a router receives an advertisement of a function ID A, it first compares A's popularity with its threshold p and determines whether this function is hot or cold. The router inserts the compute-aware routing information into RIB/FIB if it is hot or ignores it if it is cold. In each RIB/FIB, the popularity of an EC service or function is not constant, but varies. And the router can determine to delete an entry if its popularity degrades to less than the threshold.

In the active publishing mode, an entry with a hot function ID has been generated in the RIB/FIB and the compute-aware routers should be able to forward the computing request packet based on the function ID via the output port towards the proper computing container. However, in the passive serving mode, because an entry with a cold function ID does not appear in the RIB/FIB, a received computation request packet carrying this cold function ID has to be converted by the compute-aware router as a subscription message propagating over the outputs of the shortest-path trees to all other compute-aware routers.

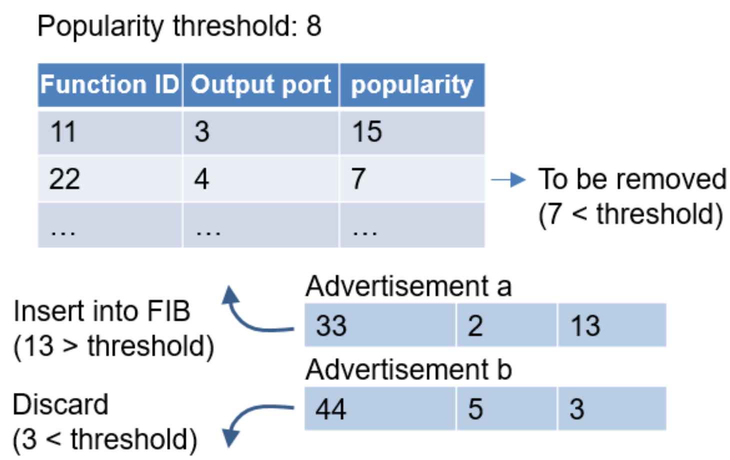


Figure 22 Popularity-based FIB size suppression

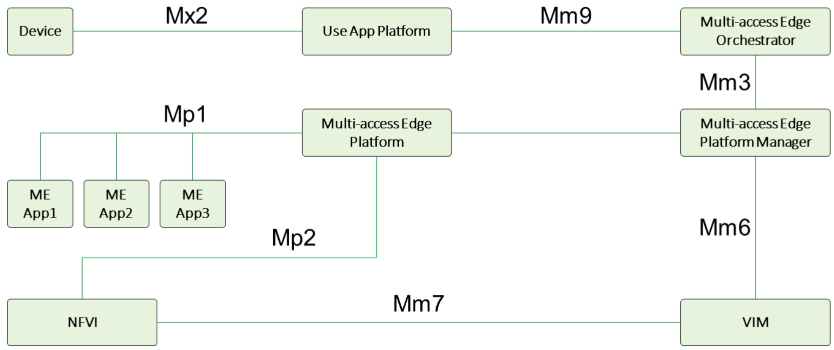
Benefits:

1) The overlay compute-aware routing network decouples the advertisement or subscription forwarding of compute-aware routing information and RIB/FIB building from topology maintaining. Each layer focuses on its own responsibilities. The underlay layer maintains the topology information, and the overlay layer efficiently forwards advertisements or subscriptions via the shortest-path trees, keeping the advertisement or subscription traffic to a minimum in both modes. If we define Routing Efficiency(RE) = Number of flooring messages / Number of overlay routing messages, Mathematical analysis results show that RE is quite large and proportional to the number of network nodes *n*.

	2) It is known that active publishing method achieves much higher efficiency than passive serving method, but solely adopting it will lead to the problem of RIB/FIB explosion. By proposing a popularity-based active publishing policy, a compromise between the two methods is reached.
Related and Derivative Use Cases	Edge-Computing Overlay Networking Compute-aware routing Seamless Edge Cloud Networking Computing power transaction through computing token
Inputs to high level requirements	• The underlay routing network function should be supported by the compute-aware router responsible for topology discovering, node/link failure handling, and shortest-path tree calculating. • The overlay network functions of compute-aware routing should be supported by the compute-aware router responsible for providing edge-computing services in both active publishing mode and passive serving mode. • The popularity property should be included in the compute-aware routing information based on which the compute-aware router should compare the popularity in the received compute-aware routing information with its popularity threshold and determine whether or not to insert the received compute-aware routing information into RIB/FIB.

5.8 Multi-access Edge Computing in MCN

Title	Multi-access Edge Computing into MCN
Story Highlights	Multi-access Edge Computing (MEC) describes a multi-access edge system that enables edge applications to run efficiently and seamlessly in a telecommunication network. ETSI MEC also describes solutions that allow the deployment of MEC in a NFV environment by including recommendations as for where the specification work needs to be done.
Business Drivers or Issues Being Addressed	Once Metro Edge Computing has been developed and deployed by an operator, it could be interested to create an environment where third party partners can deploy their own applications by using standard interfaces developed by ETSI MEC (Multi-access Edge Computing). Moreover, ETSI MEC already developed the reference architecture and related interfaces for having a standard environment for telco apps (ETSI GS MEC-003) and it has already integrated the reference architecture in a NFV environment (ETSI GR MEC-017).
Actors	Network Infrastructure Provider Computing Consumer Computing Provider
High-level architectural context	Simplified Reference Architecture (ETSI GS MEC-003) illustrated in Figure 23:

	 **Figure 23 Simplified Reference Architecture** The interfaces are the following: - **Mp1**: The Mp1 reference point between the mobile edge platform and the mobile edge applications provides service registration, service discovery, and communication support for services. It also provides other functionality such as application availability, session state relocation support procedures, traffic rules and DNS rules activation, access to persistent storage and time of day information, etc. This reference point can be used for consuming and providing service specific functionality. - **Mp2**: The Mp2 reference point between the mobile edge platform and the data plane of the virtualisation infrastructure is used to instruct the data plane on how to route traffic among applications, networks, services, etc. This reference point is not further specified. - **Mm3**: The Mm3 reference point between the mobile edge orchestrator and the mobile edge platform manager is used for the management of the application lifecycle, application rules and requirements, and keeping track of available mobile edge services. - **Mm6**: The Mm6 reference point between the mobile edge platform manager and the virtualisation infrastructure manager is used to manage virtualised resources, e.g., to realize the application lifecycle management. - **Mm7**: The Mm7 reference point between the virtualisation infrastructure manager and the virtualisation infrastructure is used to manage the virtualisation infrastructure. This reference point is not further specified. - **Mm9**: The Mm9 reference point between the user application lifecycle management proxy and the mobile edge orchestrator of the mobile edge system is used to manage mobile edge applications requested by UE application. This reference point is not further specified. - **Mx2**: The Mx2 reference point between the user application lifecycle management proxy and the UE application is used by a UE application to request the mobile edge system to run an application in the mobile edge system, or to move an application in or out of the mobile edge system. This reference point is only accessible within the mobile network. It is only available when supported by the mobile edge system.
Related and Derivative Use Cases	**Existing use cases**: All the other use cases can reuse ETSI MEC architecture and interfaces to deploy the desired applications.
Inputs to high level requirements	The edge clouds provided by a Network Infrastructure Provider could become a shared infrastructure where 3rd party partners can install and deploy their own applications by means of standard reference points.

6 High Level Requirements from Use Cases

[R-1] The edge clouds provided by a Network Infrastructure Provider should be able to become a pool shared by Computing Consumers for the support of Edge to Edge Collaboration.

[R-2] The aggregation network should be able to become an edge cloud fabric which can direct traffic between different edge sites.

[R-3] The backbone network may be able to become an edge cloud fabric which can direct traffic between different edge sites.

[R-4] Computing task can be offloaded from one edge site to other edge sites through the edge cloud fabric.

[R-5] The multiple edge sites are abstracted by an Edge Node controller just like one cloud.

[R-6] The EN controller support resource tidal scheduling and load balancing function for the support of allocating a proper edge node for edge computing.

[R-7] The computing container should be able to run the routing protocol and advertises the computing capability and the function IDs which it support as routing information to the routers in the MCN. A computing container can be a site, server, VM, or container.

[R-8] The routing protocol (e.g., IGP/BGP) is used in the distributed MCN control plane in order to automatically select a proper edge-computing node or site for computation tasks or data sent from Computing Consumers.

[R-9] A router computes a route for computation tasks or data based on both the computing capabilities and the network capabilities.

[R-10] A seamless edge cloud networking should be implemented through the end-to-end SR-like computing pipe from CPE/AN to Edge Cloud.

[R-11] The endpoints of the SR-like pipe may be router-based ANs or Aggregation Nodes or CPE devices of computing consumers.

[R-12] The SRv6 should be extended into the edge cloud to support not only network programming but also computing programming.

[R-13] The “Computing Token” is a business abstraction of edge computing capability provided by a carrier.

[R-14] The “Computing Code” is a technical abstraction of computing capability of a carriers’ edge site, which encodes computing capability level, machine type, server load, or computing latency, etc.

[R-15] A router in the metro-compute network obtains “Computing Code” from edge site via IGP/BGP and uses both network metrics and computing metrics derivative from Computing Code to calculate a computing service route.

[R-16] The computing token transfer, the accounting and settlement should be performed based on the blockchain or 3rd party agent between owners of edge computing power (e.g., carriers) and consumers of edge computing power (e.g., Internet companies).

[R-17] A metro-compute network architecture should divided into two layers: the underlay network and the edge-computing overlay network.

[R-18] An overlay function of computing power and function discovery should be supported by the leaf routers at edges responsible for discovery and advertisement of the computing capability and the identifier of the functions or services served by the computing container to the compute-aware routers via IGP/BGP.

[R-19] An overlay function of compute-aware routing information advertisements should be supported by the compute-aware routers to propagate the compute-aware routing information within compute-aware routers via IGP/BGP and generate the corresponding entries in RIB/FIB.

[R-20] An overlay function of compute-aware forwarding should be supported by the ingress routers or egress routers in the computing path by extending segment routing based on function IDs.

[R-21] An overlay function of compute-aware route calculation should be supported by the ingress routers or egress routers in the computing path for the support of inter-site load balancing or in-site load balancing for edge-computing services.

[R-22] The underlay routing network function should be supported by the compute-aware router responsible for topology discovering, node/link failure handling, and shortest-path tree calculating.

[R-23] The overlay network functions of compute-aware routing should be supported by the compute-aware router responsible for providing edge-computing services in both active publishing mode and passive serving mode.

[R-24] The popularity property should be included in the compute-aware routing information based on which the compute-aware router should compare the popularity in the received compute-aware routing information with its popularity threshold and determine whether or not to insert the received compute-aware routing information into RIB/FIB.

[R-25] The edge clouds provided by a Network Infrastructure Provider could become a shared infrastructure where 3rd party partners can install and deploy their own applications by means of standard reference points.

Appendix: Recommendations for BBF Work Projects

There is a unique value for operators, that only operators as Network Infrastructure Providers that have already owned a large number of edge sites and will be able to transform to edge-computing provider or edge-computing service provider, especially after SDN/NFV revolution. In the IT world, Internet companies or OTTs will be able to shift to light asset mode through edge-computing power sharing from Telco, save asset investment and O&M Costs of massive distributed edge-computing nodes.

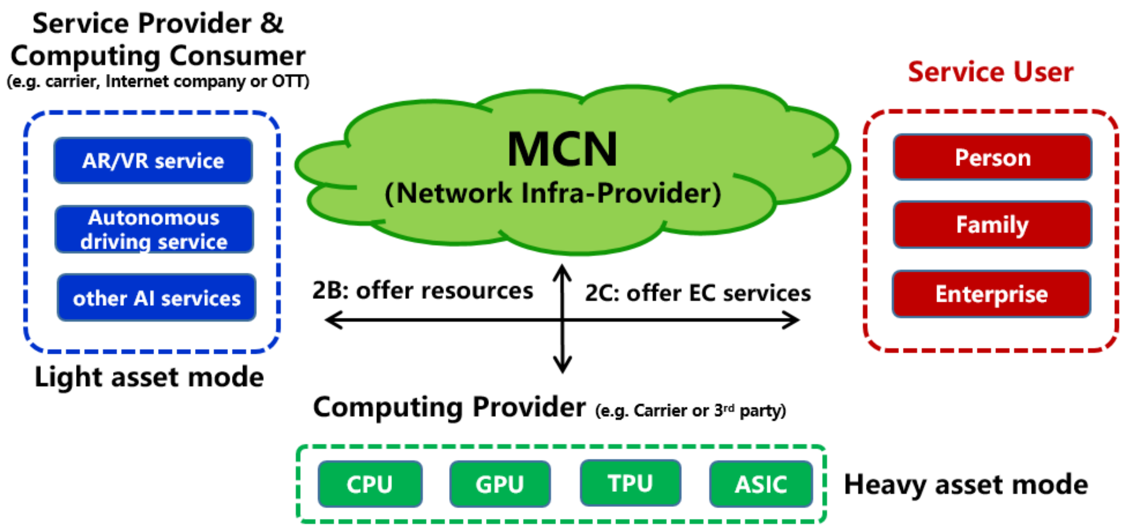


Figure 24 New business model in the intelligent society

The BBF focus is on the broadband network covering CPE, CO, and PoP, which are exactly the Edge Cloud related areas. By exploring a new metro compute networking architecture with in-depth integration of computing and network on top of the cloud-based broadband networks, the BBF society will keep its leading position in the field of multi-service broadband networks.

MCN not only reflects a trend of a new business model in the intelligent society as illustrated in Figure 24, but also represents new cloud-based broadband networks by connecting isolated edge sites (e.g., Cloud CO) as one cloud to serve edge computing services. This leads to a change in the broadband network architecture and functionalities as well as its exposure to the computing consumers (e.g., Internet companies). The main gaps can be grouped in the following areas for implementing the use cases described in this project document:

- MCN reference architecture and requirements

  There are two main gaps: how to integrate the MCN into the MSBN and the CloudCO architecture. The MCN control plane in context of MSBN is illustrated in Figure 25 based on non-MEC service functions, while the MCN control plane in context of MSBN is illustrated in Figure 26 based for MEC service functions. The MCN data plane in context of MSBN is illustrated in Figure 27 and remains the same regardless of the whether MEC or non-MEC service functions are deployed.

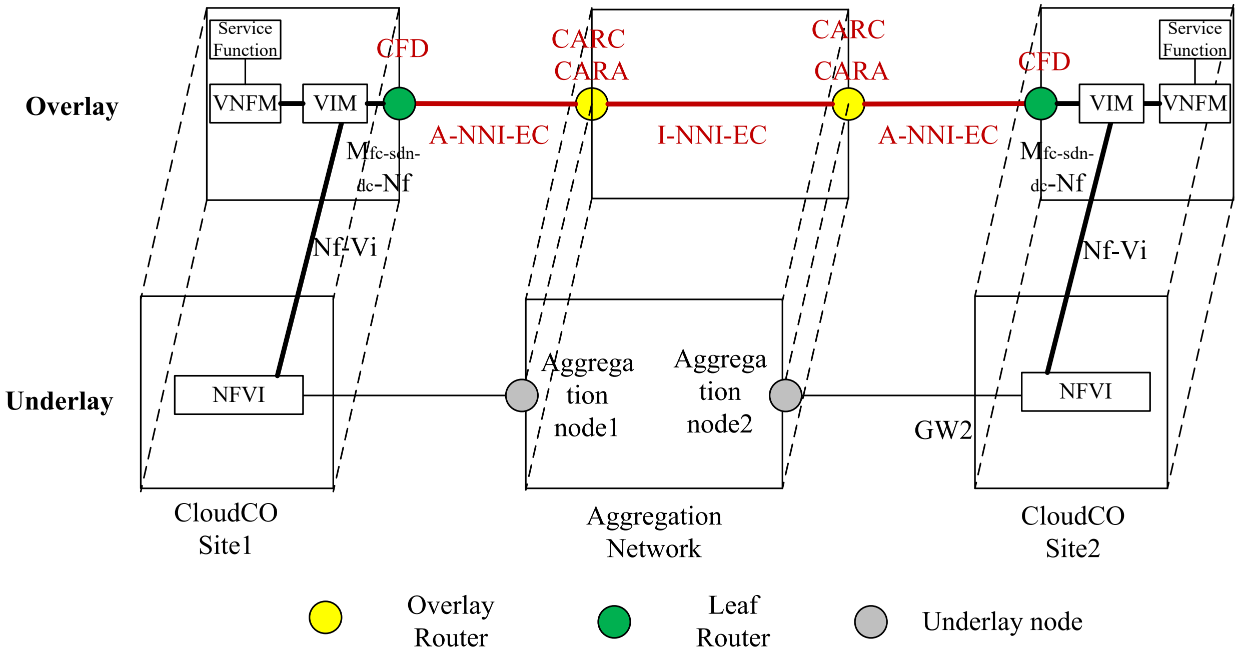


Figure 25 MCN control plane in the context of MSBN for non-MEC service functions

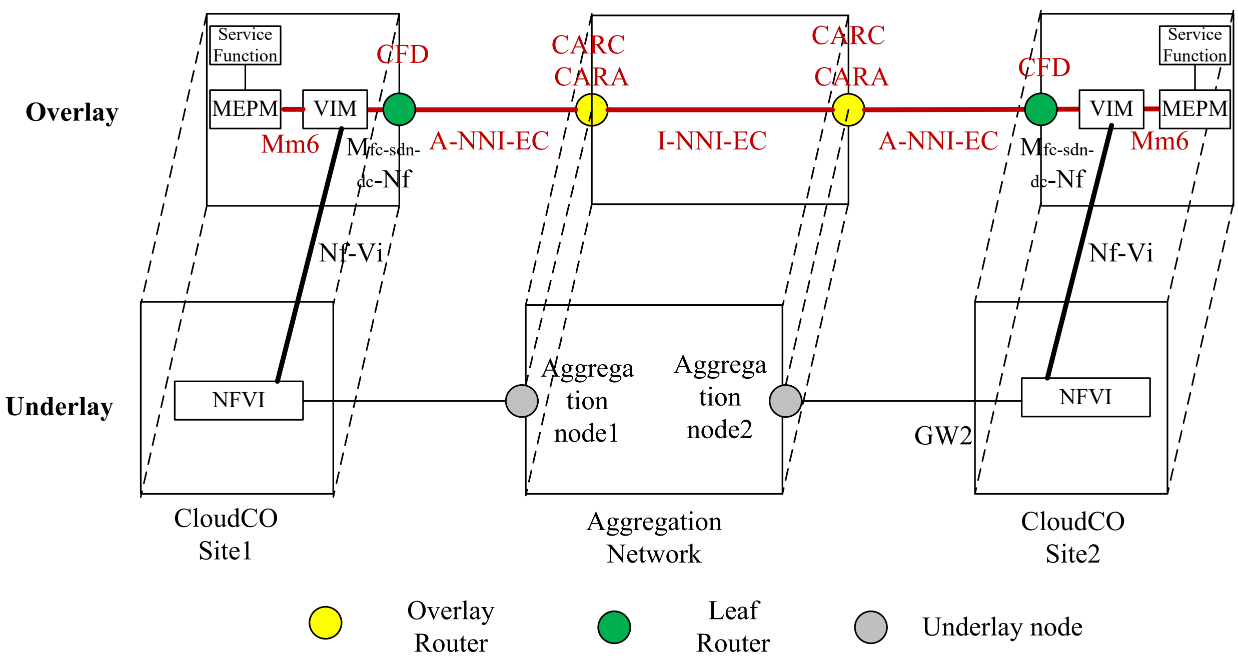


Figure 26 MCN control plane in the context of MSBN for MEC service functions

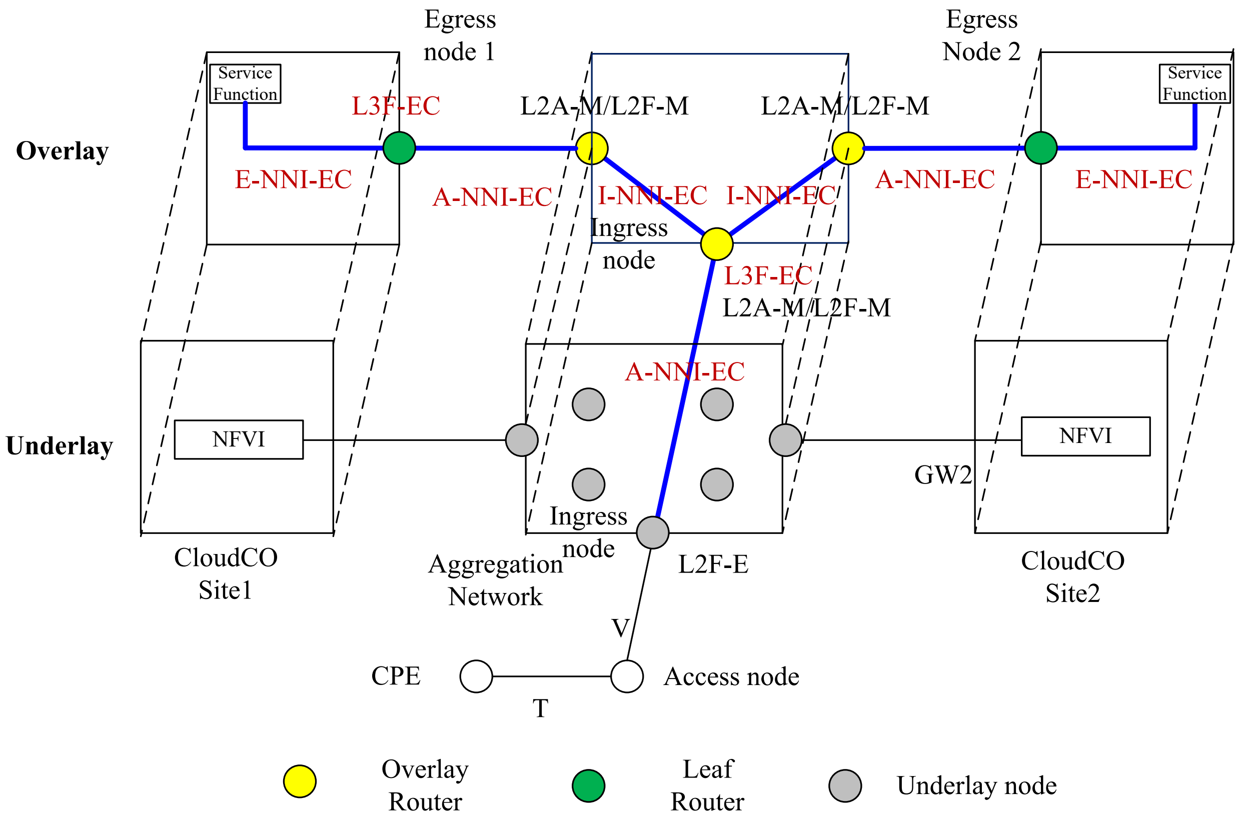


Figure 27 MCN data plane in the context of MSBN

Using the integration approach for the MCN with the MSBN, the MCN can be integrated into the CloudCO architecture. The integration with the CloudCO architecture provides a common framework that enables the operator's ability to create a single environment where its own applications and third party applications can be deployed. The Figure 28 shows a possible approach to deploy applications that are exposed to the MCN.

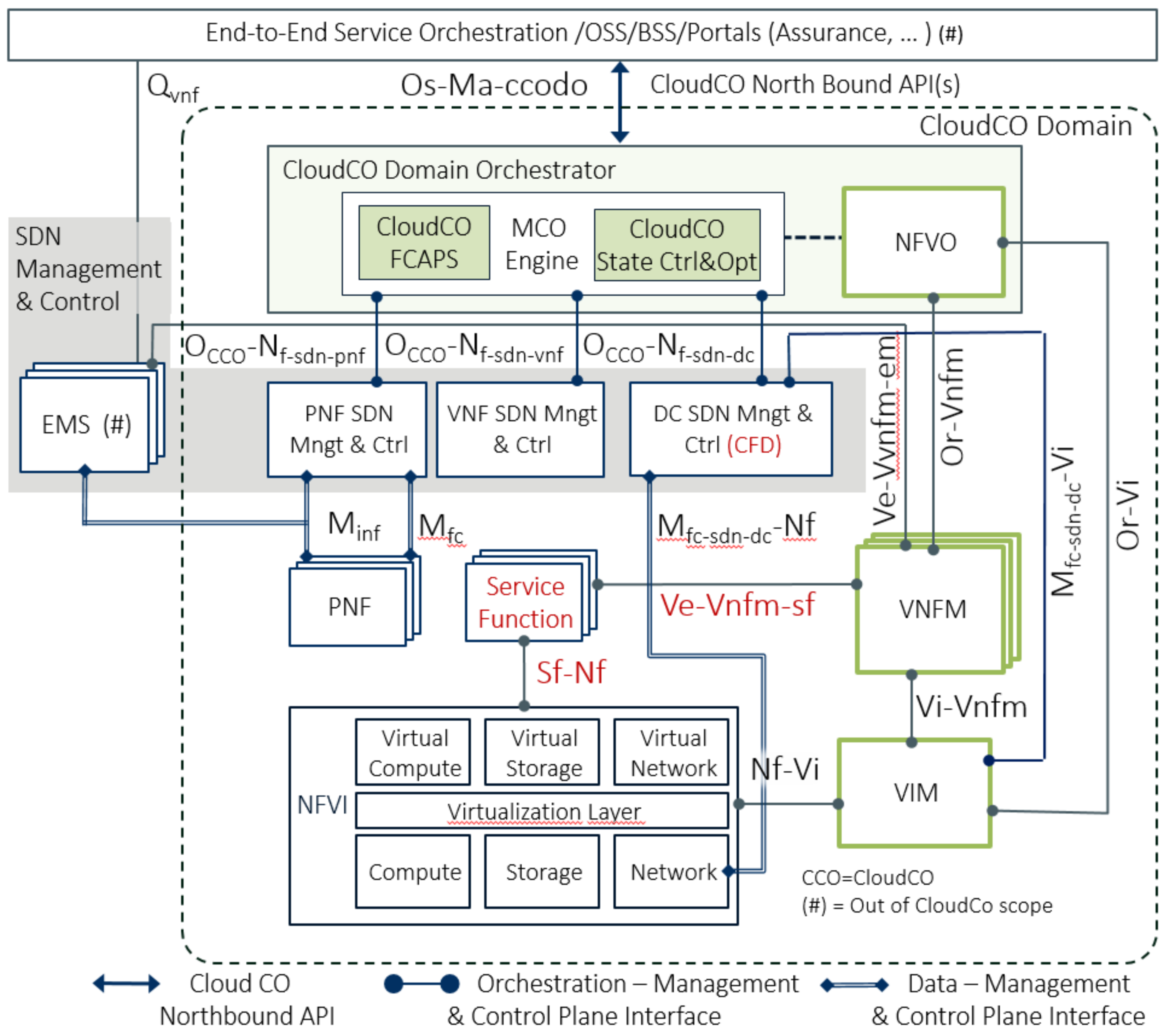


Figure 28 MCN Integration into CloudCO Architecture for non-MEC service functions

The Figure 29 extends the deployment of applications to MEC service functions. In Figure 29, the green boxes represent the CloudCO functional elements, while the yellow boxes represent the Multi-access Edge Computing functional elements.

> **Note:** The Multi-access Edge Orchestrator is shown inside the CloudCO Domain Orchestration function (CCO DO), because logically located at this layer but in many deployments, the Multi-access Edge Orchestrator can be deployed as a separate function elsewhere.

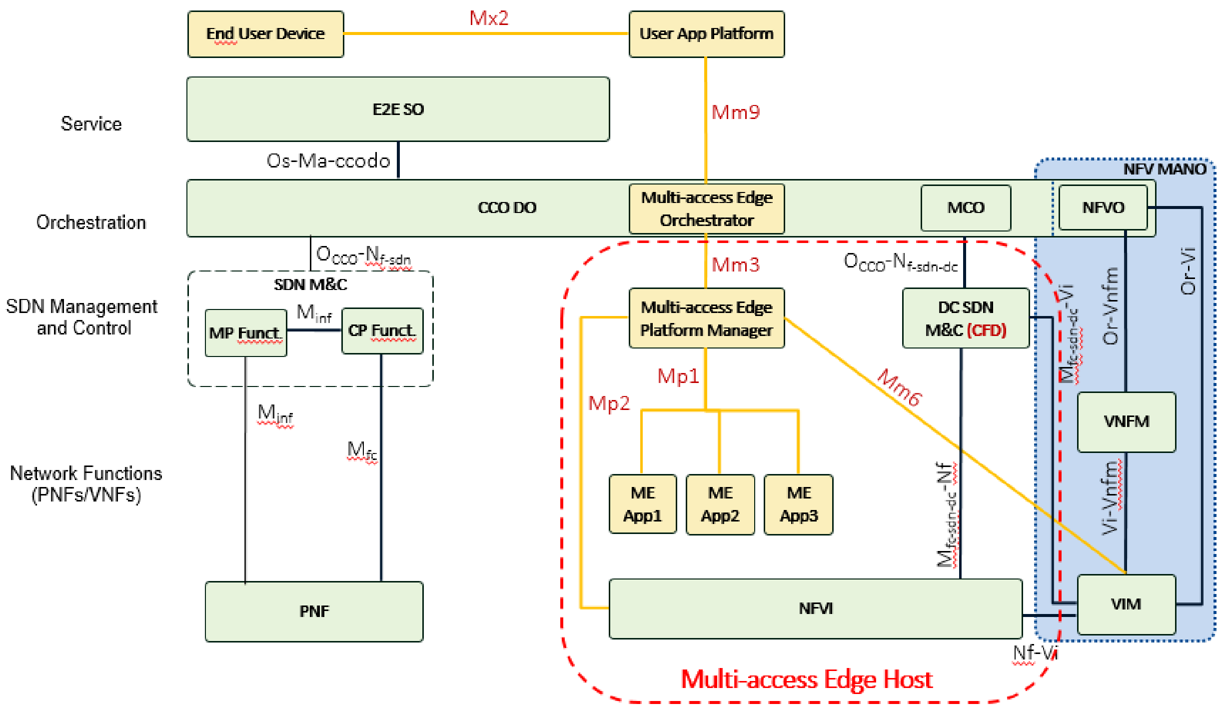


Figure 29 MCN Integration into CloudCO Architecture based on MEC applications

The integration of the MCN into the CloudCO and MSBN architectures requires modifications and extensions to several framework elements (e.g., DC SDN M&C). For example, the edge to edge collaboration, abstracted edge cloud, the seamless edge cloud networking, and edge-computing overlay network as described in this project document will necessitate modifications to the CloudCO interfaces and additional requirements on the functional entities.

Some edge-computing network functions will be deployed as VNFs in the CloudCO sites or as PNFs at aggregation or IP edge nodes. Thus, the functional and nodal requirements, protocols, and interfaces needed to be enhanced to support the MCN capabilities.

The following new functional modules are needed to be incorporated into the CloudCO and MSBN architectures:

- CFD (Computing power and Function Discovery) function at leaf routers is used for discovery of the computing capability and the functions or services served by of the edge sites. CFD function can be supported by DC SDN Managers & Controllers.
- CARC (Compute-Aware Route Calculation) function at the compute-aware routers (e.g., aggregation nodes) is used for the route calculation based on the compute-aware routing information and the generation of the corresponding forwarding entries in FIB.
- CARA (Compute-Aware Routing Information Advertisement) at the compute-aware routers (e.g., aggregation nodes) is used to propagate the compute-aware routing information in the aggregation network.
- L3F-EC (L3F-Edge-Computing) function at the compute-aware routers (e.g., aggregation nodes), for example at the ingress nodes of computing-aware routing domain (e.g., aggregation nodes or even access nodes) and at the egress leaf routers of edge site where edge-computing services are deployed, is used to perform unicast or anycast network connectivity according to the identifier of

computing function, which dynamically directs computing traffic coming from UE to a suitable edge-computing site.

- MCN protocols and interfaces

  Some use cases clearly identify that specific network protocols and interfaces have to be defined in order to correlate computing power information of edge sites (e.g., Cloud CO sites) and network topology information, such that operators can provide customers with optimal computing power selection, allocation, and network connection, and schedule user computational requests to the optimal computing site. The general computing interface between a MCN network node and a computing instance has to be defined to exchange the computing power information. This interface may have to be irrelevant to applications, enabling the metro compute networking to be decoupled from ever-changing application innovations and maintaining its stability. The interface between Computing Provider and Computing Consumer is required to be defined in the use case of computing power transaction.

  The following logical interfaces for the integration MCN into MSBN architecture:

  - A-NNI-EC(A-NNI-Edge-Computing) between Leaf Router and Aggregation Node is used for the advertisement of the compute-aware routing information.
  - I-NNI-EC(A-NNI-Edge-Computing) is used for the propagation of the compute-aware routing information among the aggregation nodes.
  - E-NNI-EC(E-NNI-Edge-Computing) is used for edge-computing application/service provider handoff.

  The following new reference points are needed for the integration MCN into CloudCO architecture based on non-MEC service functions:

  - Sf-Nf between the NFVI Layer and the Service Functions provides transparent network services to edge-computing service functions.
  - Ve-Vnfm-sf between the Service Functions and the VNFM provides lifecycle management of Service Functions managed by the VNFM.
  - $M_{fc\text{-}sdn\text{-}dc}$-Nf between the CFD function of DC SDN Manager & Controller and VIM is reused to discover the computing capability and the service functions supported by an edge site.

  Additionally, there are some new reference points for the integration MCN into CloudCO architecture based on MEC service functions:

  - Mp1: The Mp1 reference point between the multi-access edge platform and the edge-computing services or functions provides service registration, service discovery, and communication support for services. The Mp1 reference point also provides other functionality such as application availability, session state relocation support procedures, traffic rules and DNS rules activation, access to persistent storage and time of day information, etc. This reference point can be used for consuming and providing service specific functionality.
  - Mp2: The Mp2 reference point between the multi-access edge platform and the data plane of the virtualisation infrastructure is used to instruct the data plane on how to route traffic among applications, networks, services, etc. This reference point is not further specified.
  - Mm3: The Mm3 reference point between the multi-access edge orchestrator and the multi-access edge platform manager is used for the management of the application lifecycle,

application rules and requirements and keeping track of available multi-access edge services.

- Mm6: The Mm6 reference point between the multi-access edge platform manager and the virtualisation infrastructure manager is used to manage virtualised resources e.g., to realize the application lifecycle management.
- Mm9: The Mm9 reference point between the user application lifecycle management proxy and the multi-access edge orchestrator of the multi-access edge system is used to manage multi-access edge applications requested by UE application. This reference point is not further specified.
- Mx2: The Mx2 reference point between the user application lifecycle management proxy and the UE application is used by a UE application to request the multi-access edge system to run an application in the multi-access edge system, or to move an application in or out of the multi-access edge system. This reference point is only accessible within the network. It is only available when supported by the multi-access edge system.

- Edge-computing power abstraction

  Computing power abstraction is the basis of computing power usage. Computing power has been integrated with networks and services and has product attributes in some use cases. Therefore, it is suggested that the edge-computing power abstraction has to be standardized so that the industry promoted by BBF can reach a consensus on edge-computing power transact and guide the development of computing power-related products in the multi-service broadband network.

Based on the gaps and previous sections, it is suggested that the future new technical projects should be considered to include the following works:

- MCN reference architecture and requirements.

  Define the reference architecture for metro compute networking, specify the functional and nodal requirement related to this architecture consistent with TR-384 [2] and TR-178 [4].
- MCN protocols and interfaces

  Identify protocols and interfaces of metro compute networking in order to correlate computing power information of edge sites (e.g., Cloud CO in TR-384) and network topology information, including the general computing interface between a MCN network node and a computing instance, the interface of MCN with Cloud CO, and the interface between Computing Provider and Computing Consumer in the use case of computing power transaction.
- Edge-computing power abstraction

  The abstraction of computing power of edge sites has to be standardized so that it can be understood by MCN for compute scheduling at network level.
- Coordinate with WWC 5G Network and Edge Computing requirements
- Cooperate with other industry and SDOs, particularly ETSI MEC ISG and IETF as needed.

End of Broadband Forum Technical Report TR-466

