ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Report

(09/2023)

TR.cpn-col-sec

Security considerations of collaboration of multiple computing power networks

Technical Report ITU-T TR.cpn-col-sec

Security considerations of collaboration of multiple computing power networks

Summary

This Technical Report analyses concept, business roles, use cases and security risks of collaboration of multiple computing power networks, as well as relevant general security characteristics and requirements, and specifies a security reference framework and capabilities.

Computing power network (CPN) is one type of network that realizes optimized computing resource allocation, networking, computing service dealmaking and provision, by distributing computing, storage, and network resources (Recommendation ITU-T Y.2501). CPN ecosystem is composed of a variety of business players which are distributed in different areas and in different security environments. A CPN usually includes a communication network and a transaction provider and connects computing service consumers, computing service providers and computing resources providers. Multiple CPNs may include multiple communication networks and transaction providers provided by different operators. Therefore, there are many security issues of collaboration of multiple CPNs to be considered, such as that in CPN data transportation planes, in CPN control planes, in CPN transaction planes, in CPN service consumer parts, in CPN service provider parts, and when interacting among them, and so on.

Keywords

Collaboration, computing power network, security.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Technical Report ITU-T TR.cpn-col-sec

Security considerations of collaboration of multiple computing power networks

1 Scope

This Technical Report analyses concept, business roles, use cases and security risks of collaboration of multiple computing power networks, as well as relevant general security characteristics and specifies requirements, reference framework and capabilities.

The scope includes:

– Concept, business roles, use cases of collaboration of multiple computing power networks in aspects of security;

– Analysis of security risks, general security characteristics and requirement of collaboration of multiple computing power networks;

– Specification on a reference security framework of collaboration of multiple computing power networks, and relevant general security capabilities.

2 References

[ITU-T Y.2501] Recommendation ITU-T Y.2501 (2021), *Computing power network – Framework and architecture*.

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.1.2 capability [b-ITU-R M.1224-1]: The ability of an item to meet a service demand of given quantitative characteristics under given internal conditions.

3.1.3 core cloud [b-ITU-T Y.3508]: A cloud computing, that manages resource pools including resources in the edge of the network and enables cloud service.

NOTE – Enabled cloud service on the core cloud is provided by a cloud service provider (CSP).

3.1.4 device [b-ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.5 edge cloud [b-ITU-T Y.3508]: A cloud computing deployed to the edge of the network accessed by cloud service customers (CSCs) with small capacity resources enabling cloud service.

NOTE 1 – Enabled cloud service on the edge cloud is a lightweight cloud service provided by a cloud service provider (CSP) depending on the cloud service category.

NOTE 2 – Lightweight cloud service refers to a portion of cloud service to reconfigure the functionality of cloud service to fit on edge cloud such as the base station and gateway with small capacity resources.

3.1.6 edge computing [b-ITU-T Y.3073]: This refers to a strategy to deploy processing capability at the network edge where end terminals are connected, and to perform the processing of data which is derived from and fed to the end terminals.

3.1.7 Internet of things [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing, and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.8 multi-access edge computing (MEC) [b-ITU-T J.1303]: System that provides an IT service environment and cloud-computing capabilities at the edge of an access network that contains one or more types of access technology and is in close proximity to its users.

3.1.9 thing [b-ITU-T Y.4000]: In the Internet of things, the object of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into the communication networks.

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

AI Artificial Intelligence

CPN Computing Power Network

PII Personally Identifiable Information

5 Conventions

None.

6 Overview of collaboration of multiple computing power networks

6.1 Computing power network defined in [ITU-T Y.2501]

[ITU-T Y.2501] introduced a computer power network (CPN). A definition of CPN as below is derived from [ITU-T Y.2501], for the convenience of discussion in this Technical Report.

The computing power network (CPN): A new type of network that realizes optimized resource allocation, by distributing computing, storage, network, and other resource information of service nodes through a network control plane (such as a centralized controller, distributed routing protocol, etc.).

NOTE – CPN combines network context and user requirements to provide essential support for optimal distribution, association, transaction and scheduling of computing, storage and network resources.

[ITU-T Y.2501] provided a CPN framework (see Figure 6-1). It shows a CPN which includes computing power network consumer (CPN consumer), computing power network provider (CPN provider), computing power network transaction platform (CPN transaction platform), computing power network control plane (CPN control plane), network operator, etc. In addition, it shows an artificial intelligence (AI) empowered platform that enhances the capabilities of the CPN transaction platform.

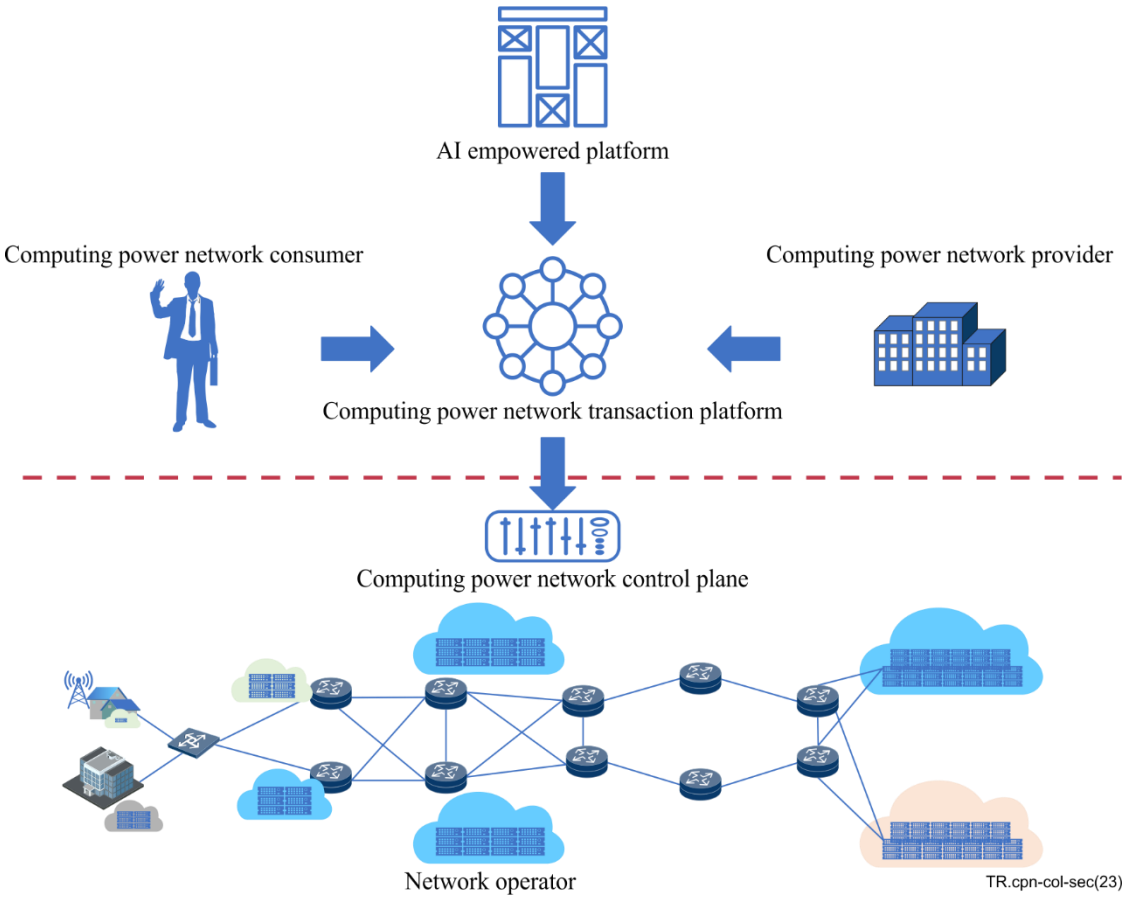


Figure 6-1 – Computing power network framework [ITU-T Y.2501]

Appendix I provides a brief description of business roles and deployment scenarios of computing power networks. The CPN consumer and CPN provider in Figure 6-1 are the same as the CPN service consumer and CPN service provider in Figure II.1 respectively.

Appendix II provides a group of use cases to illustrate the concept and collaboration of single and multiple CPN(s).

In addition, [ITU-T Y.2501] provided a CPN functional architecture (see Figure 6-2). The functionalities of a CPN are distributed in four layers, including the resource layer, control layer, service layer, and orchestration and management layer.

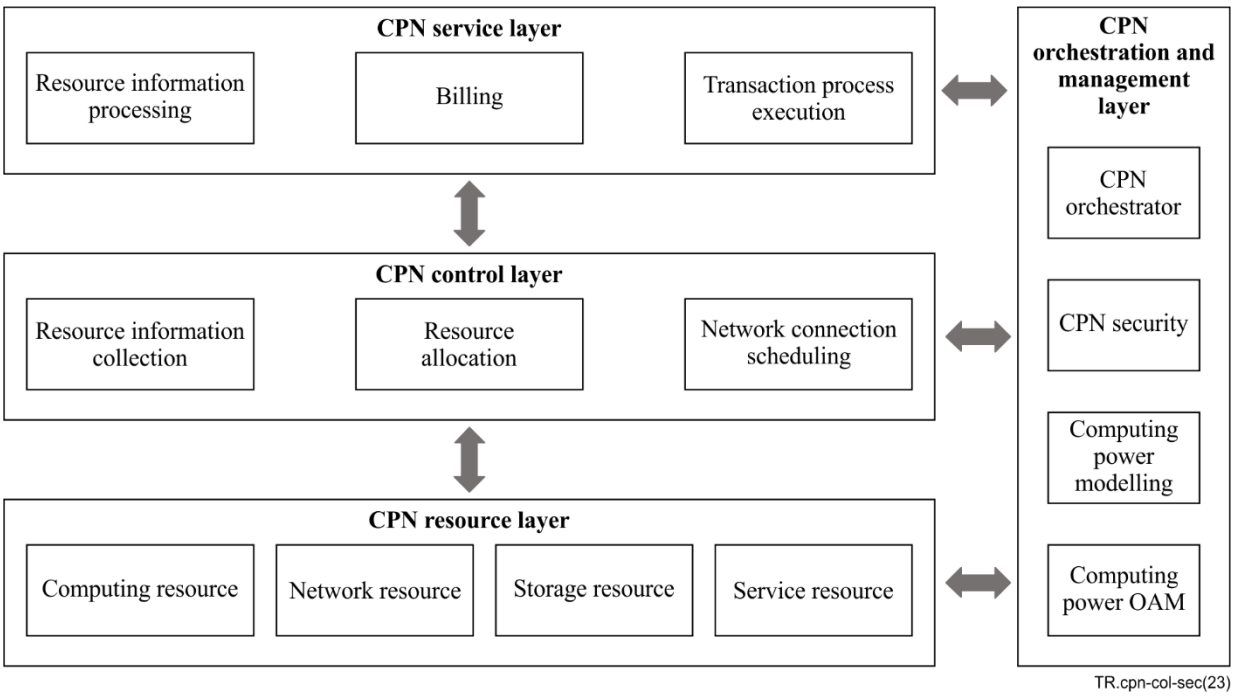


Figure 6-2 – Computing power network functional architecture [ITU-T Y.2501]

According to [ITU-T Y.2501], a CPN has a network control plane (CPN control plane) in the CPN control layer, which realizes optimized resource allocation of the computing, storage, and networking resources in the CPN resource layer. And the CPN control plane provides orchestration and management and security capabilities for data computing, networking and storing.

Traditionally, computing and storage resources usually are in edge clouds and core clouds (partly in ends), and networking resources usually are in network domains (see Figure 6-3). The providers and operators of those resources usually are different.

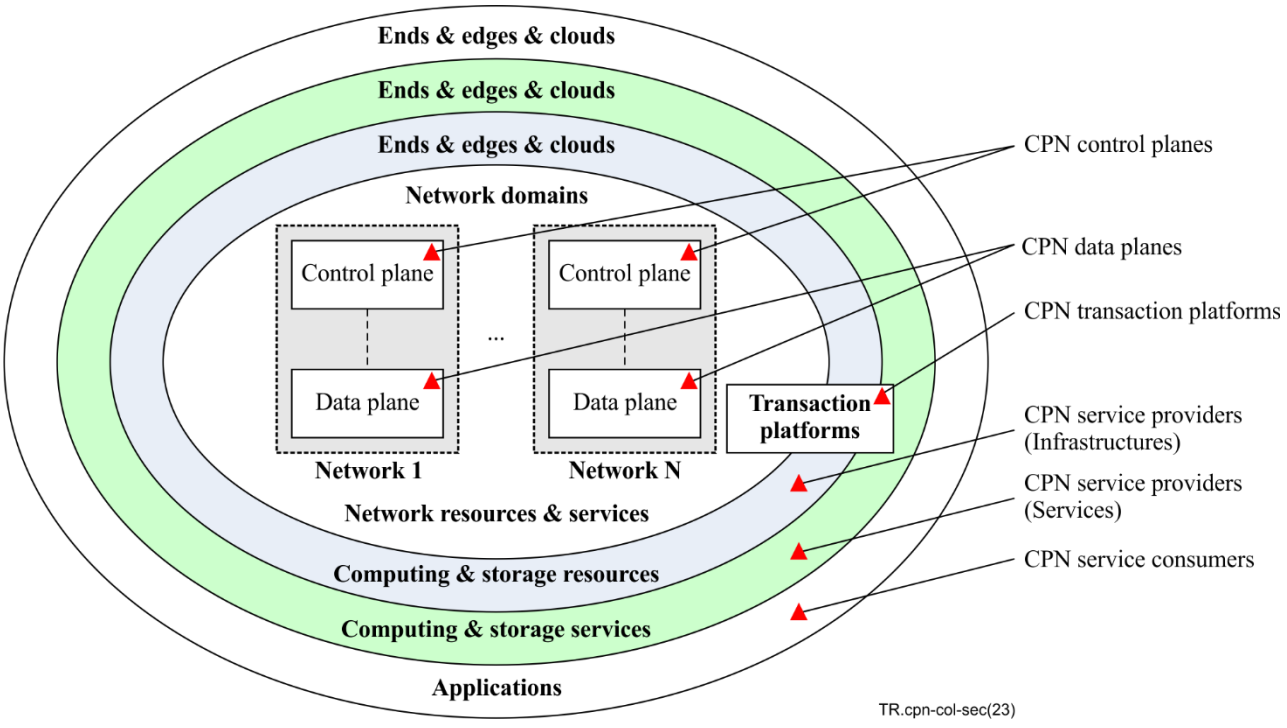


Figure 6-3 – Allocation of resources and services for CPN

NOTE 1 – Without loss of generality to keep the discussion concise and clear in this Technical Report, it uses "cloud" to refer to end and edge cloud, and core cloud if no special statement. Meanwhile, the computing and storage resources and relevant services may be provided in ends, edge clouds and/or core clouds.

NOTE 2 – The computing and storage resources and relevant services for networking services are not analysed in this Technical Report.

The CPN control plane and data plane of a given CPN are in the network domain, therefore, they usually cannot control the computing and storage resources in edge clouds and core clouds directly. The CPN control plane of a given CPN can collaborate with the CPN service providers (infrastructures and services) to exchange information on data computing and storing, and then provides capabilities of optimized networking resource allocation to CPN service consumers and CPN service providers. A CPN transaction platform of a given CPN is across clouds and network domains, which collaborates with the CPN control plane(s) and CPN service providers to provide optimized networking services and optimized resource allocation and services of data computing and storage.

The capabilities of a given CPN may be classified into three categories, according to the undertaking tasks, including computing services, networking services, and collaboration brain:

– Computing services: for data computing and storage, provided by CPN service providers, and performed in clouds.
– Networking services: for data networking, provided by CPN control plane(s) and data planes, and performed in network domains.
– Collaboration brain: for collaboration controlling, provided by CPN control plane(s) and CPN transaction platform(s), and performed across clouds and network domains.

The collaboration brain of a given CPN collects and traces the status of the networking resources and services in the network domain, and exchanges information on storage and computing resources and services in clouds with CPN service providers continuously. And it allocates optimized networking resources and services for data transportation, and coordinates optimized resources and services for data computing and storage, according to the requests and status of CPN service consumers and CPN service providers.

6.2 Multiple computing power networks and related collaboration

A single CPN usually consists of a bearer network (including one CPN control plane and at least one CPN data plane) and a CPN transaction platform and connects and serves multiple CPN service consumers and CPN service providers.

In Figure 6-4, it depicts the collaboration of a single CPN and relevant general reference points (R1 to R8). It may be different for the collaboration and relevant reference points depending on the deployment scenarios of the single CPN.

The collaboration and relevant reference points of a single CPN mainly includes as below:

– R1: Supporting the interaction between the CPN control plane and the CPN transaction platform.
– R2: Supporting the interaction between CPN service consumers and CPN transaction platform.
– R3: Supporting the interaction between CPN service providers and CPN transaction platform.
– R4: Supporting the interaction between the CPN control plane and CPN service consumers, interaction between the CPN control plane and CPN service providers (cloud service providers), and interaction between CPN control plane and CPN service providers (cloud infrastructure providers).
– R5: Supporting interactions between the CPN data plane and CPN service consumers & CPN service providers.

– R6: Supporting the interaction between the CPN control plane and the CPN data plane of the same bearer network.

– R7: Supporting interactions between CPN transaction collaborators in a CPN transaction platform.

– R8: Supporting interactions between cloud service providers in cloud infrastructures.

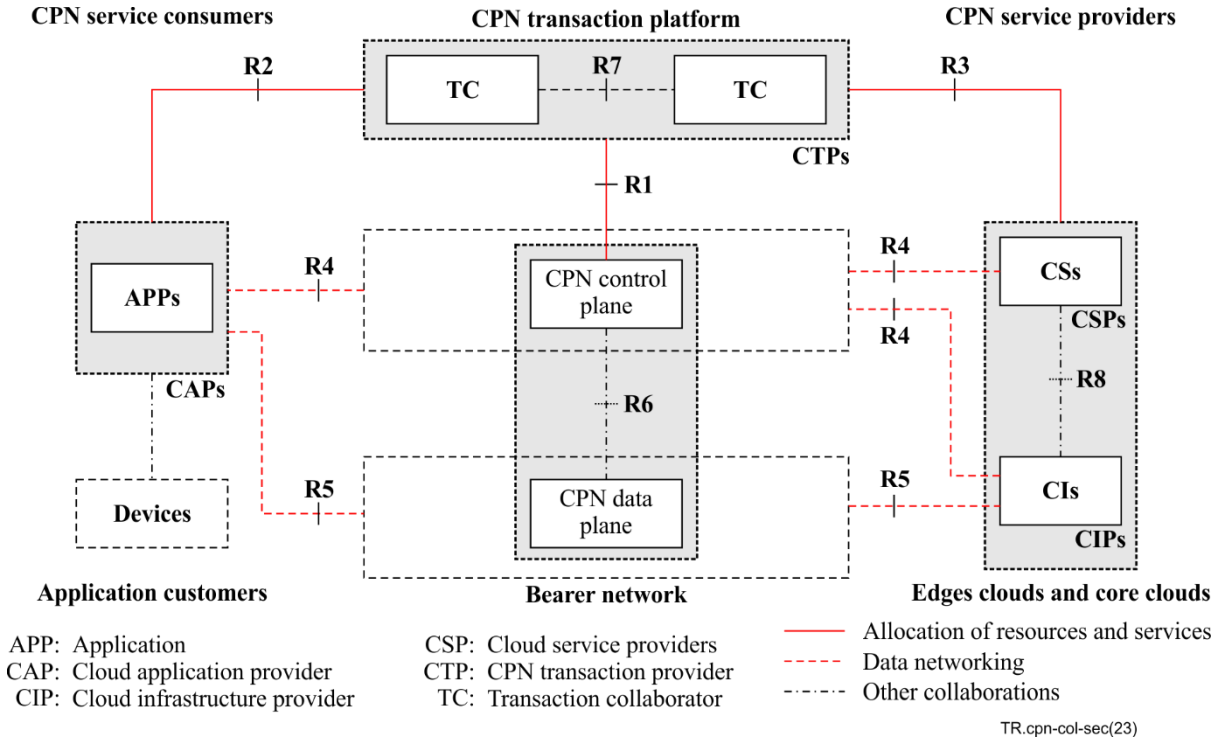


Figure 6-4 – Collaboration of multiple CPNs

Multiple CPNs can collaborate with each other to provide data networking and computing and storage services for CPN service consumers and CPN service providers. In Figure 6-5, it depicts the collaboration of multiple CPNs and relevant general reference points (R1 to R10). It may be different for the collaboration and relevant reference points depending on the deployment scenarios of the multiple CPNs. In addition, Appendix I.2 lists six types of traditional deployment scenarios of multiple CPNs.

The collaboration and relevant reference points of multiple CPNs, besides the R1 to R8 listed in Figure 6-4, includes another two references as below:

– R9: Supporting interaction between multiple CPN control planes of different bearer networks.

– R10: Supporting interaction between multiple CPN data planes of different bearer networks.

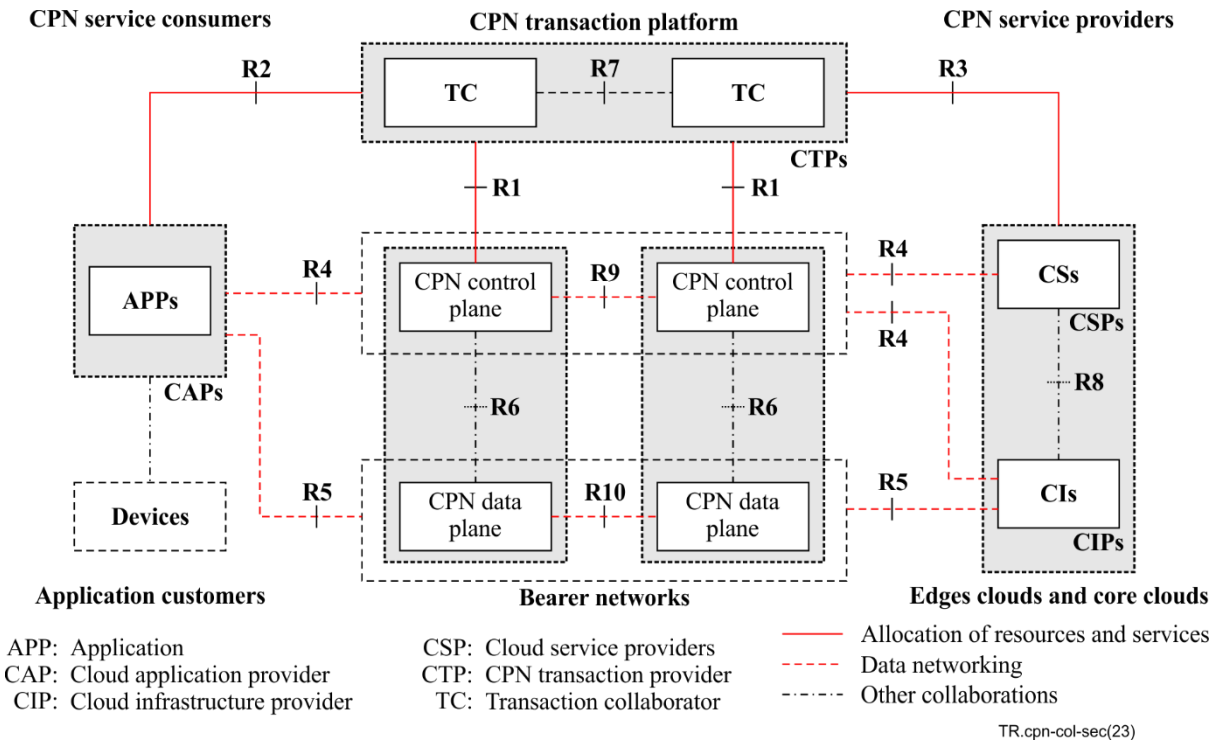


Figure 6-5 – Collaboration of multiple CPNs

NOTE 1 – For the brevity of the description of collaboration between the logical functional entities of multiple CPNs, it only shows two bearer networks and two TCs in Figure 6-5.

NOTE 2 – Reference point R6 is only in the bearer network, and reference point R8 is only in the edge cloud or core cloud, therefore, this Technical Report will not discuss about reference points R6 and R8.

The stakeholders of the collaborations mentioned above belong to multiple operators, and relevant logical functional entities are distributed in different domains and environments, therefore, there exists many security risks to be considered.

7 Security risks of collaboration of multiple computing power networks

7.1 Security risks of collaboration for communication networks

A communication network for CPN usually includes one control plane and one data transportation plane. The control plane of a communication network connects a variety of types of CPN service consumers, CPN service providers and CPN infrastructure providers and is aware of data transportation capabilities of the communication network, and makes optimized allocation of networking resources and services to transmit data for CPN service consumers and CPN service providers. There are many traditional security risks to be considered for communication networks for CPN.

When collaborating with multiple CPNs, the control planes of those communication networks for CPNs interact with each other, and they make deals for cross-network collaboration and data transportation. And those data transportation planes transfer data across the communication networks. It brings new security risks for communication networks for CPNs, such as data security and personally identifiable information (PII) protection when transmitting data cross-networks.

7.2 Security risks of collaboration for transaction platforms

A CPN transaction platform keeps interactions with the CPN service providers to follow their computing capabilities and keeps interactions with communication networks to follow their networking capabilities. It makes deals for CPN service consumers and CPN service providers

according to their requirements and the capabilities of the related computing and networking resources and services. Each of them has some security risks to be considered.

In the case of multiple CPNs, CPN service consumers, CPN service providers and communication networks usually come from different operators and use different technical solutions and in very complex environments, therefore, there are many security risks to be considered for the collaborations for CPN transaction platforms of those multiple CPNs.

7.3 Security risks of collaboration for CPN service consumers

CPN separates CPN service consumers and CPN service providers, CPN service consumers just care about the services they need, and do not care about who and where to provide those services. In this case, data security and PII protection, the trustworthiness of CPN service providers and networking infrastructures should be considered by the CPN service consumers. In case of multiple CPNs, those situations and risks become more prominent.

7.4 Security risks of collaboration for CPN service providers

CPN separates CPN service consumers and CPN service providers, CPN service providers just care about providing the services required and do not care about who and where to request those services. In this case, data security and PII protection, the trustworthiness of CPN service consumers and networking infrastructures should be considered by the CPN service providers. In addition, the CPN service providers share the dynamic information of the capabilities of their services with the CPN control plane(s) and CPN transaction platform. It takes risks of leakage of privacy of their services. In the case of multiple CPNs, those situations and risks become more prominent.

7.5 Security risks of collaboration for CPN infrastructure providers

In a given CPN, CPN infrastructure providers provide underlying infrastructures for network connectivity (to connect to communication networks) and for data computing and storage (to support local computing services). Those underlying infrastructures face traditional security risks for data processing and transportation. In addition, the CPN infrastructure providers share the dynamic information of the capabilities of their underlying infrastructures with the CPN control plane(s) and CPN transaction platform. It takes risks of leakage of privacy of the underlying infrastructures.

7.6 Security risk of collaboration for application consumers

CPN separates CPN service consumers and CPN service providers and makes them unknown to each other. From the perspective of application consumers, they may not know where their data and information are to be transferred and processed. The main risks are related to data security and PII protection. In multiple CPNs, those situations and risks may become more prominent.

8 General security requirements of collaboration of computing power networks

The CPN security module listed in the CPN orchestration and management layer is responsible for applying security related controls to mitigate the security threats in the CPN environments [ITU-T Y.2501]. The CPN security module is considered to provide mechanisms to support trusted transactions, and to ensure the security of applications published by third-parties, and to provide security mechanisms to authorize and authenticate computing power providers [ITU-T Y.2501].

More security requirements are needed for the CPN security module to support the collaboration of multiple CPNs to meet the security risks as listed in clause 7.

8.1 Security requirements for collaboration for CPN control plane

For a given CPN, the security requirements for collaboration for the CPN control plane may include as below:

– It shall provide a security mechanism to protect data security and personally identifiable information (PII) for itself when it allocates networking resources and services for computing service consumption requests from the connected CPN transaction platforms.

– It shall provide a security mechanism to protect data security and PII for the entities (including the connected CPN transaction platforms, the CPN service consumers, and the CPN service providers) when it allocates networking resources and services for computing service consumption requests from the connected CPN transaction platforms.

For given multiple CPNs, besides the related requirements for a single CPN, the security requirement for collaboration for the CPN control planes may include as below:

– It shall provide a security mechanism to protect data security and PII for the entities (including the connected CPN transaction platforms, the CPN service consumers, and the CPN service providers) when they allocate networking resources and services across bearer networks for computing service consumption.

8.2 Security requirements for collaboration for CPN data plane

For a given CPN, the security requirements for collaboration for the CPN data plane may include as below:

– It shall provide a security mechanism to protect data security and PII of the entities (including the CPN service consumers and the CPN service providers) when it performs networking services allocated by the corresponding CPN control plane.

For given multiple CPNs, besides the related requirements for a single CPN, the security requirement for collaboration for the CPN data planes may include as below:

– It shall provide a security mechanism to protect the data security and PII of the entities (including the CPN service consumers and the CPN service providers) when they perform networking services across multiple data planes.

8.3 Security requirements for collaboration for the CPN transaction platform

For a given CPN, the security requirements for collaboration for the CPN transaction platform may include as below:

– It shall provide a security mechanism to protect data security and PII for the CPN service consumers when it makes deals for computing service consumption from the connected CPN service consumers.

– It shall provide a security mechanism to protect data security and PII for the CPN service providers when the CPN service providers update the dynamic information of their computing services.

– It shall provide a security mechanism to protect the service security of the allocated computing services of the connected CPN service providers.

– It shall provide security mechanism to protect data security and PII for the connected CPN control planes when they negotiate networking resources and services for computing service consumption.

For given multiple CPNs, besides the related requirements for a single CPN, the security requirement for collaboration for the CPN transaction platform may include as below:

– It shall provide a security mechanism to protect data security and PII for the entities (including the connected CPN control planes, the CPN service consumers, and the CPN service providers) when they allocate networking resources and services across CPNs for computing service consumption.

8.4 Security requirements for collaboration for CPN service consumer

For any CPN, the security requirement for collaboration for the CPN service consumers may include as below:

– It shall provide a security mechanism to protect data security and PII for the entities (including the connected CPN transaction platforms, the CPN control planes, and the CPN service providers) when it negotiates and consumes computing services.

8.5 Security requirements for collaboration for CPN service provider

For any CPN, the security requirement for collaboration for the CPN service providers may include as below:

– It shall provide a security mechanism to protect data security and PII for the entities (including the connected CPN transaction platforms, the CPN control planes, and the CPN service consumers) when it negotiates and provides computing services.

8.6 Security requirements for collaboration for CPN infrastructure provider

For any CPN, the security requirement for collaboration for the CPN infrastructure providers may include as below:

– It shall provide a security mechanism to protect data security and PII for the entities (including the connected CPN transaction platforms, the CPN control planes, and the CPN service consumers) when it provides support for computing service consumption.

9 Reference security framework and general capabilities of collaboration of computing power networks

Figure 9-1 depicts a reference security framework of the collaboration of CPNs. Without loss of generality, it includes four CPNs provided by different operators, each of which consists of a bearer network (including a CPN control plane and a CPN data plane) and a CPN transaction platform. And they connect multiple CPN service consumers, multiple CPN service providers, and CPN infrastructure providers.

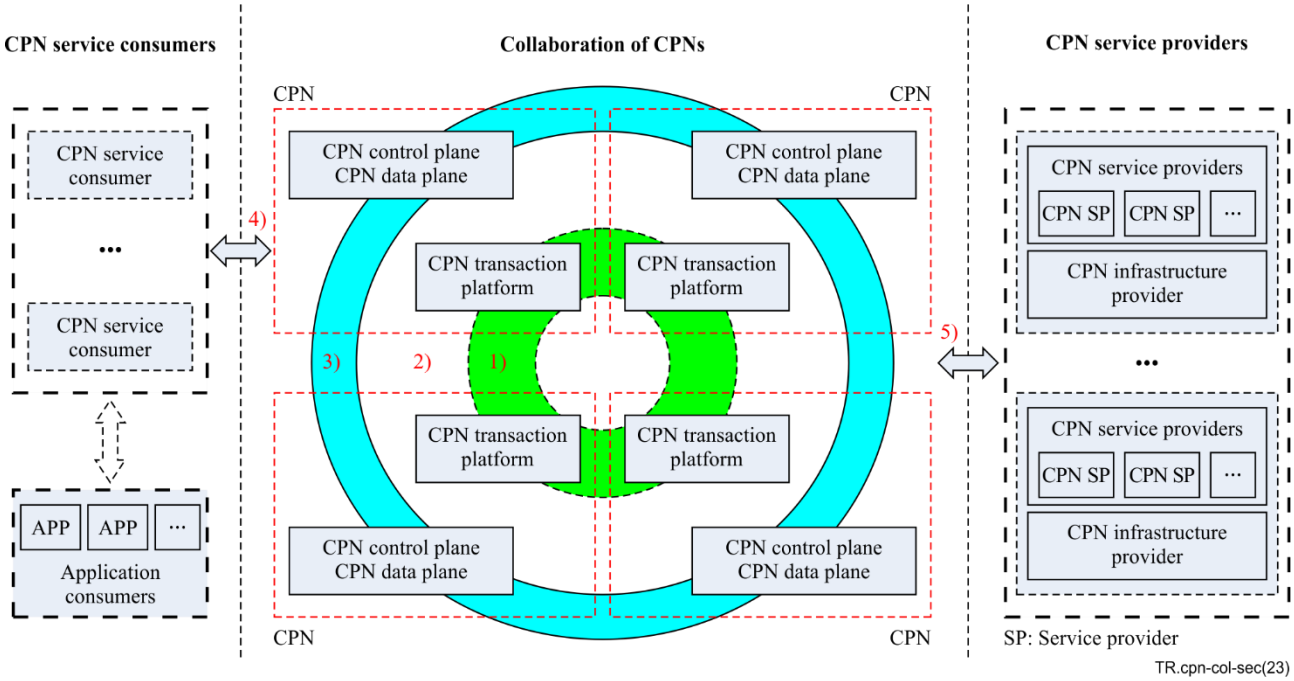


Figure 9-1 – A reference security framework of collaboration of CPNs

In regard to the reference security framework listed above, the collaborations of CPNs mainly include, at least as below:

1) Collaboration among multiple CPN transaction platforms provided by different operators, which interact together and make deals for CPN service consumers and CPN service providers.
2) Collaboration between CPN transaction platforms and CPN control planes, which may be operated by different operators, for negotiating data delivering routes (maybe across bearer networks) for CPN service consumers and CPN service providers.
3) Collaboration among bearer networks for delivering computing services (delivering data for CPN service consumers and CPN service providers); in the cases of multiple CPNs, the data may be transferred across multiple bearer networks. This collaboration usually occurs in bearer networks; therefore, this Technical Report will not address it.
4) Collaboration between CPN service consumers and multiple CPN transaction platforms for dealmaking for consuming computing services, and collaboration between CPN service consumers and multiple bearer networks for interacting with CPN service providers.
5) Collaboration between CPN providers and multiple CPN transaction platforms for dealmaking for providing computing services, and collaboration between CPN providers and multiple bearer networks for interacting with CPN service consumers.

9.1 CPN transaction platform

A CPN transaction platform usually consists of multiple transaction collaborators, which connect to corresponding CPN control planes, CPN service consumers, and CPN service providers.

Each of the transaction collaborators of a given CPN transaction platform exposes reference point R7, (see Figure 6-4) and they utilize reference point R7 to collaborate to make deals for computing service consumption for CPN service consumers and CPN service providers.

For the CPN control plane, the transaction collaborators utilize the reference points (R1, exposed by CPN control planes) to negotiate networking resources to provide optimized networking services to CPN service consumers and CPN service providers for computing service consumption.

For CPN service consumers, the transaction collaborators expose reference points R3, to support CPN service consumers' registration and requests. The transaction collaborators collaborate to identify, authenticate, and authorize the CPN service consumers and relevant requests.

For CPN service providers, the transaction collaborators expose reference points R4, to support CPN service providers' registration and status updates. The transaction collaborators collaborate to identify, authenticate, and authorize the CPN service providers and relevant requests.

9.2 CPN control plane and CPN data plane

A bearer network usually includes one CPN control plane and one or multiple CPN data plane(s). The CPN control plane exposes reference point R6 (see Figure 6-4) and utilizes this reference point to collaborate with the CPN data plane. R6 usually are internal for bearer networks.

The CPN control plane exposes reference point R1 to support interaction with transaction collaborators of the CPN transaction platform to allocate networking resources and services for CPN service consumers and CPN service providers.

The CPN control plane exposes reference point R4 to support CPN service consumers and CPN service providers to request and validate assigned networking resources and services.

The CPN data plane exposes reference point R5 to support CPN service consumers and CPN service providers to use assigned optimized networking resources and services to exchange information.

If having multiple CPN control planes, reference point R9 (see Figure 6-5) is used to interact with each other to allocate networking resources and services across bearer networks.

If having multiple CPN data planes, reference point R10 is used to interact with each other to support CPN service consumers and CPN service providers to exchange information across bearer networks according to assigned networking resources and services.

Appendix I

Business roles and deployment scenarios of computing power networks

I.1 Business roles of multiple computing power networks

A CPN ecosystem is composed of a variety of business players (see Figure I.1), including application consumers (users), cloud application providers, cloud service providers, cloud infrastructure providers, network providers, and CPN transaction providers. Without loss of generality, CPN service consumers include cloud application providers and application customers, and CPN service providers include cloud service providers and cloud infrastructure providers. Each business player plays at least one business role in collaboration with multiple CPNs, but more roles are possible.

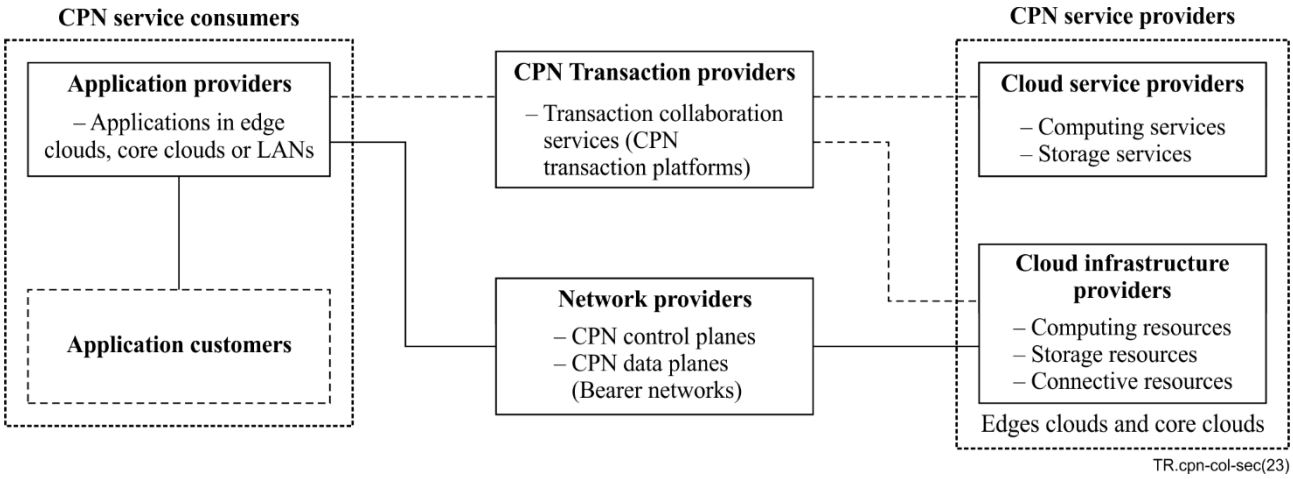


Figure I.1 – Business roles of computing power networks

NOTE – For the brevity of discussion, without loss of generality, this Technical Report only focuses on the collaborations of the entities in the domains of networks, edge clouds and core clouds, not including that in local area networks.

I.1.1 Application consumer

An application consumer is a user who uses applications provided by cloud application providers.

I.1.2 Application provider

A cloud application provider provides cloud applications for its users (application customers). A cloud application can use local and/or remote capabilities for data computing and storage. A cloud application uses remote capabilities of cloud services provided by cloud service providers.

A CPN service consumer is one type of cloud application provider, in edge clouds and/or core clouds, which provides cloud application(s) to application consumer(s).

A CPN service consumer interacts with one or multiple CPN service provider(s) to consume computing and storage services.

I.1.3 Cloud infrastructure provider

A cloud infrastructure provider provides computing, connective, and storage resources to cloud service providers, in edge and/or core clouds.

The cloud infrastructures provide computing, connective and storage resources to cloud services in relevant clouds.

The cloud infrastructure can support connected networks (CPN control planes) and cloud services to be aware of the capabilities of its computing, connective and storage resources, if requested.

NOTE – Herein the connective resource provides capabilities to connect the computing and storage services in edge and/or core clouds, and to communicate with connected outside networks.

I.1.4 Cloud service provider

A cloud service provider provides cloud services (data computing and/or storing) in edge and/or core clouds.

The cloud services use computing, connective and storage resources of one or multiple underlying cloud infrastructures to establish and provide services to CPN service consumers.

The cloud services can make awareness of the capabilities of the underlying cloud infrastructures, and exchange relevant information with connected networks (CPN control planes).

Cloud service providers and cloud infrastructure providers belong to CPN service providers.

I.1.5 Network provider

A network provider provides one or multiple bearer networks to connect clouds (edge clouds and/or core clouds). Bearer networks connecting clouds are usually enhanced by technologies related to IPv6+ and SRv6, etc.

NOTE – A network provider may provide multiple types of communication networks, such as access networks and bearer networks. Herein the network provider points to that providing one or multiple bearer networks.

A bearer network usually includes a control plane and a data plane. The CPN control plane and the CPN data plane usually are the same as the control plane and the data plane of a given bearer network respectively.

The CPN control plane of a bearer network may perceive and/or acquire information from the connected CPN service providers to make awareness of the capabilities of relevant computing, connective and storage resources. Under the awareness, the CPN control plane, collaborating with relevant CPN data planes, can predict and schedule optimized networking routes between the clouds for demanded communications, such as for a dedicated CPN service consumer and a relevant CPN service provider.

A CPN includes at least one network provider and may include multiple network providers that provide multiple communication networks for the given CPN.

I.1.6 CPN transaction provider

A CPN may include a transaction platform that provides transaction collaboration services to make deals for CPN service consumers and CPN service providers to interact with each other for the consumption of computing and storage services.

A CPN may not include any CPN transaction platform.

A CPN transaction platform of a given CPN is provided by a single CPN transaction provider or multiple CPN transaction providers. A CPN transaction provider in a CPN transaction platform is a name transaction collaborator.

I.2 Deployment scenarios of computing power networks

There are various types of collaboration modes according to the deployment scenarios of computing power networks.

Without loss of generality, herein is listed six types of traditional deployment scenarios:

– Single bearer network and no CPN transaction platform (sN-noneTP),

– Multiple bearer networks and no CPN transaction platform (mN-noneTP),

– Single bearer network and single CPN transaction collaborator (sN-sTC),

– Multiple bearer networks and single CPN transaction collaborator (mN-sTC),

– Single bearer network and multiple CPN transaction collaborators (sN-mTC),

– Multiple bearer networks and multiple CPN transaction collaborators (mN-mTC).

In those scenarios, there are multiple CPN service consumers and CPN service providers in edge and/or core clouds. For example, there are multiple cloud application providers (CAP-1 to CAP-N4, N4 is a positive integer) in Figures I.2 to I.7, which provide multiple cloud applications individually as consuming computing and storage services from remote CPN service providers; And the CPN service providers include multiple cloud service providers (CSP-1 to CSP-N3, N3 is a positive integer) and multiple cloud infrastructures (CIP-1 to CIP-N2, N2 is a positive integer). CSPs and CIPs provide cloud services and cloud infrastructures.

I.2.1 Single bearer network and no CPN transaction platform (sN-noneTP)

In this deployment scenario, there is a single bear network, but not any transaction platform.

The applications (CPN service consumers) are coupled with dedicated cloud services (CPN service providers) in edges and/or core clouds (see Figure I.2). The dedicated cloud services for an application usually are pre-set.

The bear network (BN-1) provides data transportation services for the applications and their coupled cloud services.

If the bear network supports customized data transportation technologies (such as IPv6+ and SRv6+), it may support customized data transportation services for the applications and their coupled cloud services. The control plane of the bear network can schedule optimized routes in the bear network for data transportation, according to the connection conditions of the applications and their coupled cloud services, and then the data plane of the bear network can transport data according to the scheduled optimized routes.

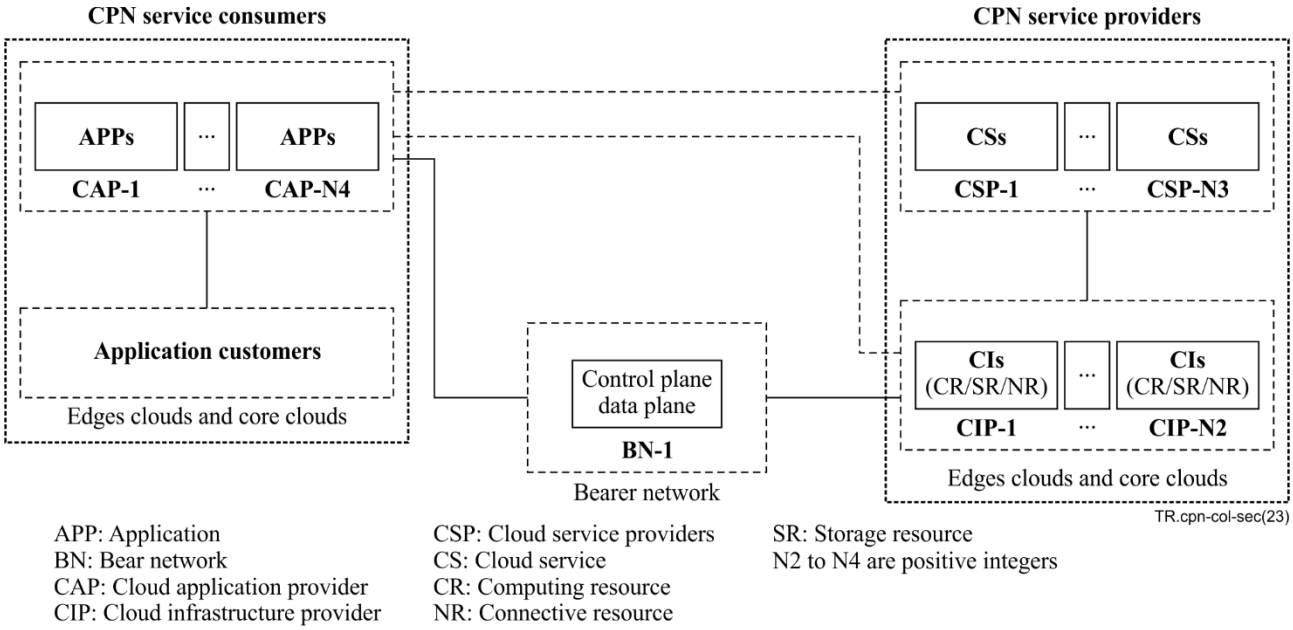


Figure I.2 – Single bearer network and no CPN transaction platform

I.2.2 Multiple bearer networks and no CPN transaction platform (mN-noneTP)

In this deployment scenario, there are multiple bear networks provided by multiple network operators, but not any transaction platform.

In this deployment scenario, the collaborations between CPN service consumers and CPN service providers are similar to that in the deployment scenario of sN-noneTP (see Figure I.3).

The bear networks (BN-1 to BN-N1, N1 is a positive integer) collaborate together to provide data transportation services for the applications and their coupled cloud services.

Similarly, if the bear network supports customized data transportation services, the control planes of the bear networks can schedule optimized routes in the bear networks for data transportation, according to the connection conditions of the applications and their coupled cloud services, and then the data planes of the bear networks can transport data according to the scheduled optimized routes.

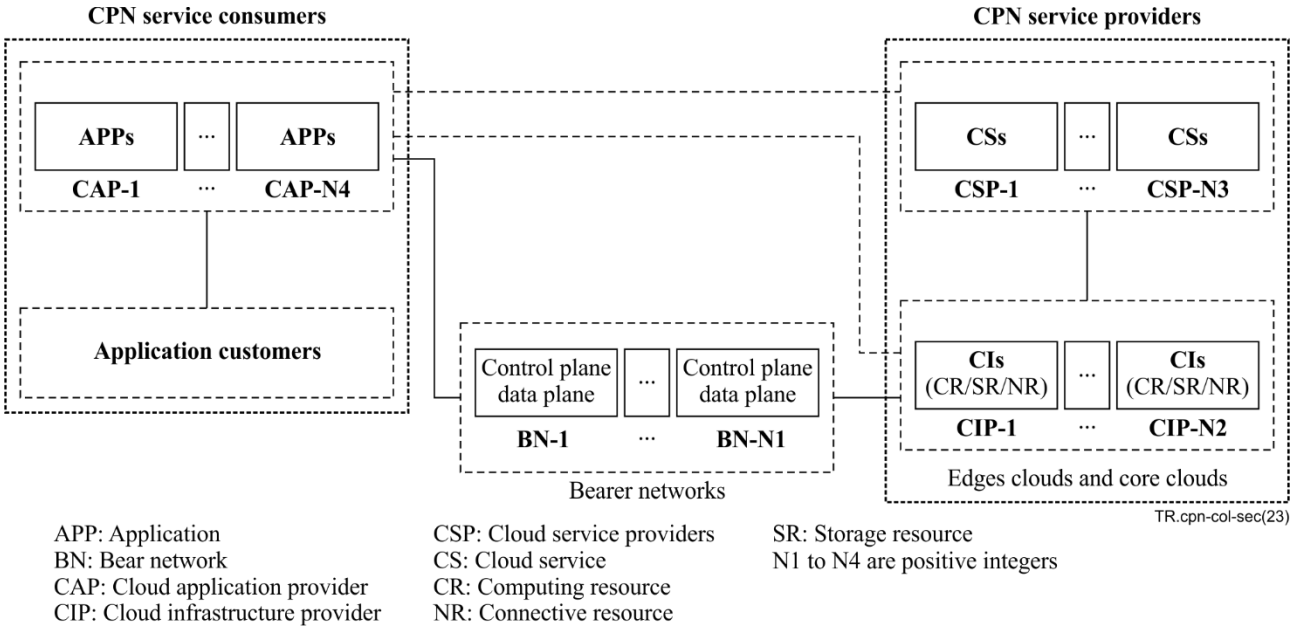


Figure I.3 – Multiple bearer networks and no CPN transaction platform

I.2.3 Single bearer network and single CPN transaction collaborator (sN-sTC)

In this deployment scenario, there is a single bear network and a CPN transaction platform provided by a single transaction collaborator.

The applications (CPN service consumers) are decoupled with remote cloud services (CPN service providers) in edges and/or core clouds (see Figure I.4). The cloud services for an application usually are not pre-set but assigned by the CPN transaction platform.

There is only one transaction collaborator which makes deals individually for the consumption requested by the CPN service consumers.

The bear network (BN-1) provides data transportation services for the applications and their assigned cloud services. The data transportation services are similar to that in the deployment scenario of sN-noneTP (see Figure I.4).

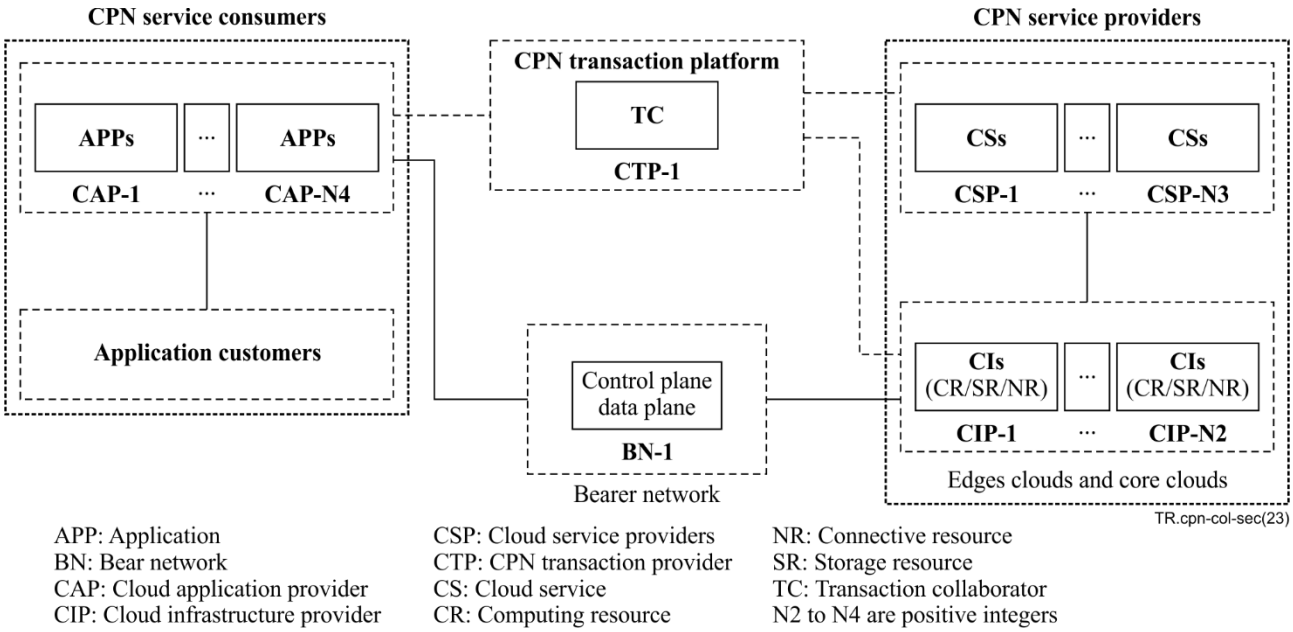


Figure I.4 – Single bearer network and single CPN transaction collaborator

I.2.4 Multiple bearer networks and single CPN transaction collaborator (mN-sTC)

In this deployment scenario, there are multiple bear networks provided by multiple network operators and a CPN transaction platform provided by a single transaction collaborator.

In this deployment scenario, the collaborations between CPN service consumers and CPN service providers are similar to that in the deployment scenario of sN-sTC (see Figure I.5).

There is only one transaction collaborator which makes deals individually for the consumption requested by the CPN service consumers.

The bear networks (BN-1 to BN-N1, N1 is a positive integer) collaborate together to provide data transportation services for the applications and their assigned cloud services. The collaborations of data transportation services among the networks are as that in the deployment scenario of mN-noneTP (see Figure I.5).

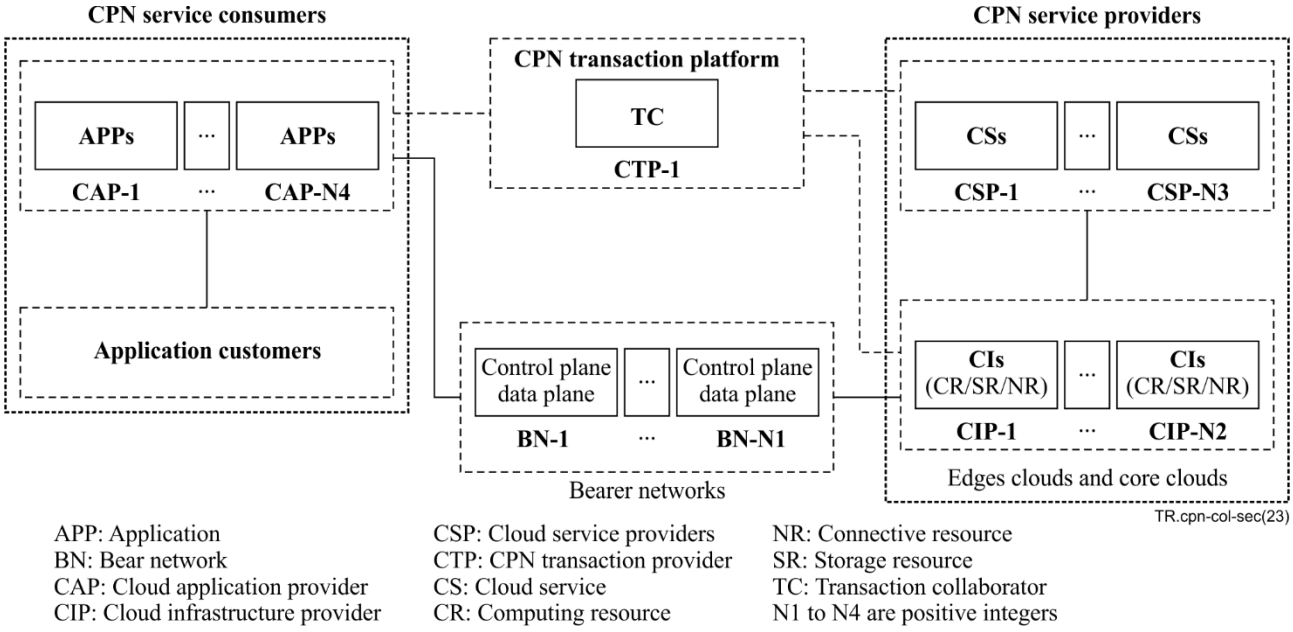


Figure I.5 – Multiple bearer networks and single CPN transaction collaborator

I.2.5 Single bearer network and multiple CPN transaction collaborators (sN-mTC)

In this deployment scenario, there is a single bear network and a CPN transaction platform provided by multiple transaction collaborators.

The applications (CPN service consumers) are decoupled with remote cloud services (CPN service providers) in edges and/or core clouds (see Figure I.6). The cloud services for an application usually are not pre-set but assigned by the CPN transaction platform.

There are multiple transaction collaborators provided by multiple CPN transaction providers (CTP-1 to CTP-N5, N5 is a positive integer) which makes a deal together for the consumption requested by the CPN service consumers.

The bear network (BN-1) provides data transportation services for the applications and their assigned cloud services. The data transportation services are similar to those in the deployment scenario of sN-sTC (see Figure I.6).

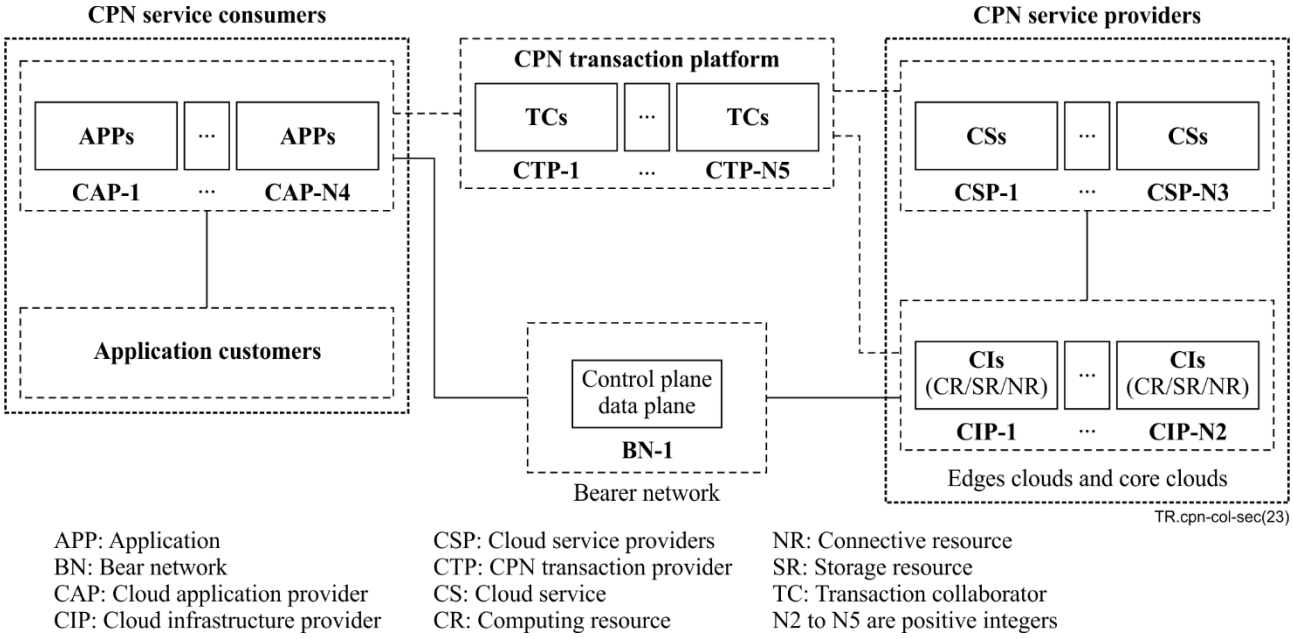


Figure I.6 – Single bearer network and multiple CPN transaction collaborators

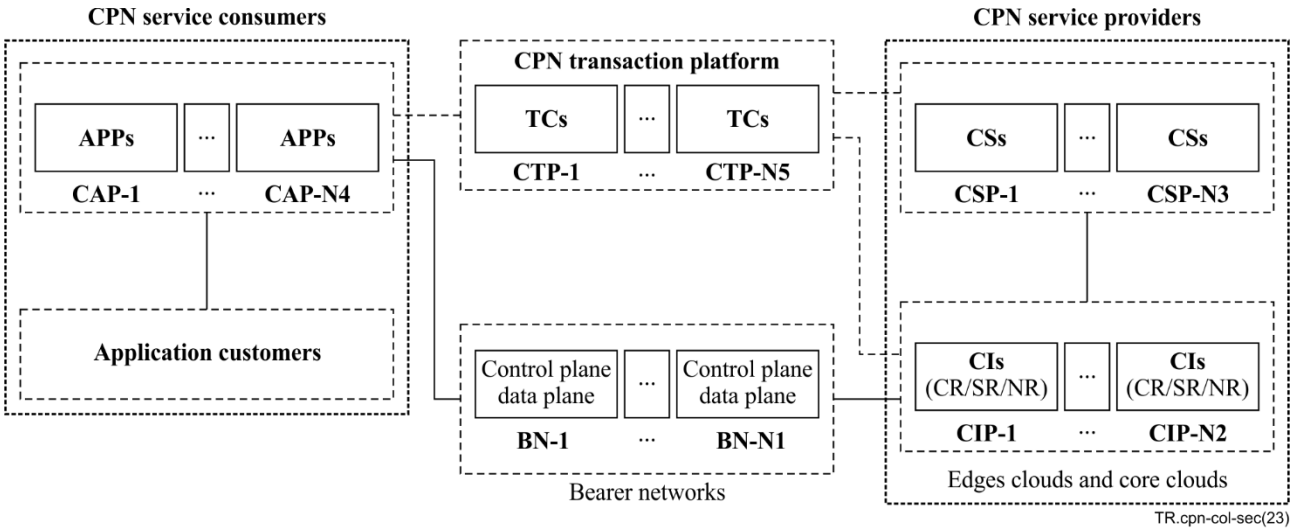
I.2.6 Multiple bearer networks and multiple CPN transaction collaborators (mN-mTC)

In this deployment scenario, there are multiple bear networks provided by multiple network operators and a CPN transaction platform provided by multiple transaction collaborators.

In this deployment scenario, the collaborations between CPN service consumers and CPN service providers are similar to that in the deployment scenario of sN-mTC (see Figure I.7).

There are multiple transaction collaborators provided by multiple CPN transaction providers (CTP-1 to CTP-N5, N5 is a positive integer) which makes a deal together for the consumption requested by the CPN service consumers.

The bear networks (BN-1 to BN-N1, N1 is a positive integer) collaborate together to provide data transportation services for the applications and their assigned cloud services. And the collaborations of data transportation services among the networks are as that in the deployment scenario of mN-sTC (see Figure I.7).



APP: Application
BN: Bear network
CAP: Cloud application provider
CIP: Cloud infrastructure provider
CSP: Cloud service providers
CTP: CPN transaction provider
CS: Cloud service
CR: Computing resource
NR: Connective resource
SR: Storage resource
TC: Transaction collaborator
N1 to N5 are positive integers

Figure I.7 – Multiple bearer networks and multiple CPN transaction collaborators

Appendix II

Use cases of collaboration of multiple computing power networks

This appendix provides a group of use cases to illustrate the concept of collaboration of multiple computing power networks.

II.1 Use case: VR rendering without support of CPN

This use case shows a virtual reality (VR) client in a user device which requests a VR rendering service in the edge cloud to render VR materials, and the VR rendering service interacts with some VR video decoders in remote core clouds to decode videos of the VR materials, without the support of CPN.

In this use case, without loss of generality, there are some business roles (see Appendix I) as below:

– Three groups of VR video decoders in remote core clouds, including VVD1 to VVD9, which provide services to decode VR videos.

  Group G1 includes VR video decoders VVD1, VVD2 and VVD3, etc.

  Group G2 includes VR video decoders VVD4, VVD5 and VVD6, etc.

  Group G3 includes VR video decoders VVD7, VVD8 and VVD9, etc.

– A bearer network, which provides data communication service, and usually consists of two parts, a control plane and a data plane.

  In the data plane of the bearer network, there are some routers, R1 to R7, etc.

– A VR client, in the user device.

– A VR rendering service, in the edge cloud.

Generally, when the VR client requests the VR rendering service to render a VR material remotely (step 1), the VR rendering service may request a pre-defined service provider (such as VVD4) to decode VR videos in the VR material (step 3). Before step 3, the VR rendering service may interact with the control plane of the bearer network to negotiate an optimized route to deliver data with VVD4 (step 2). In this case, there is no CPN to leverage the VR rendering service.

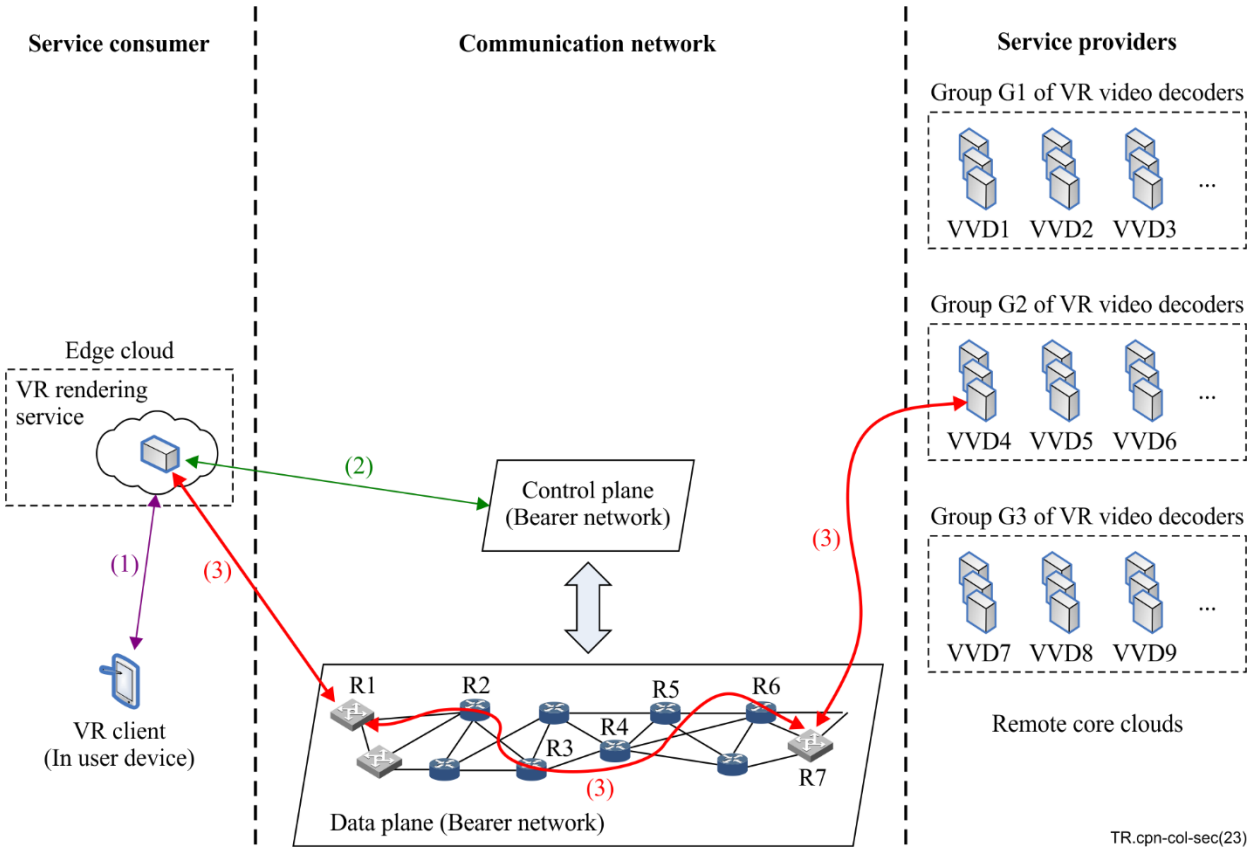


Figure II.1 – VR rendering without support of CPN

II.2 Use case: VR rendering supported by a single CPN

This use case shows a virtual reality (VR) client in a user device which requests a VR rendering service (CPN service consumer) in the edge cloud to render VR materials, and the VR rendering service interacts with some VR video decoders (CPN service providers) in remote core clouds to decode videos of the VR materials, with the support of a single CPN.

In this use case, without loss of generality, there are some business roles (see Appendix I) as below:

– Groups of CPN service providers, including three groups of VR video decoders in remote core clouds, which provide computing services to decode VR videos for CPN service consumers.

  Group G1 includes VR video decoders VVD1, VVD2 and VVD3, etc.

  Group G2 includes VR video decoders VVD4, VVD5 and VVD6, etc.

  Group G3 includes VR video decoders VVD7, VVD8 and VVD9, etc.

– A CPN bearer network, which provides data communication service, and usually consists of two parts, a CPN control plane, and a CPN data plane.

  In the CPN data plane, there are some routers, R1 to R7, etc.

– A CPN transaction platform, acts as a dealmaker for the CPN service consumption.

– A VR client, in the user device.

– A VR rendering service, in the edge cloud, which is a CPN service consumer to request the CPN service providers to decode the VR videos remotely.

This single CPN consists of the above CPN transaction platform, CPN control plane and CPN data plane (Bearer network), and it connects the above VR rendering service and groups of VR video decoders.

Generally, when the VR client requests the VR rendering service to render a VR material remotely (step 1), the VR rendering service negotiates with the CPN transaction platform to get information of the available VR video decoders (such as VVD4) (step 2). Then, the VR rendering service negotiates with the CPN control plane (Bearer network) to get optimized routes (such as from R1 to R7) for interacting with VVD4 (step 3). After that, the VR rendering service interacts with VVD4 through the CPN data plane with the optimized route (step 4).

In this case, the CPN leverages the interaction and communication of the CPN service consumers and the CPN service providers, mainly as below:

– the CPN transaction platform acts as a dealmaker to find available VR video decoders according to the requests of the VR rendering service;

– the CPN control plane (Bearer network) provides an optimized route according to the requested service type and the requests of the VR rendering service and the selected VR video decoder;

– the CPN data plane provides data communication service according to the optimized routes for the VR rendering service and the selected VR video decoder.

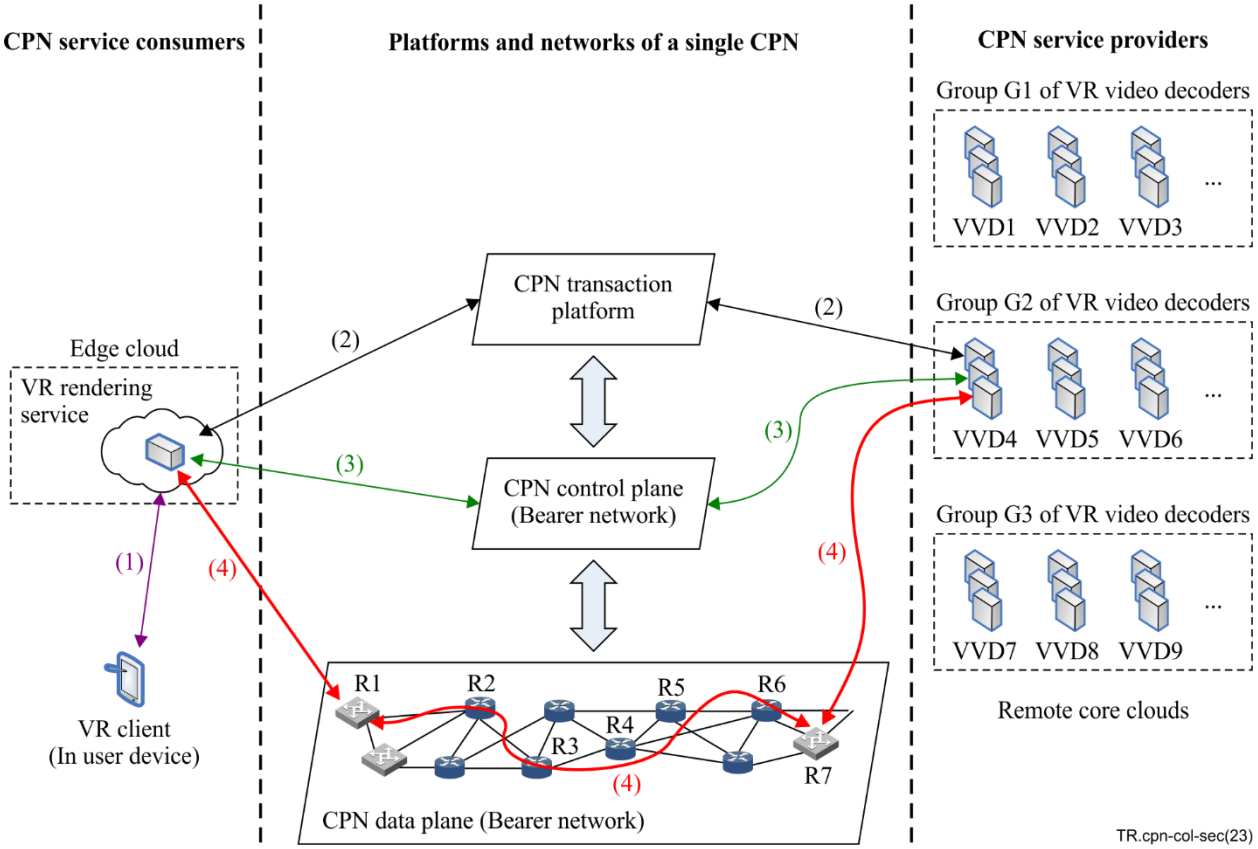


Figure II.2 – VR rendering supported by a single CPN

II.3 Use case: VR rendering supported by a collaboration of multiple CPNs

This use case shows a virtual reality (VR) client in a user device which requests a VR rendering service (CPN service consumer) in the edge cloud to render VR materials, and the VR rendering service interacts with some VR video decoders (CPN service providers) in remote core clouds to decode videos of the VR materials, by the support of multiple CPNs.

In this use case, without loss of generality, there are some business roles (see Appendix I) as below:

– Groups of CPN service providers, including three groups of VR video decoders in remote core clouds, which provide computing services to decode VR videos for CPN service consumers.

  Group G1 includes VR video decoders VVD1, VVD2 and VVD3, etc.

  Group G2 includes VR video decoders VVD4, VVD5 and VVD6, etc.

  Group G3 includes VR video decoders VVD7, VVD8 and VVD9, etc.

  Groups of CPN bearer networks provide data communication service, and usually each of them consists of two parts, a CPN control plane and a CPN data plane.

  Each of the CPN data planes consists of a group of routers, such as:

  • CPN data plane DTP1 managed by CPN control plane CP2 includes routers R1, R2, R3, etc.

  • CPN data plane DTP2 managed by CPN control plane CP3 includes routers R4, R5, etc.

  • CPN data plane DTP3 managed by CPN control plane CP4 includes routers R6, R7, etc.

– Groups of CPN transaction platforms, TP1 to TP6, each of them acts as a dealmaker for CPN service consumption.

  A CPN transaction platform may connect a group of CPN service providers, such as:

  • CPN transaction platform TP1 connecting group G1 of VR video decoders;

  • CPN transaction platform TP2 connecting group G2 of VR video decoders;

  • CPN transaction platform TP3 connecting group G3 of VR video decoders.

  A CPN transaction platform may make deals for CPN service consumers on behalf of the connected CPN service providers.

– A VR client, in the user device.

– A VR rendering service, in the edge cloud, which is a CPN service consumer to request the CPN service providers to decode the VR videos remotely.

Generally, when the VR client (In user device) requests the VR rendering service to render a VR material remotely (step 1), the VR rendering service negotiates with a group of CPN transaction platforms (such as TP1 to TP6) to get information of an available VR video decoder (such as VVD4) (step 2). And then, the VR rendering service negotiates with a group of CPN control planes (such as CP1 to CP5) to get optimized routes (such as from R1 to R7, across bearer networks) for interacting with VVD4 (step 3). After that, the VR rendering service interacts with VVD4 through relevant CPN data planes (such as DTP1 to DTP3) with the optimized routes.

In this case, the multiple CPNs leverage the interaction and communication of the CPN service consumers and the CPN service providers, mainly as below:

– The group of CPN transaction platforms act as dealmakers to find available VR video decoders according to the requests of the VR rendering service;

– The group of CPN control planes provide optimized routes according to the requested service type and the requests of the VR rendering service and the selected VR video decoder, and the route may be across multiple CPN transportation platforms;

– The group of CPN data planes provide data communication service according to the optimized routes for the VR rendering service and the selected VR video decoder.

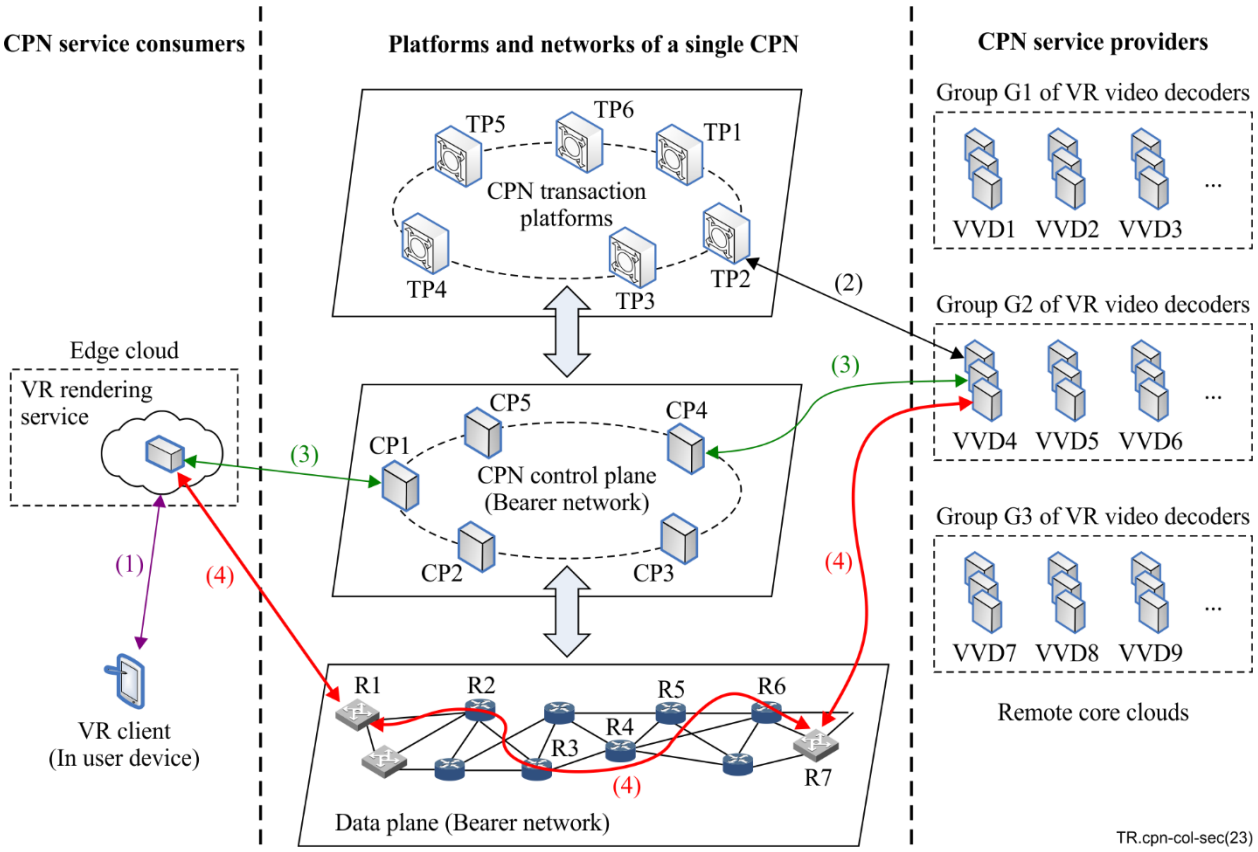


Figure II.3 – VR rendering supported by collaboration of multiple CPNs

Bibliography

[b-ITU-T J.1303] Recommendation ITU-T J.1303 (2022), *Specification of a cloud-based converged media service to support Internet protocol and broadcast cable television – System specification on collaboration between production media cloud and cable service cloud.*

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.

[b-ITU-T Y.3073] Recommendation ITU-T Y.3073 (2019), *Framework for service function chaining in information-centric networking*.

[b-ITU-T Y.3508] Recommendation ITU-T Y.3508 (2019), *Cloud computing – Overview and high-level requirements of distributed cloud*.

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ITU-R M.1224-1] Recommendation ITU-R M.1224-1 (2012), *Vocabulary of terms for International Mobile Telecommunications (IMT)*.