ETSI GR IPE 002 V1.1.1 (2022-04)

IPv6 Enhanced Innovation (IPE);
IPv6 based Data Centers, Network and Cloud Integration

Disclaimer

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

Reference
DGR/IPE-002

Keywords
cloud, data centres, IP, IPv6, SDN

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) IPv6 Enhanced Innovation (IPE).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The opportunity to evolve our network and Cloud infrastructure is now upon us. As enterprises choose the Cloud services to meet their business use cases, the successful integration of IPv6 [i.1] as the network protocol embedded within the Network/Cloud architecture increases the performance and decreases the administrative overhead for all of the services connected and offers much more.

Today, dynamic on-demand interoperability between Cloud instances with an SDN is an achievable low-risk opportunity using IPv6 as the network protocol, employing IPv6 as designed, and not only because of the increased address space. PMTUD [i.2] allows the connected hosts to fragment the packets at each host, significantly reducing the need for another piece of network infrastructure and providing clear views of End to End functionality across Cloud platforms. The present document aims Cloud to demonstrate that IPv6 network protocol is the optimum architecture required for future Network/Cloud convergence. IPv6 is the most promising network protocol prospect to support Data centre's hyper-converged architecture.

Cloud computing is the delivery of computing services - including servers, storage, databases, networking, software, analytics, and intelligence - over the Internet to offer faster innovation, flexible resources, and economies of scale. Cloud services are generally hosted at a remote Data Centre managed by a Cloud Service Provider (CSP). Over the past decade, the provisioning of computing and storage capabilities through Cloud services has been widely accepted by enterprises, more and more enterprise applications evolve from local deployment to Cloud deployment.

The arrival of the Cloud era is also driving the transformation of traditional networks, Cloud service provisioning requires faster, better, and more flexible network connection services, which pose requirement to the network. Cloud and network are breaking through the boundaries and converging with each other, which is generally called network-Cloud convergence or network-Cloud integration.

From operational perspective, network-Cloud convergence refers to comprehensive integration of Cloud computing resources and network facilities, to create an integrated supply, operation, and servicing system by leveraging new CT and IT technologies. Network-Cloud convergence is not only technology change, but business transformation involving organizational structure, production process, management model, and human-resource reconstruction. In combination with other new technologies, e.g. AI, big data, and blockchain, network-Cloud, etc., network-Cloud convergence is shaping the information infrastructure comprehensively.

With the global spread and rapidly increasing adoption of Internet Protocol version six (IPv6), IPv6 become a universal network protocol for the global Internet. In addition, IPv6 also shows enhanced features such as SRv6 [i.4] which allows to determine flexible end-to-end paths by encoding an ordered list of instructions, called "segments", in the form of 128-bits address. The role of IPv6 and its enhanced features in network-Cloud convergence will be discussed in combination with its specific scenarios. Network-Cloud convergence may cover multiple evolving scenarios, clause 5 of present document illustrates several typical use cases of network-Cloud convergence as below:

1) Virtual Private Cloud
2) Enterprise Site to DCs
3) Inter-connection of Clouds
4) Data Centre Network
5) Telecom Cloud Network

For enterprise customers, they need to enhance their competitive advantage with the multi-Cloud deployment, high-performance Cloud-edge collaboration and integrated service provisioning, pose corresponding requirements on the networking side, as in use case 1, 2, 3 and 4. However, the network also poses requirement to the Cloud system itself, as in use case 5. With SDN/NFV as the basic architecture, operators can build a simple, automatic, and intelligent network based on Cloud, so the network can quickly and flexibly adjust resources for service innovation. Telecom Cloud is an extension of traditional network functions, it has higher and more strict requirements than traditional IT systems in terms of real-time, large capacity, and latency.

Clause 6 covers related technologies of network-Cloud convergence, the first one is application-aware IPv6 network (APN) [i.4]. To facilitate service provisioning, perform fine-granularity traffic steering and network resource adjustment, APN uses the programmable space of IPv6 data message Extension Headers, such as Hop-by-Hop Options Header and Segment Routing Header, to carry related application-aware information. The second one is about Hyper-converged Data Centre network, which includes building an IPv6 lossless Data Centre based-on intelligent lossless technologies and improving storage network performance in Data Centres.

Clause 7 discusses Technology advantage of IPv6, network management and Cloud, hyper-converged Data Centre network and conclusions in clause 8.

1 Scope

The present document discusses the following network-Cloud integration use cases which may or will adopt IPv6 as its basic network protocol.

- Virtual private Cloud - Clause 5.1
- Enterprise site to DCs - Clause 5.2
- Inter-connection of Clouds - Clause 5.3
- Data centre network - Clause 5.4
- Telecom Cloud network - Clause 5.5

Each clause provides the description, architecture and requirements, etc.

Every use case is briefly discussed, requiring a working knowledge of IPv6. Clause 6 introduces the related IPv6 technologies which are related to network and Cloud integration. Clause 7 and clause 8 give the benefit analysis of IPv6 for the network-Cloud integration and conclusions of the present document.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

[i.1] IETF RFC 8200: "Internet Protocol, Version 6 (IPv6) Specification".

[i.2] IETF RFC 4821: "Packetization Layer Path MTU Discovery".

[i.3] IETF RFC 8402: "Segment Routing Architecture".

[i.4] IETF draft-li-apn-framework-04: "Application-aware Networking (APN) Framework".

[i.5] NIST SP 800-145: "A NIST definition of Cloud computing".

[i.6] NIST SP 500-292: "Recommendations of the National Institute of Standards and Technology".

[i.7] GAIA-X: "Driver of digital innovation in Europe featuring the next generation of data infrastructure", Federal Ministry for Economic Affairs and Energy (BMWi) May 2020.

[i.8] IDSA, International Data Spaces Association.

NOTE: Available at https://internationaldataspaces.org/.

[i.9] GAIA-X.

NOTE: Available at https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

[i.10] IDSA:"Reference Architecture Model", Version 3.0, Fraunhofer ISST, April 2019.

[i.11] DIN SPEC 27070: "Reference architecture of a security gateway for the exchange of industry data and services", IDSA, February 2020.

[i.12] GAIA-X: "Technical architecture", Federal Ministry for Economic Affairs and Energy (BMWi), Release, June 2020.

[i.13] IETF RFC 6071: "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap".

[i.14] IETF RFC 4193: "Unique Local IPv6 Unicast Addresses".

[i.15] Recommendation ITU-T Y.3322: "The functional architecture and implementations of S-NICE (Software defined Network Intelligence Capability Enhancement)".

[i.16] IETF RFC 4443: "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version6 (IPv6) Specification".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

internet: collection of networks which attach to a variety of computing and communications devices

Internet: worldwide collection of networks on which the World Wide Web is based

GAIA-X: federated and secure data infrastructure establishing an ecosystem in which data is made available, collated, and shared in a trustworthy environment

Orchestration: method of automating individual equipment configurations as well as large numbers of network equipment configurations in real time

Point of Presence (PoP): physical location reserved for different carrier's circuit interconnect and termination equipment for rapid interconnection of fibre services between the different vendors

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

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

Segment Routing (SR): source-based routing technique that simplifies traffic engineering and management across network domains by steering packets through an ordered list of instructions to realize end-to-end policy without creating any per-flow state in the network

Virtual Private Cloud (VPC): a logical isolated area composed Cloud of the Cloud's computation, storage and network with the associated routing and security rules

3.2 Symbols

Void.

3.3 Abbreviations

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

AI	Artificial Intelligence
APN	Application-aware Networking
BRAS	Broadband Remote Access Server
CE	Customer Edge

CPE	Customer Premise Equipment
CSP	Cloud Service Provider
CT	Communication Technology
DC	Data Centre
DCI	Data Centre Interconnect
DNS	Domain Name System
ECMP	Equal Cost Multi-Path
ECN	Explicit Congestion Notification
FC	Fibre Channel
FTP	File Transfer Protocol
GW	Gateway
HPC	High-Performance Computing
HTTP	Hyper Text Transfer Protocol
IaaS	Infrastructure as a Service
IB	InfiniBand
ICMP	Internet Control Message Protocol
IDSA	International Data Spaces Association
IETF	Internet Engineering Task Force
IFIT	In-situ Flow Information Telemetry
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
IT	Information Technology
MAN	Metropolitan Area Network
MPLS	Multi-Protocol Label Switching
MSP	Managed Service Provider
NAT	Network Address Translation
NE	Network Element
NFV	Network Functions Virtualization
NIC	Network Interface Card
NVMe	Non-Volatile Memory express™
NVMe-oF	NVMe over Fabric
O&M	Operations and Management
OS	Operating System
PaaS	Platform as a Service
PE	Provider Edge
PMTU	Path Maximum Transmission Unit
PMTUD	PMTU Discovery
PoP	Point of Presence
QoE	Quality of Experience
QoS	Quality of Service
RDMA	Remote Direct Memory Access
RoCE	RDMA over Converged Ethernet
SaaS	Software as a Service
SATA	Serial Advanced Technology Attachment
SDN	Software Defined Network
SD-WAN	Software Defined Wide Area Network
SFC	Service Function Chain
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SR	Segment Routing
SRv6	Segment Routing for IPv6
SSD	Solid State Disk
TCP	Transmission Control Protocol
ToR	Top of Rack
UDP	User Datagram Protocol
ULA	Unique Local Address
V2X	Vehicle to Everything
VIP	Very Important Person
VPC	Virtual Private Cloud

VPLS	Virtual Private LAN Services
VPN	Virtual Private Network
VXLAN	Virtual eXtensible Local Area Network
WAN	Wide Area Network

4 New trends of information infrastructure

4.1 Overview of Cloud and network convergence

With the rapid growth of the digital economy enabled by the Internet, enterprises do not have sufficient internal computing resources and infrastructure to support their own growth. Traditional acquisition, installation and commissioning of on-premise Information Technology can take months with impacts on projects and potential customers.

Data Centres were initially developed to house large mainframe computers used mainly to run batch workloads and upgraded in second time adding interactive capabilities. Modems were added to these systems to allow remote management and maintenance, performed by a centralized IT group. As the size and cost of IT systems decreased and the processing power grew exponentially, the need for large Data Centres reduced. The new 32-bit and 64-bit based computer systems using Virtual Machines allowed multiple customers workloads to be run on a common cluster of servers. Since the management of IT resources is not the core business of the enterprise using them, the management could be outsourced to MSPs allowing the company to concentrate on their products and services.

Managed Service Providers developed IT services that could be sold to companies reducing their infrastructure investments by paying a monthly fee to get the infrastructure as a service from the MSP.

In the late nineties, a large retail e-commerce site, decided that what they had developed for themselves could be sold to the marketplace so they could get a return on their web-based IT investments. That contributed significatively to jump start the Cloud Provider industry.

Cloud computing is a model enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [i.5]. This Cloud model has five basic characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Cloud computing provides three kinds of service modes including SaaS, PaaS, and IaaS. Cloud Provider acquires and manages the computing infrastructure required for providing the services, runs the Cloud software that provides the services, and makes arrangement to deliver the Cloud services to the Cloud Consumers through network access [i.6].

In traditional networks, network-Cloud integration is only implemented at the commercial level. Cloud and network are independent with each other in planning, construction and operation products. The carrier network is not business-oriented, but just connected. The value lies in connecting the Cloud and cannot provide one-stop services of the Cloud network. Driven by the boom of Cloud computing, the network needs to be built around the Cloud and the network architecture is optimized with the concept of Cloud computing. Network resources can be dynamically and flexibly scheduled and allocated according to service needs and granting proper quality of experience to the user of the service. This new change is called the network-Cloud convergence.

Since the beginning, network-Cloud convergence revolves around the basic resource layer of Cloud network and constantly advances and deepens from intra-Cloud, inter-Cloud and Cloud access to multi-Cloud collaboration and network-Cloud-edge-terminal collaboration.

In the first implementations, network-Cloud convergence occurred in the intra-Cloud network (in DC). To meet the demand for high-frequency and fast transmission of massive data brought by Cloud services, Leaf-Spine/Clos architecture and large layer-2 network technology were introduced to integrate the capability of network in DC and Cloud seamlessly.

Along with the dramatic increase of inter-DC traffic, the focus of network-Cloud convergence shifts to inter-Cloud networks, i.e. Data Centre Interconnection. The efficient transport and fast forwarding of east-west traffic between Data Centres is implemented by deploying large-capacity, non-blocking and low-latency DCI networks.

While more and more applications of enterprise shifting to the Cloud, Cloud access set new requirements becoming a fundamental part of the whole service. Some new type of networking technology, with SD-WAN as the representative, through a software-defined way, enables simple, flexible and low-cost Cloud access.

With the improvement of real-time and interactive demands of services, it is hard for the traditional centralized Cloud deployment to meet the high-performance requirements of services like V2X and industrial Internet, the performance and service availability needs to be improved using multi-Cloud collaboration, Cloud-edge collaboration, and even Cloud-network-edge collaboration.

4.2 General requirements to network-Cloud convergence

Network-Cloud convergence is not only driven by technological advancement, but the changing requirements of customers. Enterprise customers need to enhance their competitive advantage with the multi-Cloud deployment, high-performance Cloud-edge collaboration, integrated service provisioning. Although network and Cloud begin to converge, their role in this process are quite different, the Cloud will gradually become the centre of infrastructure and the network will be the foundation. Accordingly, the planning of the network of operators will follow the requirements of the Cloud, which can be illustrated in the following dimensions:

1) Network performance: Refers to the network coverage, network bandwidth and other parameters, which are influenced by the following factors:

   - Network coverage: Wired/wireless network coverage, which meets the expansion and range of the Cloud to the edge, ensuring "where there is Cloud, there is a network".

   - Network bandwidth: Sufficient network bandwidth assurance and flexible bandwidth adjustment capability, which may be invoked by Cloud application instance at any time.

2) Network availability: Refers to the ability of the network to provide reliable and stable connection to the Cloud application, with SLA assurance and differentiation assurance:

   - SLA assurance: Quality of definiteness provided that matches the service, especially providing high-quality assurance for high-level services to meet customer’s specific requirements for network quality.

   - Differentiation assurance: The quality of network provides differentiated connection service for the Cloud applications and realizes multiple levels of service through technologies such as multi-layer redundancy and backup, multiple routing, QoS mechanism and dynamic resource scheduling.

3) Network intelligence: Refers to the capabilities that can autonomously decide and take action to meet the flexible and changing demands of the Cloud:

   - Elastic scalability: The network coverage, bandwidth and other performance may be adjusted and scaled up/down as needed to meet the customer and service requirements.

   - Rapid fault discovery and automatic traffic switching: The fault may be quickly located. The loads may be switched automatically to ensure stable network performance and avoid the degradation of customer experience.

   - Dynamic optimisation of E2E network resources: Network resources may be dynamically optimized in real time according to the Cloud service demands, user access and other factors.

4) Flexible adaptability: The network capability services can be configured and terminated in a one-stop manner, with the type, function and performance of the services capable of being easily modified and changed:

   - Rapid provision: Starting from the demand of Cloud, automate the deployment and opening of network resources, and realize the integrated provision of Cloud network resources, saving the service provision time to the greatest extent.

Network-Cloud convergence may cover multiple evolving scenarios, e.g. virtual private Cloud, enterprise to DC, inter-connection of Clouds and data-centre networks. In addition, the operators' network is being virtualized gradually to guarantee service agility, instantly scale capacity and performance to demand. The description of network-convergence use cases is mainly done in clause 5.

Clause 5.1 describes the virtual private Cloud, including its definition, architecture and benefit of IPv6 as a new network technology. Clause 5.2 analyses enterprise site to DC connectivity, which requires operators to quickly and agilely connect from the enterprise site to DC. For achieving e2e QoS in a hybrid-Cloud environment, the connectivity has to be able to select the path matching the target SLA and having the ability to scale according to service-based criteria. Since enterprise may place their data in multiple Cloud pools, operators need to provide inter-Cloud connections between Cloud pools operated by the same Cloud provider or different Cloud providers. Clause 5.3 illustrates the architecture and general requirements of the inter-connection of Clouds. Clause 5.4 illustrates data-centre networks, in particular its components, including intra-DC and inter-DC network, are discussed. Clause 5.5 examines the telecom-Cloud network with the intends to build new networks that can quickly and flexibly adjust resources for service innovation. The clause introduces the network element virtualization, network architecture change and the new-generation O&M system to optimize service and business processes.

4.3 European digital sovereignty with GAIA-X and IDSA

In 2019 the European Union launched GAIA-X whose origin stems from the German Federal Government to create the next generation of data infrastructure for Europe, its companies and its citizens. This infrastructure needs to meet the highest standards in terms of digital sovereignty and aims to foster innovation. The targeted infrastructure is regarded as the cradle of an ecosystem, where data and services can be made available, collated and shared in a trusted environment. The goal was to establish a more robust framework in 2020 and to launch the very first use cases by 2021 [i.7].

The International Data Spaces Association (IDSA) [i.8] had earlier in 2019 defined a reference architecture and a global standard for creating and operating virtual data spaces. The International Data Spaces Architecture is based on commonly recognized data governance models facilitating secure exchange and easy linkage of data within business ecosystems. This architecture and components correspond to the requirements of GAIA-X.

Field Code Changed

Europe's plan for digital sovereignty uses two main axes. The first one is Cloud sovereignty, in order to have Cloud services that comply with European regulation. The solution for this sovereign Cloud infrastructure hinges on the federation of European Cloud services along the GAIA-X Association [i.9]. The second one is data sovereignty with the goal of being able to safely share data among participants in a consortium, the foundation of which will be the IDSA's reference architecture model [i.10].

Field Code Changed

IDSA is an initiative driven by the German Industry 4.0 companies and firmly backed by the German Federal Government. Against the idea that competition diminishes trust and damages relationships, normally trust and competition go hand in hand [i.11].

IDSA's Reference Architecture provides an abstract "business view" description of the roles a participant can play in the Data Spaces [i.10]. "Core Participant" roles are roles assumed by organizations that own, provide and/or consume or use data in the data space. These roles include Data Owner, Data Provider, Data Consumer and Data Application Provider.

Field Code Changed

They also issue certificates to core software components (e.g. Connectors) that are to be deployed in the data space. To securely exchange and share data in an IDSA-compliant data space, any participant deploys a technical component called the Industrial Data Space Connector. A Connector can be an Internal Connector that runs within a participating organization or an External Connector that executes data exchange between participating organizations. The requirements to be met by a Connector for cross-company exchange of industrial manufacturing data are specified in [i.11].

GAIA-X focuses on providing a trusted infrastructure to allow secure and sovereign data exchanges by certifying its nodes and actors and by relying on verifiable claims done by nodes. A high-level overview of the GAIA-X Architecture [i.12] with its major elements and functions is provided in figure 1.

The GAIA-X ecosystem as a whole is structured into:

- The Infrastructure Ecosystem in which activity is focused on providing or consuming infrastructure services that are primarily represented by the Asset called Node in GAIA-X. It includes infrastructure components to store, transfer and process data. Stakeholders involved in this ecosystem include Cloud service providers, network providers, and (edge) Cloud providers.
- The Data Ecosystem that supports Data Spaces and the building of smart services in industry verticals. The main Asset is Data.

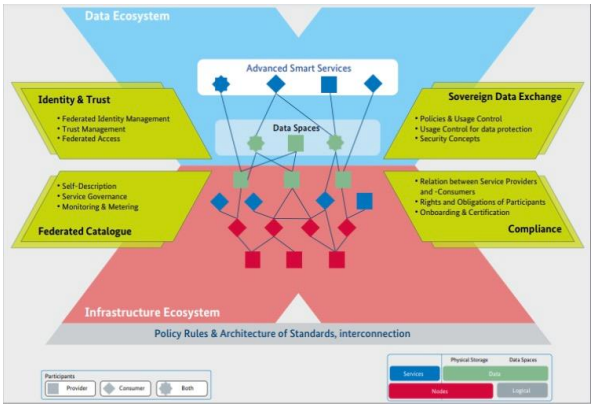

Figure 1: High-level view of the GAIA-X architecture

In short, IDSA defines a federated technical architecture that aims to guarantee data security and protection for all involved participants. It establishes mutual trust among them and ensures data sovereignty for all data providers. Therefore, the data space concepts and components proposed by IDSA are used to support the federated and interoperable infrastructure that the European project GAIA-X aims to address [i.13].

In Europe the data regulation is set in the Data Governance Act and Data Act. GAIA-X is at the heart of the coordination: to provide use cases and technical architectures for European common dataspace for the data stream; to supply federation and interoperability for the European alliance for industrial data, Edge and Cloud for the Cloud stream. Whether it is GAIA-X or IDSA, both approaches rely on a federation approach.

5 Usage scenarios description

5.1 Virtual private Cloud

A virtual private Cloud is a Cloud service that enables enterprises to build their own private Cloud computing environment based on the shared public Cloud infrastructure. A virtual private Cloud creates an isolated, user-independently configured and managed Virtual network environment for Cloud servers, Cloud containers, Cloud databases and other resources, so as to improve the security of resources on the Cloud and simplify users' network deployment.

VPC logical isolation is achieved using virtual network capabilities and security features that give enterprise customers fine-grained control over which IP addresses or applications can access to specific resources. Users can define security group, VPN, IP address segment, bandwidth and other network features in VPC, and easily manage and configure the internal network through VPC to achieve safe and fast network changes. At the same time, users can customize the access rules of elastic Cloud servers within and between security groups to strengthen the security protection of elastic Cloud servers.

There are two application scenarios as follows:

- Dedicated Cloud Network
  Users can define the network and create subnets that manage the elastic compute services network planes. Subnets support IP address management and the DNS service. VPCs are completely isolated, while users can configure access rules to enable communication between subnets. In addition, VPC provides advanced security features, such as security groups and network access lists, in order to help control access to resources in their VPCs.

- Internet Access
  When the resources deployed on the VPC need to access the Internet or provide external services, the elastic compute services need to be configured with public network IP addresses to achieve Internet connection.

The most obvious change that IPv6 brings to Cloud computing is its huge pool of addresses which not only solves the serious problem of running out of addresses and brings advantages such as NAT avoidance for virtual hosts that need communications with the public Internet. The ubiquity of IPv4 and the exhaustion of addresses lead to the wide use of network translator in Cloud computing. Virtual machine instances are not configured with unique, routable IP addresses, but rather use NAT mechanism to map routable IP addresses to virtual private Cloud. Therefore, the failure to establish proper end-to-end connections with Cloud services or virtual severs rented in the Cloud may affect the security, confidentiality, and integrity of data stored in the Cloud, as well as the functions of IPSec [i.14]. Proper protection of virtual private Cloud can be offered through IPv6 deployment in which support for IPSec is mandatory and can function at its fullest. For the scenario of VPC, some virtual host may not adopt global unicast IPv6 addresses since they only need to communicate within the VPC and do not have the need to communicate with the public Internet. In this case, another kind of IPv6 address, the ULA [i.15] can be used to identify each host within VPC. ULA is a unicast address type and is limited to the fc00::/7 prefix, its purpose in IPv6 is analogous to IPv4 private network addressing.

Besides, IPv6 provides multiple addresses for each interface, link-local, global-unicast and ULA, which is different from the "each interface address" addressing scheme in IPv4. It offers various ways of host and network management methods and streamlines address management.

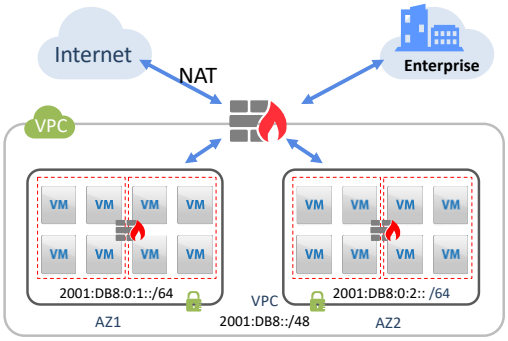

Figure 2: Virtual private Cloud

5.2 Enterprise site to DCs

With the rapid development of the Cloud industry, small and medium-sized enterprises, e.g. those with less than 1 000 employees, seldom have self-built DCs. They tend to deploy their services on a public Cloud or edge Cloud and are most likely to continue using this in the future as their main service mode. To meet the requirements of these enterprises, operators need to provide connections from the enterprise site to DC quickly and agilely. When these connections are available, each application can optimize its workload placement and leverage resources on-premises, in the edge Cloud of the ISP or in public Clouds. In addition, the Cloud application are configured with rules allowing them to scale in order to address the service workload variation overtime.

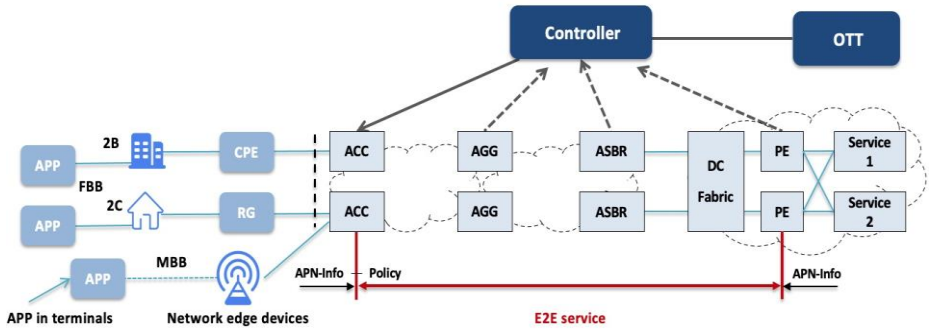

Figure 3: Connections of Enterprise Site to DCs

Achieving e2e QoS requires more favourable solutions to create new connections with granted SLA and high reliability. Enterprise services having applications on-premises and in public Cloud currently have two main connectivity options:

- Internet connectivity: Low cost connectivity with an overlay connectivity is setup from the customer premises to the public Cloud. In general, this connectivity does not offer any granted SLA.
- Dedicated connectivity: Operator makes available a dedicated connectivity between the Cloud provider and the customer premises. The Cloud provider creates a dedicated virtual private connection to the ISP boundary. Currently the connectivity is costly and inflexible to service change.

Other factors need to be considered for service e2e QoE (Quality of Experience) to be guaranteed, for example:

- Congestion in the ISP network
- Congestion in Internet Exchange for peering connection and towards the internet
- Congestion in Public Cloud provider internet access

Those limitations could have negative impacts on the connections from the enterprise site to the Cloud. Public Cloud system, enterprise and ISP need to coordinate a proper interconnection to synchronize the service handling in terms of e2e guaranteed SLA and fault resiliency. Application workload placement and relative application scaling have to be aligned with the connectivity based on intelligent path computation and dynamic connectivity creation and scaling. Correspondingly, network connectivity has to comply with the service requirements leveraging on multiple functionalities, like traffic steering (path, slice, and service chain) and fine-grain performance measurement & visualization. The connectivity has to follow a similar paradigm, being able to select the path matching the target SLA and having the ability to scale according to service-based criteria. Measurable SLA, constant monitoring and proactive management are needed to obtain a determined service quality.

5.3 Inter-connection of Clouds

Generally, enterprises may place their data and applications and data in multiples Cloud sites or pools belonging to the same Cloud provider, although in most cases, they belong to different Cloud providers. For single data access, data may be pulled from lots of disparate sources in different geographic locations. Therefore, operators need to provide inter-Cloud connections between Cloud pools operated by the same or different Cloud providers. Some of the connections may be based on the public Internet. Some may be based on dedicated MPLS/VPLS networks. Since inter-connection of Clouds can contain multiple network segments or functions, in a virtualized manner on standardized hardware platforms, orchestrator and controller are deployed to quickly scale and deploy network connection services. In particular, controllers of a Cloud operator may provide open interface to the orchestrator, which may be operated by network operator, to activate and terminate these connections across multiple networks, manage the elastic scaling at run-time, and optimize their use of the underlying infrastructure with high performance and reliability.

The orchestrator refers to different types: functional orchestration and collaborative orchestration. The function orchestration is composed of SDN orchestrator, NFV orchestrator and Cloud management platform. The SDN orchestrator connects with controllers, such as metropolitan area network controllers, backbone network controllers and DC controllers, and provides the capabilities of cross-domain network configuration and monitoring. The NFV orchestrator configures and orchestrates virtual network elements. The Cloud management platform controls management and orchestration of Cloud computing resources in the DC.

Functional orchestration provides information provision to applications, such as provision of network topology, route path setting and delivery node selection. In addition, it also provides conflict management and negotiation mechanism to maintain policy consistency among different controllers [i.15]. Collaborative orchestration unified scheduling of SDN orchestrator, NFV orchestrator and Cloud resource management platform to provide end-to-end configuration and orchestration of services.

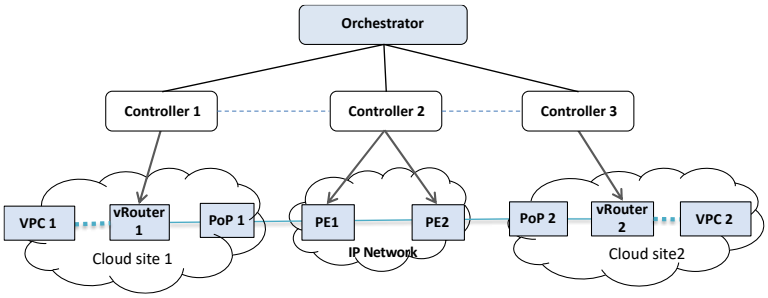

Figure 4: Inter-connection of Clouds

Major requirements to inter-Cloud connections can be inferred and listed as below.

1) Performance guarantees

   The network should guarantee performance to applications with stringent requirements of delay, jitter as well as a reliable connection for the inter-Cloud connections. To select the path to meet the needs of the applications, separated tools for measuring application performance are required. With the collection of this information, utilization of path selection avoid heavily utilized path or route presenting a longer path. Underlay routing, that is not performance-based, cannot provide those functionalities.

2) Security

   As mentioned above, some connections between Clouds may run over the public Internet. In this case, security, such as data privacy and anti-attack, should be given high priority. The first and also the most common way to guarantee security is via a secure channel, such as an IPSec tunnel. When a data path from Cloud A to Cloud B is set up, the IPSec tunnel is initiated via the controller or other management system. In addition, since multiple enterprises may share the same connection between Clouds, information of customer A should not be leaked to customer B and vice versa, even if they share the same link.

3) Agility

   Service agility is a basic requirement to the network-Cloud convergence, including communications between Clouds. Service agility depends not only on high-capability underlay, but also on an integrated resource management and operation system which can dispatch the resources within the Cloud and public network in response to customers' demands. However, when multiple Cloud providers are involved in an application, the interconnection and coordination between the integrated resource management and operation systems should be implemented to ensure that the setup and configuration of the connection runs smoothly without any malfunction caused by the interconnection or inconformity.

4) Scalability

There may be different Cloud interconnect models having different scalability. Some architectures do not scale very well and usually surface the N-squared problem. When a new Data Centre is added, the number of additional connections added is the same as that of other Data/Cloud Centres. One typical model to alleviate this problem is via a Cloud interconnect, when enterprises have access to multiple Clouds from a single connection in a single location. Or when enterprises have lower traffic and require lower capacities compared to dedicated one-to-one interconnect. This is a connection to multiple Cloud providers through a single connection to a provider's exchange switch. Colocation providers or internet exchanges may offer this service. Some overlays are used to manage the complexity. These overlays come in the form of an IPSec tunnel with some type of overhead for segmentation. Most of the time, VXLAN would be used to setup layer two segments across the layer three network infrastructure.

5.4 Data Centre network

A Data Centre network is a large, sophisticated distributed system. It comprises hundreds of thousands of servers, tens of thousands switches and routers, and millions of cables and fibres. It connects servers with high speed and provides high server-to-server bandwidth. A Data Centre network is usually composed of intra-DC networks and network services, and inter-DC network and network connectivity services. In addition, DC networking elements can act as strict L2 switches and/or provide IP routing capabilities, including network service virtualization.

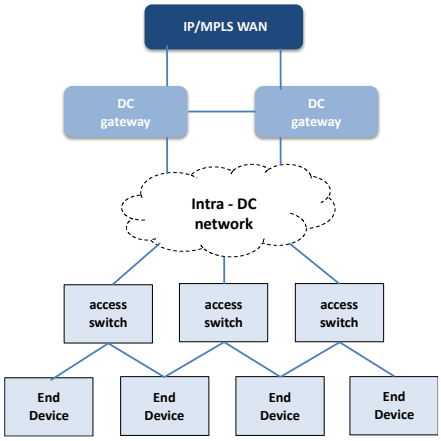

Figure 5: Typical architecture of Intra-DC network

An Intra-DC Network is a network composed of high-capacity core nodes (Ethernet switches/routers). A generic architecture for Data Centres is depicted in Figure 4. It provides a view of the physical components inside a DC. There are 2 major components in an intra-DC network:

- Access switch: Ethernet switch aggregating all Ethernet links from the end devices in a rack representing the entry point in the physical DC network for the hosts. For instance, it may also provide routing functionality, virtual IP network connectivity, or Layer 2 tunnelling over IP. Access switches are usually multi-homed to aggregation switches in the Intra-DC network. A typical example of an access switch is a Top of Rack (ToR) switch. Other deployment scenarios may use an intermediate Blade Switch before the ToR, or an End-of-Row (EoR) switch, to provide similar functions to a ToR.
- DC gateway: Gateway to the outside network providing DC interconnect and connectivity to Internet and VPN customers. DC gateway may be simply a router connected to the Internet and/or an IP VPN/L2VPN PE. Some network implementations may dedicate DC GWs for different connectivity types (e.g. a DC GW for Internet and another for VPN).

To avoid congestion, the intra-DC network always adopts the leaf-spine architecture, which consists of two layers: the leaf layer and the spine layer, which reduces the hops and guarantees reduced delay. At the first tier, tens of servers use 10 GbE or 25 GbE Ethernet NICs to connect to a Top of Rack (ToR) switch and form a Pod. Tens of ToR switches are then connected to a second tier of Leaf switches. These servers and ToR and Leaf switches form a Pod set. Multiple Pod sets then connect to a third tier of Spine switches. Using existing Ethernet switches, an intra-DC network can connect tens of thousands or more servers with high network capacity. Leaf-spine architecture provides a redundancy multi-path network. ECMP (equal cost multi-path) is used to load-balance traffic across all the paths. ECMP uses the hash value of the TCP/UDP five-tuple for the next hop selection. As a result, the exact path of a TCP connection is unknown at the server-side even if the five-tuple of the connection is known. For this reason, locating a faulty Spine switch is not easy.

The inter-DC network interconnects with the intra-DC networks and connects the intra-DC networks to the public Internet. It uses high-speed, long haul fibres to connect Data Centres networks at different geolocations. Software-defined networking is further introduced for better wide area network traffic engineering.

With the development of the 5G and Cloud era, more and more services and data have migrated to the Cloud. As data hub connecting computing and storage resources, IPv6 evolution of Data Centre network becomes increasingly important. However, with the development of IPv6 services and increasing traffic, Data Centre networks face new challenges. Traditional IPv6 networks provide best-effort forwarding, which does not meet the computing and storage requirements for zero packet loss. In the Cloud era, the service deployment speed is accelerated. Manual network deployment cannot meet the requirements of rapid service development. The network is becoming more complex and larger, which has exceeded the limit of manual processing. Therefore, in addition to using IPv6 technologies to meet increasing address requirements, networks need to integrate other advanced technologies such as Cloud computing, artificial intelligence, and big data analytics to evolve to IPv6. In the IPv6 era, Data Centre networks will move towards hyper-converged architecture, which has the following three characteristics:

- Unified architecture: Traditional Data Centres use dedicated networks, such as InfiniBand and Fibre Channel (FC), to carry high-performance computing (HPC/AI) and storage. These dedicated network architectures are not compatible with IPv6. Therefore, IPv6 Data Centre networks should overcome the limitations of multi-protocol architectures for computing, storage, and service networks. It has to build a hyper-converged network architecture with zero packet loss over IPv6, implementing protocol convergence for Data Centre service networks, computing, and storage networks.

- Automatic deployment: The Data Centre network lifecycle is automated, services are deployed within minutes, and simulation verification is implemented based on the IPv6 network, ensuring 100 % correct service deployment.

- Intelligent O&M: The scale of IP networks increases by 100 times than before. The relationship between network objects such as ports and policies reach millions. Network O&M cannot be performed manually. In the IPv6 era, a more comprehensive network system management solution is required to monitor the network health status in real-time at the device layer, network protocol layer, and service running layer. This is needed to detect the network status in advance, and quickly locate and solve network faults, improving O&M efficiency.

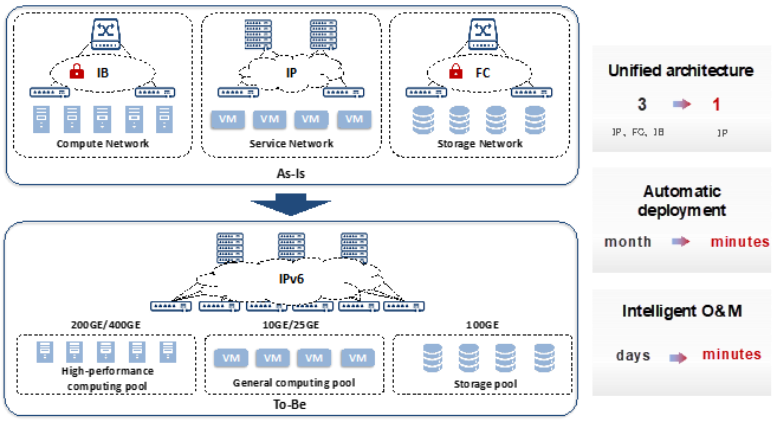

Figure 6: Hyper-converged Data Centre network architecture

5.5 Telecom Cloud network

The arrival of the Cloud era is driving not only the transformation of enterprises' IT systems and the mode of service provisioning, but also the evolution and upgrade of traditional networks of operators, it is evident that Clouds and networks are breaking through each other's boundaries. The goal of Cloudified-network is to build simple, automatic, and intelligent networks that can quickly and flexibly adjust resources for service innovation.

Regarding to the network element, traditional networks, such as MAN, use equipment with closed architecture, which means that not only the hardware is dedicated but also the software is closely coupled with the hardware. This architecture is not flexible enough to meet the various requirement of the changing market. The rapid innovation on the internet has brought uncertainty in network service and traffic, and the network with dedicated hardware is difficult to meet service growth needs. The design concept of the IT industry needs to be introduced into networks. With SDN/NFV as the basic architecture, more and more network elements will be Cloudified, such as vBNG/vBRAS, vCPE and vFW.

Another change is network architecture. Separation of control and forwarding can improve the resource utilisation efficiency, simplify device design, and allow flexible service deployment. The Cloud-based control plane is deployed centrally or distributed and schedule the resource based on the requirement of up-layer services, traffic pattern and volume, performance index, etc. Due to the high complexity of multi-vendor and cross-domain management, it is suggested that controllers should be simplified as far as possible and be deployed in different domains. The controllers in different domains should coordinate with each other to create connections. Different from the control plane, the forwarding plane mainly provides high-speed and differentiated packet forwarding. Compared with traditional networks, the control-forwarding separation architecture can reduce the requirement of the network equipment.

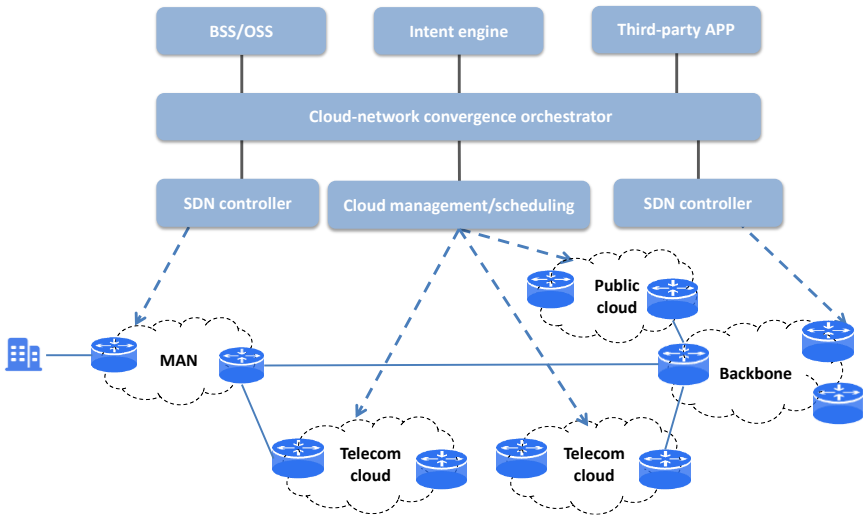

Figure 7: Architecture of Cloudified telecom network

The focus of improving the network-Cloud convergence experience is to optimize service processes. To deliver network-Cloud converged products and services, operators need to build a new-generation O&M system. Integrated network-Cloud orchestration is the key to the new-generation O&M system and the basis for one-point service provisioning and end-to-end service guarantee. With this new architecture, operators need to have the network ability of closed-loop automation. Data collection is the basis of closed-loop automation. Traditional network management methods, such as SNMP and FTP, are inefficient. To meet real-time collection requirements, it is necessary to introduce telemetry that can achieve millisecond sampling, improve the collection ability and support real-time data reporting. The introduction of intelligence can further enhance the network-Cloud collaboration efficiency and give users a better experience. Building the intelligent system is a gradual process, which can be applied first in network elements and individual function points to enable point-like network element optimisation and intelligent fault analysis, optimisation and intelligent fault analysis. Moreover, intelligent abilities of network elements are connected to form end-to-end intelligence capabilities to support fault location and demarcation recovery and self-healing. Along with the network-Cloud convergence, the introduction of intelligence into the new architecture needs further research.

6 Related IPv6 technology

6.1 Application-aware IPv6 networking (APN6)

With the development of 5G and industry verticals, many new businesses have emerged with diverse and high requirements for network bandwidth, latency, jitter, and packet loss, etc. Applications such as online gaming, live video streaming, and video conferencing have high requirements on network performance. It is important for network operators to provide differentiated SLA guarantees for various applications to increase revenue.

Application-aware Networking (APN) has been proposed in IETF. The application-aware IPv6 network uses the programmable space of IPv6 data message Extension Headers, such as Hop-by-Hop Options Header and Segment Routing Header, to carry related application-aware information. Application characteristic information such as application-aware identification and network performance requirements is held in the packet encapsulation, to facilitate service provisioning, perform fine-granularity traffic steering and network resource adjustment. It defines the application-aware options (i.e. application-aware ID option and service-aware para option), which can be used in the above listed different IPv6 extension headers for the purpose.

The application information carried in the data message in the APN6 network can indicate:

- the application which the data message belongs to;
- the user information that uses the application;
- the key streams in the application (i.e. the video stream/voice stream in the video conference, and the Cloud game Action instructions, etc.);
- the SLA requirements, or network performance requirements parameters (i.e. bandwidth, delay, jitter, packet loss rate).

Application-aware information can be directly generated by user terminal devices/applications, or can be generated by network edge devices, corresponding to the host-side solution and network-side solution of APN6, respectively.

APN6 is an ongoing work and almost 10 drafts have been submitted to IETF, they cover clarifications and requirements, frameworks, use cases, security, Gap analysis, etc. APN6 can be further combined with new network services (i.e. Network slicing, IFIT, SFC, etc.) to perform performance testing for key VIP applications and achieve effective performance degradation positioning and demarcation.

6.2 Hyper-converged Data Centre Network

6.2.1 Building an IPv6 lossless Data Centre based on intelligent lossless technologies

As is well known, traditional IP networks use the best-effort mechanism. The inherent packet loss feature brings a great impact on service performance and stability.

Impact: The intelligent lossless technology based on IPv6-based intelligent scheduling can accurately schedule queues based on traffic characteristics such as queue lengths, ensuring high throughput, low latency and zero packet loss.

The RoCE technology has high requirements on the packet loss rate of the underlying network, and the performance deteriorates sharply when it exceeds 1e-05. Therefore, zero packet loss, low latency, and high throughput are the three core features of the high-performance all-IP Data Centre network.

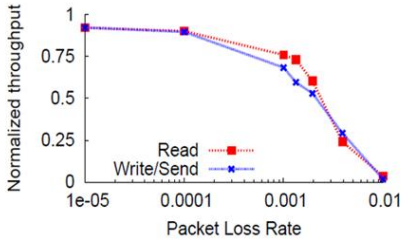

Figure 8: Impact of network packet loss on throughput

The three core indicators interact with each other, have a seesaw effect, and at the same time reach optimality, thus posing a great challenge: "zero packet loss" which will reduce the bandwidth, resulting in ultra-low throughput, which will in turn increase the transmission delay of large streams.

"Low latency" means that queues of switches are reduced, resulting in low throughput.

High throughput means that high link utilisation needs to be maintained, which leads to congestion and queuing of switches, leading to the high latency of small flows. The core technology behind this feature is the congestion control algorithm.

The general congestion control algorithm of a lossless network requires coordination between the network adapter and the network. Each node needs to configure tens of parameters, and the total number of parameters of the network reaches hundreds of thousands. To simplify the configuration, only general configurations can be used. As a result, the three core indicators cannot be met for different traffic models.

In order to obtain intelligent lossless all-IP Data Centre network, intelligent algorithms such as AI Explicit Congestion Notification (ECN) and AI training based on the live network traffic model are needed. Network traffic changes can be predicted, and ECN thresholds can be adjusted based on traffic characteristics such as queue lengths, enabling to accurately control lossless queue cache. In this way, the optimal performance of the entire network is ensured.

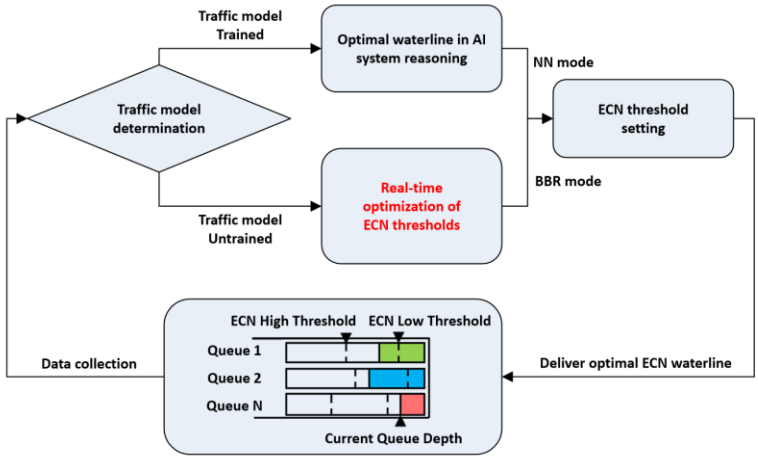

Figure 9: AI Explicit Congestion Notification Algorithm Framework

6.2.2 Improving storage network performance in Data Centres

Traditional IP networks can only converge within seconds when a storage network is faulty, which sharply deteriorates storage service and severely impacts the Data Centre performance. The intelligent lossless storage network uses state of the art protocols:

Non-Volatile Memory express (**NVMe**) enables fully exploiting the SSD speed and latency, supporting parallel operations to increase the total bandwidth utilisation, removing the bottleneck of the SATA protocol.

NVMe over Fabric (**NVMe-oF**) uses an alternate data transport protocol (over fabrics) as a transport mapping instead of the PCIe bus used by NVMe. Fabrics are built on the concept of sending and receiving messages without shared memory between endpoints.

Remote Direct Memory Access (**RDMA**) enables data and memory to be transferred between computer and storage ' 'device's main memory in a network without involving the processor, cache, or OS.

Converged Ethernet is an enhanced Ethernet version, also known as Data Centre Bridging and Data Centre Ethernet. This solution provides the Link Level Flow Control mechanism assuring zero loss, even when the network is saturated.

RDMA over Converged Ethernet (**RoCE**) enables to sum the benefits of RDMA and Converged Ethernet.

RoCEv2 is an Ethernet layer 3 (internet) protocol, which means packets can be routed. It supports **IPv6** e2e allowing the construction of all-IPv6 Data Centre network.

NVMe-oF over RoCEv2 is the state-of-the-art protocol**.** The maximum benefits are exploited when used with IPv6, granting a high level of automaticity of the Data centre lifecycle, with the possibility to expand the Data centre using limitless address space, where expansion rules are simple and with no exceptions.

The support of an end-to-end IPv6 based intelligent lossless storage network allows real-time detection of the loss of connectivity with servers.

Link Level Flow Control mechanism assures zero loss, even when the network is saturated. Servers, switches, and storage devices work together to detect faults and notify the entire network quickly. The fault convergence time is reduced to less than one second.

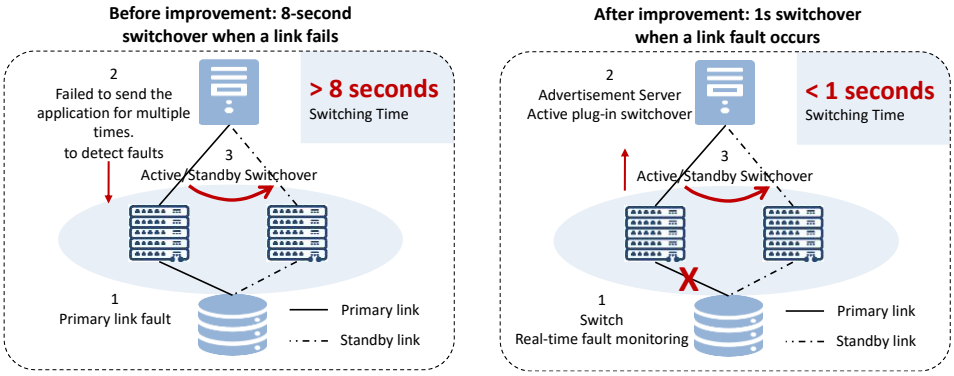

Figure 10: Improvement in fault recovery time

6.2.3 Automatic Data Centre lifecycle automation and intelligent O&M based on network-based automated driving technologies

With the development of the global IPv6 process of Data Centre networks, the industry is actively exploring the extension of general computing network automation capabilities to high-performance computing and storage networks, integrating general capabilities and fully adapting to special scenarios:

- Intent-based Expert Recommendation System:

  In the all-IPv6 network architecture, hyper-converged Data Centre network can use a unified network management and analysis platform to implement the automatic deployment of IPv6 network planning, construction, O&M, and optimisation. Perform intelligent queue planning and design based on the service intent, recommend the design scheme, and perform automatic simulation verification on the design scheme to ensure that the solution implementation result is consistent with the service intent.

- Visualized and intelligent O&M:

  Common computing network faults are mainly connectivity faults. Common O&M methods such as trace and ping can effectively detect faults, which are not sensitive to performance faults. In addition to traditional fault scenarios, high-performance computing and storage networks add the poor-quality fault category, that is, analysis of performance specifications when the network performance does not reach the expected performance.

For self-proving and quick fault locating and recovery on the network side, the network first solves the performance visualization problem and then implements dynamic closed-loop based on the perception of performance specifications and service performance status. To meet general monitoring requirements, a hyper-converged Data Centre network uses Telemetry to collect data in real-time, comprehensively evaluate network health of devices, networks, protocols, overlays, services and generate reports. This helps O&M personnel learn the network and intuitively display the overall network experience quality. In addition, IPv6 packet colouring and intelligent flow analysis (edge intelligence) technologies are used to measure network SLA indicators such as packet loss and delay to locate end-to-end network packet loss and delay.

7 Benefits analysis

7.1 IPv6 for network-Cloud convergence

In recent years, more and more enterprises and industries have moved their businesses to the Cloud. As more and more enterprise applications are Cloudified, the network needs to be flexibly called by the application on the Cloud to achieve "network as service". This requires creating an intelligent Cloud network to order Cloud network products with just one click and automatically match network resources, quickly open, and adjust the business flexibly. As a new generation of network protocol, IPv6 will provide multiple advantages to network-Cloud convergence.

Firstly, IPv6 can provide enough address resource for Cloud services. As an important part of information infrastructure, Cloud computing needs many IP addresses to number its virtual machines, and the scale of address requirement increases exponentially. Unfortunately, when the Cloud computing industry took off, it encountered IPv4 address exhaustion problem globally, as IPv4 could not provide enough addresses to Cloud services. With 128-bits address identifier, IPv6 can meet the addressing requirement of every service instance, including those in the Cloud.

Secondly, IPv6-based innovative technologies like SRv6 can help to provide network programming capability in the network. SRv6 leverages the source routing paradigm in IPv6 networks to achieve a network objective that goes beyond mere packet routing. With SRv6, an ingress node steers a packet through an ordered list of segments. Each segment represents a function to be called at a specific location in the network. A function is locally defined on the node where it is executed and may range from simply moving forward in the segment list to any complex user-defined behaviour.

Next, IPv6 can improve performance, ease of use, and troubleshooting issues in the above scenarios. The IPv6 protocol was designed to reduce the processing burden by the simple representation of the header and structure. The structure of the IPv6 addressing scheme provides the possibility of optimising and managing traffic within and between the Internet and Data Centres. For instance, ICMPv6 [i.16] delivers a more effective way for mutual communication between hosts, solving L2 broadcast and expansion problems within a local network. Also, when IPv6 is deployed, IPsec can be implemented to make all communications more secure through proper authentication and encryption.

7.2 Network and Cloud management benefits

Driven by multiple factors such as enterprise digital transformation, Cloud service and competence improvement, more and more enterprises, industries and government agencies have moved their businesses to the Cloud. With the clouding of key information systems and core production systems, enterprises have increased business reliability and usability through Cloud disaster-recovery and multi-activity deployment; flexible resource expansion has been realized through hybrid Clouds. Along with more and more applications of an enterprise being Cloudified, the network needs to be flexibly called by the application on the Cloud to achieve "network as service". As a new generation of network protocol, IPv6 will provide multiple advantages to network-Cloud integration.

The structure of the IPv6 addressing scheme provides the possibility of optimizing and managing traffic within and between the Internet and Data Centres. The new function of ICMPv6 offers a more effective way for mutual communication between hosts, which can solve L2 broadcast and expansion problems. Implementing IPv6, IPsec is mandatory to make all communications more secure through proper authentication and encryption.

Those functionalities can match the agility in service creation and management currently available in the Cloud environment with AI management technologies. Paths with granted SLA end to end, leveraging on IFIT to monitor performance, enable near real-time measurement of each single connectivity flow’s performance, helping to provide connectivity on-demand and dynamic scalability.

The trend of network-Cloud convergence and IPv6 transition is happening simultaneously and interrelated. The future network and Cloud should not only be IPv6-ready but rather IPv6-based to provide users with more agile and scalable network and Cloud services. IPv6 has been a mature and scalable protocol. By deploying IPv6, Cloud and IP network convergence can truly benefit from the improvements brought by next-generation IP. It has the advantage of flexibly adding new features and options according to the requirements of Data Centres, which is conducive to large-scale deployment of Cloud-based services.

7.3 Hyper-converged Data Centre network benefits analysis

7.3.1 Hyperconverged network benefits analysis with unified IPv6 architecture

In Figure 11, the high-performance computing zone, storage area, and general computing zone are constructed using the IB, FC, and Ethernet networks.

Servers in the computing zone need to be configured with Ethernet and IB dual network adapters. Servers in the storage zone need to be configured with Ethernet and FC dual network adapters.

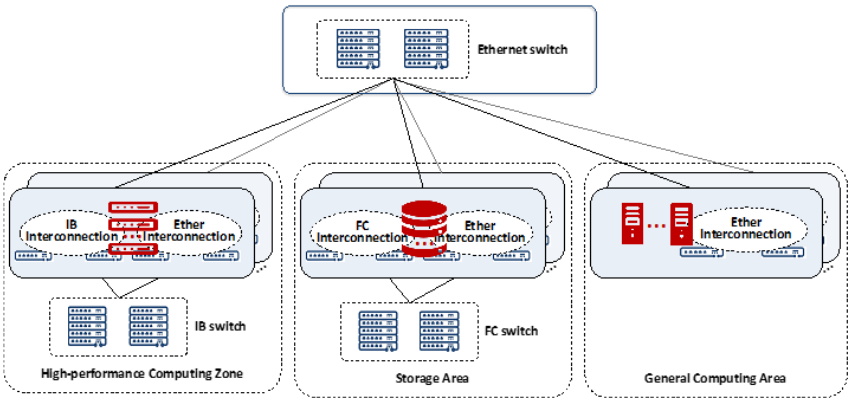

Figure 11: Architecture of multiprotocol networking

The second networking is the lossless Ethernet networking architecture. Compared with networking 1, the architecture is significantly simplified.

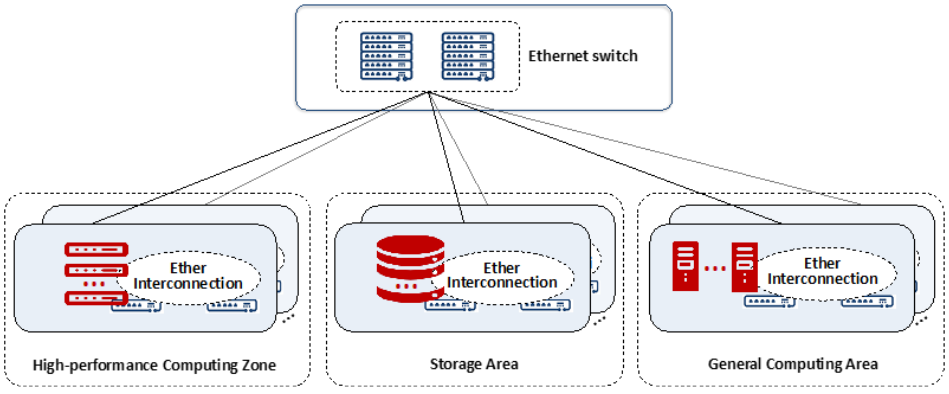

Figure 12: Architecture of the lossless Ethernet networking

To compare the costs of the two networking modes, the following assumptions can be made:

1) The number of computing servers is Nc, the number of storage servers is Ns, and the number of general computing servers is Na.

2) The prices of each port of IB, FC, and Eth switches are Pi, Pf, and Pe respectively.

3) The price per port of the IB NIC is Pni, the price per port of the FC NIC is Pnf, and the price per port of the Eth NIC is Pne.

4) In cost estimation, Nc = 1 000, Ns = 1 000, Na = 5 000, and the price per port of the Eth switch is Pe (approximately 1 000) is used as the benchmark.

$$Pi = 3 \times Pe,\ Pf = 3 \times Pe,\ Pni = 3 \times Pe,\ Pnf = 3 \times Pe,\ \text{and}\ Pne = 3 \times Pe.$$

To simplify the proof, the default convergence ratio of the Data Centre networking is 1:1. In other cases, you can similarly perform the following proof. Under the above assumptions, the estimated cost decreases by 36,4 % after adopting the full Ethernet network architecture.

In addition to cost advantages, the all-Ethernet network architecture has a sound and open ecosystem, which can effectively mitigate service continuity risks brought by private networks.

Table 1: Hyperconverged Data centre benefits

Networking	Number of IB ports	Number of Fibre Channel ports	Number of Ethernet ports	Number of IB NICs	Number of FC NICs	Number of Ethernet Cards	Cost calculation	Cost estimation	Cost Reduction Percent
Networking 1 (IB + FC + Eth)	3Nc	3Ns	3Nc + 3Ns + 3Na	Nc	Ns	Nc + Ns + Na	3Nc × Pi + 3Ns × Pf + (3Nc + 3Ns + 3Na) × Pe + Nc × Pni + Ns × Pnf + (Nc + Ns + Na) × Pne	66 000 × Pe	/
Networking 2 (All Ethernet)	0	0	3Nc + 3Ns + 3Na	0	0	Nc + Ns + Na	(3Nc + 3Ns + 3Na) × Pe + (Nc + Ns + Na) × Pne	42 000 × Pe	36,4 %

Formatted: French (Switzerland)

7.3.2 Benefits analysis of full lifecycle automated management

In the entire lifecycle of a Data Centre, more than 80 % of the time is spent on O&M. The O&M efficiency determines the operation efficiency of the Data Centre.

After more than ten years of development, many network auxiliary management software with different functions have been accumulated in the Data Centre. Historically, the number of tools used may exceed a thousand. These O&M tools are classified into four categories: NE management, network configuration, Status monitoring and data analysis. Multiple sets of O&M tools run independently. On the one hand, functions are limited and only one O&M life cycle can be solved.

The end-to-end efficiency improvement is limited. On the other hand, O&M data and analysis results cannot be shared among different tools.

The root cause of the E2E fault is analysed. O&M personnel need to perform the secondary analysis. As a result, the service experience is difficult to manage. The network department receives the fault.

More than half of user complaints are related to the service experience.

After the management, control, and analysis capabilities of the network management layer are converged, the unified Telemetry Big Data is used to implement the network management interface.

Convergence: One intelligent O&M system can implement full lifecycle management from planning, construction, maintenance, and optimisation, reducing or eliminating the need for manual operations.

Take service provisioning as an example. The network deployment time can be reduced from 3 to 5 days to several minutes, significantly improving service deployment efficiency.

8 Conclusion

Network-Cloud convergence refers to comprehensive integration of Cloud computing resources and network facilities, to create an integrated supply, operation, and servicing system by leveraging new CT and IT technologies. In order to give a detailed illustration of network-Cloud convergence, the present document lists several typical use cases of Cloud-network convergence, the architecture and requirement of each use case are analysed and the role of IPv6 is discussed as well. Based on the analysis and discussions, the following conclusions can be reached.

Firstly, network-Cloud convergence will comprehensively re-architecture the information architecture. When more and more enterprise applications put their applications and data assets into Cloud, Cloud will be the centre of the infrastructure, and the network will be built round the Cloud Data Centre. Moreover, Cloud service provisioning requires faster, better, and more flexible connections, which pose new requirements to the network, such as low latency, fast provisioning and high reliability.

Secondly, operators are Cloudifying traditional telecom network by leveraging SDN and NFV technologies to improve automation and intelligence. Cloud which hosts telecom services and network functions is called Telecom Cloud, it is an extension of traditional network. Compared with traditional IT systems, Cloudified network services pose stricter requirements to the underlying Cloud infrastructure, in terms of real-time, large capacity, high security and reliability. Telecom Cloud changes the form of network functions and pushes the evolution of network architecture.

Thirdly, as a new generation of network-layer protocol, IPv6 will play an important role for network-Cloud convergence. During the recent years, IPv6 has been widely deployed all over the world, while, SRv6 related technologies have also been under development. SRv6 is a source-routing transmission protocol, which is essentially an extension of the IPv6 basic protocol. In a SRv6-capable network, the source node guides the packet forwarding by encapsulating the list of instructions in the SRH extension header. For network-Cloud integration, IPv6 and SRv6 can provide an end-to-end transmission and network programmability for the services of customers and traffic scheduling.

Finally, network-Cloud convergence will not be realized overnight, it will take a long time. Three steps of network-Cloud convergence have been proposed in the present document, synergy, integration and unification, However, it does not mean that every network should follow this path. For any given operator, the degree and pace of network-Cloud convergence may depend on its network architecture, market policy and business strategy. Network-Cloud convergence is not only a change in the technology, but business transformations involving organizational structure, production process, management model, and human-resource reconstruction.

History

Document history		
V1.1.1	April 2022	Publication