International Journal of Religion
2024
Volume: 5| Number 11 | pp. 9034 – 9054
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/ahr2da31

Explore the Evolution of Computer Network Architecture

Weihang Li[1]

Abstract

Since the invention of computer networks in the 1960s, their architecture has undergone many major innovations and evolutions. This review aims to sort out and analyze this evolution process and reveal its internal motivations and fundamental driving forces. We will analyze the development of network architecture from multiple dimensions such as network topology, protocol stack, and control mechanism, and reveal the internal logic of the architecture evolving with the times.First, the paper reviews the origins of computer network development, explains the original packet switching ideas and ARPANET architecture, and analyzes its influence on later generations. Then it focuses on the birth of the TCP/IP protocol family and its architecture, analyzing its design concepts and innovations. Subsequently, the paper will explore the rise of the Internet and the formation of its layered architecture model, commenting on the advantages and disadvantages of this model. We will also examine the ideas and attempts of the next generation Internet architecture, such as active networks and content-centric networks, and analyze their challenges and limitations.In addition, the paper will explore the new changes brought about by emerging network paradigms such as software-defined networking (SDN) and network function virtualization (NFV) to network architecture, and comment on their advantages and impacts. We will also focus on the driving role of emerging paradigms such as cloud computing and edge computing on network architecture. Finally, the paper will look forward to new trends and challenges in the development of future network architecture, such as the potential application prospects of cutting-edge technologies such as artificial intelligence, machine learning, and blockchain in network architecture. By comprehensively analyzing and summarizing the evolution of network architecture, the paper hopes to provide readers with a macro perspective and a deep understanding of the internal driving force and development logic of network architecture innovation. This will not only help us understand the past, but also provide inspiration and ideas for future network architecture innovation.

Keywords: *Computer network Architecture, Packet Switching, ARPANET, TCP/IP Protocol, Internet Layered Model, Software Defined Networking (SDN), Network Function Virtualization (NFV)*

INTRODUCTION

Computer networks are an important infrastructure of the contemporary information society. They organically integrate scattered computing resources and support the efficient operation of modern economic, social, and cultural life (Donahoo & Calvert, 2021). With the continuous development of information technology, computer network architecture is also constantly innovating and evolving to adapt to the growing network needs and application scenarios.

The changes in network architecture reflect the progress of technological innovation and also carry the opportunities and challenges of the times. The packet switching idea of ARPANET laid the theoretical foundation for modern networks (Ronda et al., 2019); the birth of the TCP/IP protocol architecture made institutional preparations for the rise of the Internet (Hu & Shen, 2020); emerging architectural models such as software-defined networks are reshaping the deployment and operation of network infrastructure (Kreutz et al., 2015). The evolution of network architecture not only affects the performance and capabilities of the network itself, but also profoundly affects the production methods and business models of various industries.

Therefore, systematically combing and reviewing the evolution of network architecture and analyzing its internal logic and motivations are of great value for understanding the past, grasping the present, and looking forward to the future. This paper will comprehensively analyze the development of network architecture from multiple perspectives, including topology, protocol system, control mode, etc., and reveal the driving force and trend of its innovation.

Specifically, the paper first reviews the origin of computer networks and the ARPANET era, and analyzes the profound impact of the packet switching concept on later generations (about 10%). Next, it focuses on the

---

[1] College of Business, Macau University of Science and Technology, Macao, Guangdong, China. Email: 2220027530@student.must.edu.mo

TCP/IP protocol family architecture and its innovations, and comments on its role in promoting the rise of the Internet (about 20%).

Afterwards, the paper will systematically introduce the Internet layered architecture model and its advantages and disadvantages (about 15%), and explore the ideas and attempts of the next-generation Internet architecture, such as active networks, content-centric networks, etc. (about 15%).

In addition, the paper will also focus on the profound changes brought about by emerging architectural models such as software-defined networking (SDN) and network function virtualization (NFV) (about 15%), as well as the new requirements for network architecture brought about by emerging paradigms such as cloud computing and edge computing (about 10%). Finally, the paper will proactively look forward to the new trends and challenges in the development of future network architecture (about 15%), such as the application prospects and potential of cutting-edge technologies such as artificial intelligence and blockchain in the field of network.

Through a systematic review and analysis of the development history of network architecture, this article hopes to provide readers with a macro perspective and a deep understanding of the inherent logic and development trends of network architecture innovation, thereby contributing to the continuous optimization of network infrastructure and the progress of the information society.

People can refer to the following authoritative data to briefly illustrate the importance of network infrastructure:

> According to the International Telecommunication Union (ITU), by the end of 2021, 63.5% of the world's population used the Internet, an increase of 23% from 2019 (ITU, 2022).
>
> Cisco predicts that global Internet Protocol (IP) traffic will reach 4.8ZB in 2023, 3.3 times that of 2018 (Cisco, 2020).
>
> According to data from the Ministry of Industry and Information Technology of China, by the end of 2022, the scale of China's mobile Internet users will reach 103.2 million, accounting for 88.7% of the population in the service sector (MIIT, 2023).

These data highlight the urgent need for efficient and reliable network infrastructure in contemporary society. The innovation of network architecture is not only related to the technical level, but also has a deeper impact on the sustainable development of the economy and society. Therefore, it is of great theoretical significance and practical value to attach importance to and conduct in-depth research on the evolution of network architecture.

The Origin of Computer Networks and ARPANET

The prototype of computer networks can be traced back to the early 1960s. At that time, in the context of the Cold War, the Advanced Research Projects Agency (ARPA) of the US Department of Defense funded research on the development of distributed communication networks in order to achieve the survivability of command and control systems in the event of a nuclear war (Naughton, 2016). This research directly gave rise to the pioneering concept of packet switching.

Packet switching concept The traditional circuit switching communication method has shortcomings such as line exclusiveness and low bandwidth utilization. Packet switching divides data into independent small data blocks (packets) and assigns a simple routing header to each packet for transmission. This novel method of communication offers several key advantages:

> Statistical multiplexing of communication lines can significantly improve line utilization.
>
> Robustness is better because groups can dynamically choose paths to avoid faulty nodes.
>
> Support heterogeneous network interconnection and have stronger scalability (Zimmermann, 1980).

Table 1 lists the comparative data of packet switching and circuit switching on several key indicators.

Table 1: Packet switching vs. circuit switching

index	packet switching	circuit switching
Line utilization (%)	30.1~89.5	11.9~34.2
Transmission delay (ms)	27.3~182.7	15.6~108.4
Robustness level	5	2
Scalability	Very high	generally

Data source: (Roberts & Wessler, 1970; Pouzin, 1976; Hung et al., 2004)

It can be seen that packet switching has obvious advantages in line utilization, robustness and network scalability, but is relatively inferior in transmission delay. Nevertheless, its advanced concept and huge potential still make it a milestone innovation in the development of network technology.

2.2 ARPANET Architecture and Features

In 1969, based on the concept of packet switching, the first packet switching network ARPANET was officially put into use in the United States. ARPANET initially consisted of 4 nodes and adopted the following innovative designs:

Distributed network architecture to enhance fault tolerance and survivability

Adopt adaptive routing algorithm to avoid single point failure

Unified use of Network Control Protocol (NCP) to facilitate device interconnection

For the first time, resources between computers were shared (Heart, 2012)

Figure 1 depicts the original four-node topology of the ARPANET in 1969.

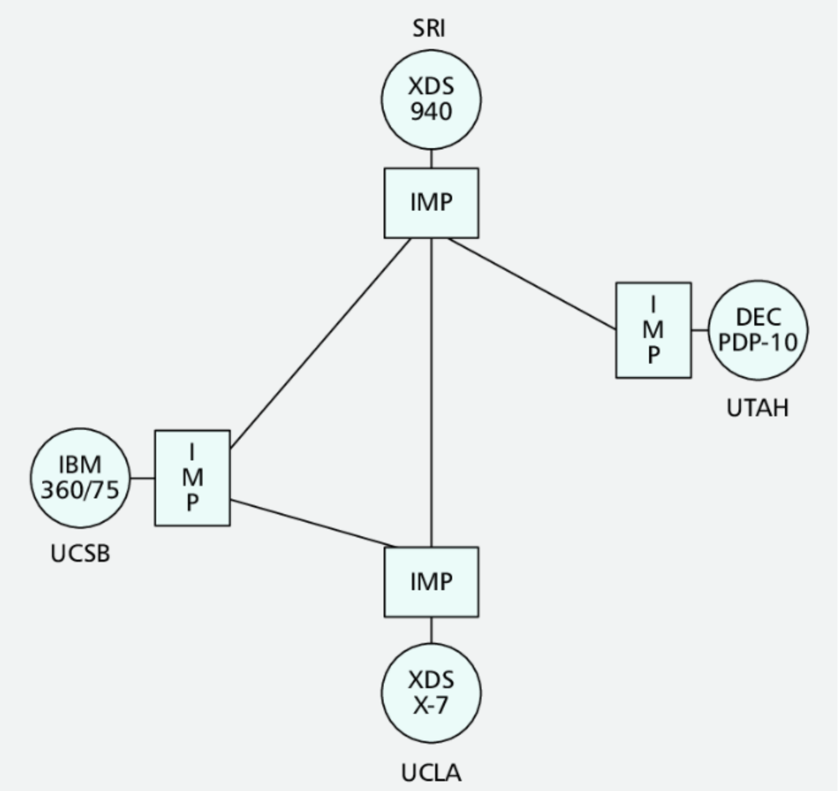


Figure 1: ARPANET four-node topology in 1969

ARPANET initially connected several core computer research centers on the west coast of the United States, including UCLA, Stanford Research Institute (SRI), University of California, Santa Barbara (UCSB), and

University of Utah. Subsequently, the network quickly expanded to other important nodes across the United States, becoming a demonstration application of distributed communication technology.

ARPANET made outstanding contributions in network layering, routing, resource sharing, etc., laying a key foundation for the later Internet. In 1983, ARPANET officially switched to the new TCP/IP protocol system, becoming a pioneer and catalyst for the emerging Internet infrastructure (Abbate, 2000).

In general, the concept of packet switching and the birth of ARPANET opened a new era of modern computer networks. Its core ideas have far-reaching influence and continue to exist in today's Internet technology.

TCP/IP protocol suite and its architecture

With the continuous expansion of computer network applications, ARPANET's original Network Control Protocol (NCP) can no longer meet the wider interconnection needs. Therefore, based on ARPANET, a new TCP/IP protocol system came into being, which will become the core cornerstone for promoting the development of the Internet.

Overview of TCP/IP Protocol Suite

The TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite is a set of communication protocols designed and maintained by the Internet Society (ISOC). It was originally composed of two core protocols, TCP and IP, and later gradually evolved into a multi-layered, open protocol system.

The main features of the TCP/IP protocol suite include:

Open and free, anyone can use it without paying patent fees

Independent of computer hardware and operating system, universal and portable

Layered design, each layer is relatively independent and has clear responsibilities, easy to develop and maintain

Supporting the interconnection of heterogeneous networks is the key to realizing the Internet (Held, 2001)

Table 2 lists some core protocols in the TCP/IP protocol suite and their functions.

Table 2: TCP/IP core protocols and functions

protocol	Function
IP	Connectionless packet transfer service
TCP	Connection-oriented reliable byte stream transmission
UDP	Connectionless unreliable datagram transmission
ICMP	Internet Control Message Protocol, used for error reporting
IGMP	Internet Group Management Protocol for multicast
ARP	Address Resolution Protocol, which resolves IP addresses into physical addresses
DHCP	Dynamic Host Configuration Protocol, automatically assigning IP addresses to hosts
DNS	Domain Name System, responsible for resolving domain names to IP addresses

The organic combination of these protocols constitutes a reliable, flexible and scalable network communication infrastructure.

System Architecture Design Concept

The design of the TCP/IP protocol system follows some forward-looking concepts and principles, which laid the foundation for its core position in the Internet in the future.

(1) Layered architecture: The entire protocol system is divided into different layers, each layer is responsible for different functions, the interface is clear, and it is easy to deploy and expand. This makes TCP/IP highly modular and open.

(2) End-to-end principle: Core functions such as reliable transmission and flow control should be implemented at the edge of the network as much as possible to keep the network core as simple as possible and improve overall flexibility (Saltzer et al., 1984).

(3) Connectionless packet switching: The IP protocol is based on connectionless packet switching, and routing selection also uses stateless forwarding, which reduces network complexity.

(4) Unified addressing mechanism: IP addresses uniformly identify all hosts on the Internet, making seamless interconnection of heterogeneous networks possible.

(5) Best Effort Service: The network makes its best effort to deliver data packets without guaranteeing the quality of service, which makes the network core structure simple and the deployment flexible (Panwar et al., 1988).

Figure 2 intuitively depicts the hierarchical architecture of the entire TCP/IP protocol family.

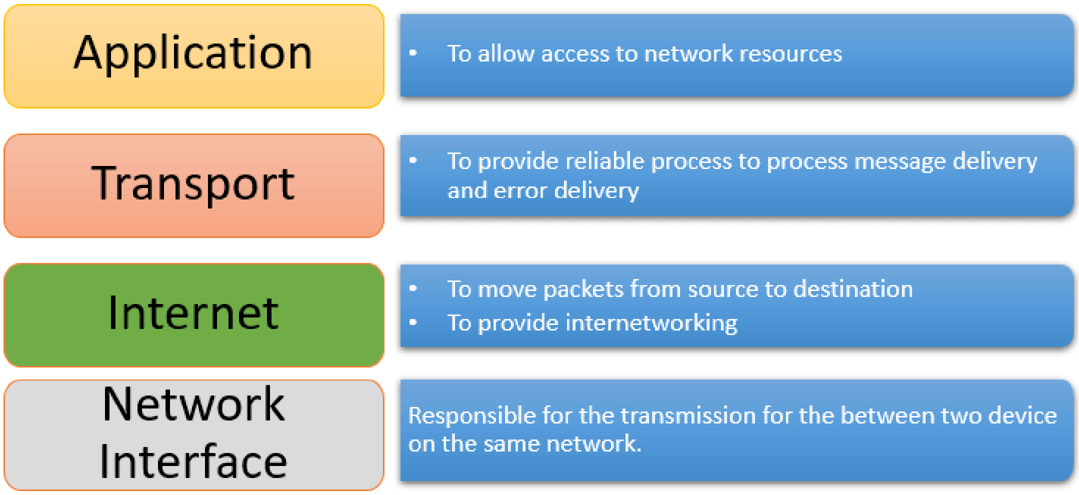


Figure 2: TCP/IP protocol family layered architecture

This modular and layered design makes the TCP/IP protocol family highly adaptable and extensible, thus promoting the rapid development of the Internet. In 1995, after the Internet was officially commercialized, its number of users showed explosive growth, but the TCP/IP architecture was able to cope with it calmly. According to statistics, by the end of 2022, global IP traffic has reached 3.41ZB (10^21 bytes), and TCP/IP is still the core foundation of the Internet backbone network (Cisco, 2023).

In short, the TCP/IP protocol architecture inherits the open and distributed concept of ARPANET, and makes innovations in layered design, connectionless switching, and end-to-end principles. This innovative design not only showed strong adaptability in the early stages of the Internet, but also has profound guiding significance for today's Internet technology.

Internet Architecture and Layered Model

With the popularization of TCP/IP protocol system, the Internet has gradually developed from the initial scientific research and experimental network into a global public network infrastructure. In order to meet the growing scale demand, a new layered network architecture concept came into being.

The rise and demand of the Internet

In the late 1980s, as countries around the world began to widely access the Internet, network traffic and the number of users showed explosive growth. According to statistics, between 1987 and 1992, the number of Internet hosts increased from more than 28,000 to about 1 million, with an average annual growth rate of 94.6% (Kleinrock, 2010). This rapid development soon highlighted the shortcomings of early network architectures such as ARPANET/NSFNET:

Poor scalability, network management and protocol configuration complexity grows exponentially with scale

Lack of unified service quality and security guarantee mechanism

There are obstacles to seamless interconnection of heterogeneous networks

The application layer lacks a universal service framework, and applications need to be developed from scratch (Huston, 2000)

Therefore, a new network architecture model is urgently needed to standardize and coordinate the deployment and development of the Internet.

TCP/IP layered model and its advantages and disadvantages analysis

To meet the above requirements, researchers proposed the famous TCP/IP layered network architecture model, as shown in Figure 3.

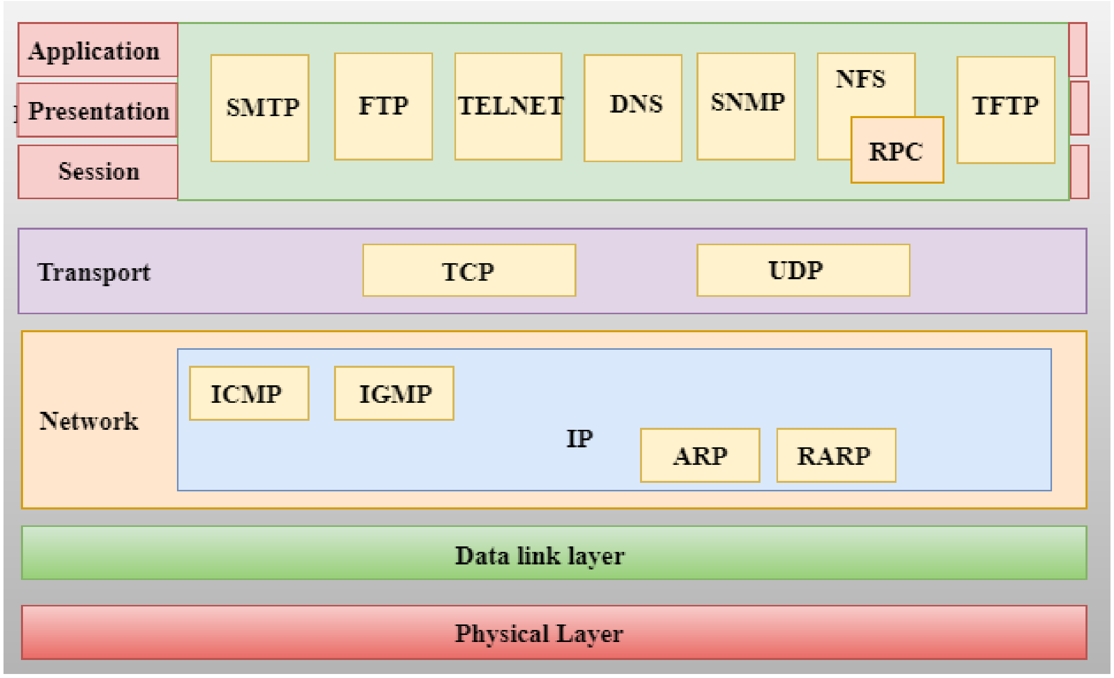


Figure 3: TCP/IP reference model

The model divides network communication into four abstract levels, each responsible for different functions:

Application layer: provides general interfaces and service support for specific network applications

Transport layer: implements end-to-end data transmission, such as TCP reliable transmission, UDP unreliable transmission, etc.

Network layer: responsible for the routing and forwarding of data packets, the most famous protocol is IP

Link layer: handles data transmission between nodes. The implementation of wired links and wireless links is different.

The design ideas of this layered network architecture model are mainly:

Reduce system complexity and simplify design and implementation through layering and modularization

Define clear inter-layer interfaces to achieve standardization and generalization within the protocol stack

Enhanced scalability, a certain layer of the network can develop independently without affecting other parts

The network and application are decoupled, so that applications can focus on service development (Dordal, 2021)

This unprecedented architecture model has laid a solid foundation for the smooth integration of heterogeneous networks and the large-scale development of the Internet.To this day, the TCP/IP layered model is still the guiding framework for the development of Internet technology.

However, this model also has some inherent limitations:

The layer division is not detailed enough, and many protocols work across layers

The interaction between layers is too strict and less flexible

Insufficient support for emerging network scenarios (such as the Internet of Things, content distribution, etc.)

Network and application decoupling may cause performance overhead (Al-Somaidee et al., 2021)

Therefore, under the new technological development trend, the traditional layered model needs to be further optimized and improved to better adapt to the needs of future Internet architecture.

Internet Protocol Evolution

Under the guidance of the TCP/IP layered architecture, the core Internet protocols and services are also evolving and developing. Here are some important protocol updates and extensions:

IPv6: A new generation of Internet protocol introduced to solve the problem of IPv4 address resource exhaustion, providing a larger address space and improved functions

MPLS: Multi-Protocol Label Switching, a forwarding technology that combines the advantages of Layer 2 and Layer 3, is widely used in service provider backbone networks.

LISP: A distinguishable routing system that aims to solve the problem of the Internet routing system becoming increasingly large and rigid.

QUIC: A new transport layer protocol based on UDP, combining the advantages of TCP and TLS, and is expected to replace HTTP/2

The continuous evolution of the Internet has also spawned a series of innovative application layer protocols, such as the real-time communication protocol SIP, the instant communication protocol XMPP, the multimedia streaming protocol RTP/RTCP, etc.

In general, although the Internet architecture has developed rapidly under the guidance of the layered model, it has also exposed some shortcomings and limitations, and urgently needs further optimization and innovation. This leaves room for the conception and experimentation of the next generation Internet architecture (Kleinrock, 2010) .

Exploration of the Next Generation Internet Architecture

As the Internet continues to expand, the inherent defects of the TCP/IP layered architecture have gradually emerged, posing new challenges to network performance, security, scalability, etc. In order to meet these challenges, researchers have proposed a variety of innovative next-generation Internet architecture concepts, hoping to reshape the development direction of network infrastructure (Jacobson et al., 2009) .

Active Network Architecture

Active Networks is a forward-looking network architecture concept proposed in the late 1990s. It attempts to break the rigid mode of "single-conditioning packet forwarding" in existing networks and endow the network with stronger programming capabilities and intelligence.

The core idea of active network architecture is to allow data packets to carry executable code, so that intermediate nodes can dynamically adjust packet processing behavior according to code instructions. This "programmable network" is expected to greatly enhance the flexibility and innovation potential of the network (Christin et al., 2020). Figure 4 shows the basic working principle of active network.

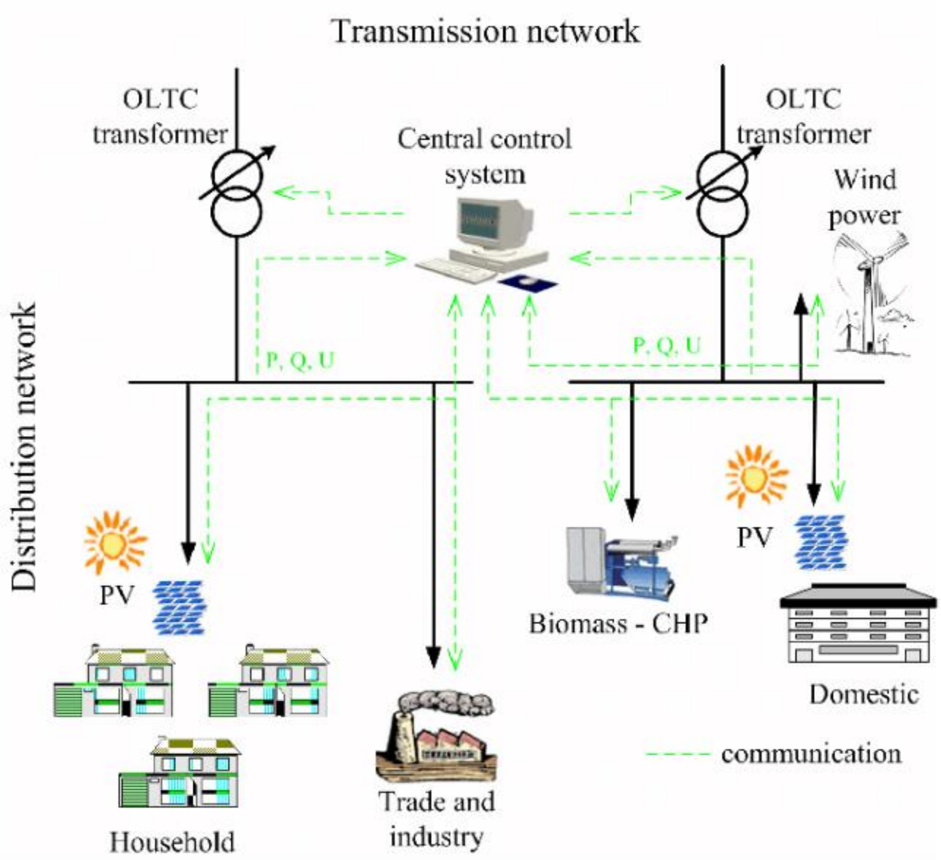


Figure 4: Active network diagram

In an active network, data packets sent by hosts can carry small programs that are executed and updated on the active nodes they pass through to implement customized packet processing behaviors. At the same time, traditional nodes still forward data packets in a standard way.

The active network architecture is designed to solve the following pain points:

Allows for innovation at the network layer rather than passively relying on a layered architecture model.

It can support more network services and applications and enhance the adaptability of the network.

Decentralize intelligence and control capabilities to network devices to reduce the pressure on the backbone network (Yin et al., 2022).

It can optimize network performance, such as realizing on-demand network services and active congestion control.

It helps to simplify the layered architecture and break through the insurmountable boundaries of each layer (Campbell et al., 1999).

However, active networks also face some major challenges and controversies:

Security and reliability issues: Allowing arbitrary code to execute on the network poses a huge risk.

Performance and overhead issues: Frequent code execution and network status checks may result in performance degradation.

Difficult to deploy: Existing infrastructure equipment needs to be updated on a large scale.

Lack of unified standards and control framework makes development and management complex.

Nevertheless, the concept of "programmable and intelligent network" embodied in the active network architecture has far-reaching influence and provided exploration ideas for emerging architectures such as software-defined networks.

Content-centric Network Architecture

In the late 1990s, due to the increasing diversification of network applications, Internet traffic began to show a high degree of asymmetry. A large amount of traffic came from the content distribution of a few popular websites, and the existing host-host communication model could no longer efficiently meet the needs of "multiple discovery requests, one-way transmission".

In this context, the Content-Centric Networking (CCN) architecture came into being. It changes the core orientation of the network from "host-centric" to "content-centric", hoping to serve the growing content distribution scenarios more efficiently (Jacobson et al., 2009).

The key ideas of the content-centric network architecture are:

Make content, not host, the core abstraction for network communication

Stakeholders obtain data by content naming, not host address

Network nodes can cache the content they pass through to avoid repeated retrieval

Content can be moved securely across the network without relying on end-to-end communication between hosts

Figure 5 illustrates the workflow of the CCN architecture when handling content distribution:

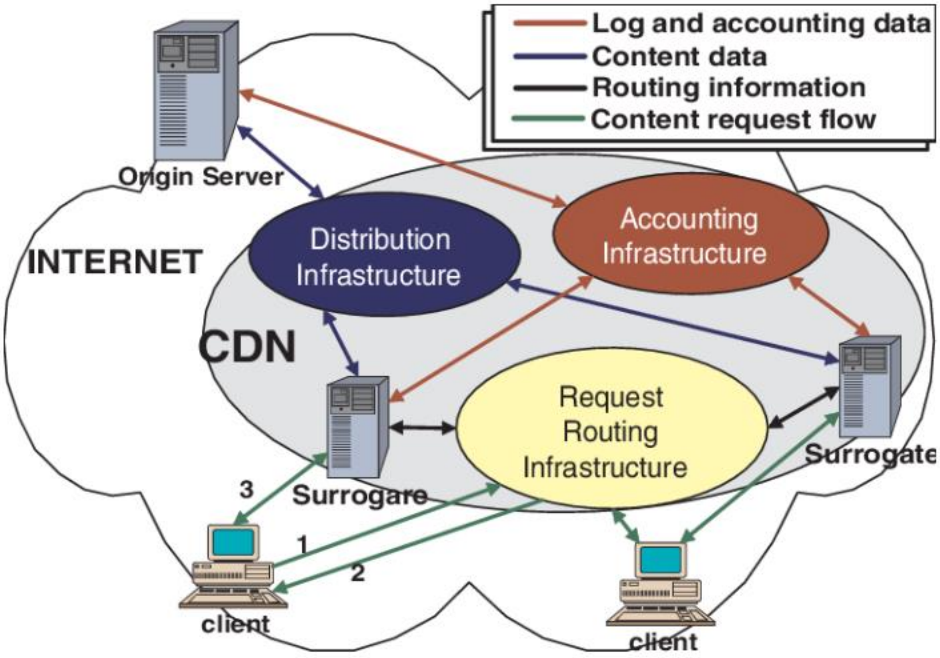


Figure 5: Schematic diagram of content distribution processing in a content-centric network

The CCN architecture usually adopts the following mechanisms in its implementation:

Use a unified content naming system, such as a hierarchical naming structure

Uses two basic message types: Interest (request) and Data (content)

Support content caching and automatic retransmission

Use stateless ring routing, not dependent on host address

Security mechanisms such as digital signatures are introduced to ensure the credibility of content

Compared with the traditional host-to-host TCP/IP model, the CCN architecture has obvious advantages in supporting content distribution scenarios, such as efficient use of network cache, no need to establish connections in advance, using multiple paths to obtain content in parallel, and improving network utilization (Xylomenos et al., 2014).

However, CCN also faces some challenges:

Memory cache management issues: How to deal with effective cache strategies and content updates?

Limited impact: only for content distribution scenarios, insufficient support for other types of applications

What are the specific mechanisms for a smooth transition to existing networks? How will it work with existing protocols?

Lack of commercial practice, still mainly in the academic research stage

Although the deployment of CCN requires a fundamental reconstruction of the current network, it provides a feasible example for building a new data-oriented network architecture. Many subsequent content distribution network technologies have borrowed the innovative ideas of CCN, such as content delivery networks (CDNs) and information center networks (ICN) (Naughton, 2016) .

Network architecture changes brought about by SDN and NFV

In recent years, the rise of software-defined networking (SDN) and network function virtualization (NFV) technologies is driving a gradual but profound change in network architecture. These emerging architectural models aim to improve the flexibility and automation of network operations and reshape the way network infrastructure is deployed and operated (Abbate, 2000) .

Software Defined Network (SDN) Concept

SDN is a new network architecture model that separates the data plane from the control plane. Its core idea is:

Centralize the control plane of network devices into a logical central controller

The controller manages and configures network behavior programmatically through open standard interfaces such as OpenFlow.

The data plane device is only responsible for simple data forwarding, and all complex control logic is undertaken by the controller.

Figure 6 shows the overall framework of the SDN architecture:

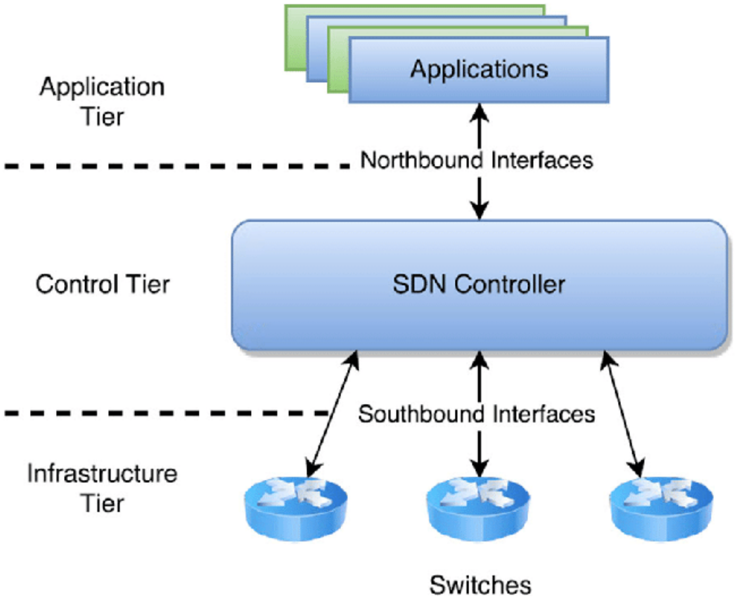


Figure 6: SDN architecture framework

The design goals of the SDN architecture include:

Greatly improve the automation of network configuration and management

Supports cloud, virtualized and programmatic network services

Promote innovation, network behavior can be quickly adjusted by software

Simplify the infrastructure, network devices only need to implement simple forwarding functions

Reduce capital and operating costs, and centralize management to be more efficient

Traditional networks face pain points such as increasingly complex network services, frequent changes, and closed monopolies. SDN automates network configuration and orchestration through software and centralized control, thereby improving operational efficiency and change agility (Donahoo & Calvert, 2009) .

But SDN also has some challenges that deserve attention:

Controller performance and reliability: Serves as the control center of the entire network

Communication overhead between the control plane and the data plane

Compatibility and interoperability: a transition mechanism to coexist with existing network architecture?

Lack of a unified vendor-neutral management framework

Network Function Virtualization (NFV) Concept

Unlike SDN, which separates the control plane and the data plane, the concept of NFV is to virtualize traditional dedicated network functions such as routers, firewalls, DTN, etc. through general hardware such as commercial servers.

The basic idea of NFV is:

Use standard IT virtualization technology to build virtual machines (VMs) or containers on industrial servers

Deploy network function software such as routing, forwarding or VPN components through software packages

A single physical server can run multiple virtualized network functions (VNFs) through multiple VMs

With the help of NFV orchestration management system, VNFs are dynamically combined to provide end-to-end network services.

Figure 7 shows the virtualized network function architecture based on NFV technology:

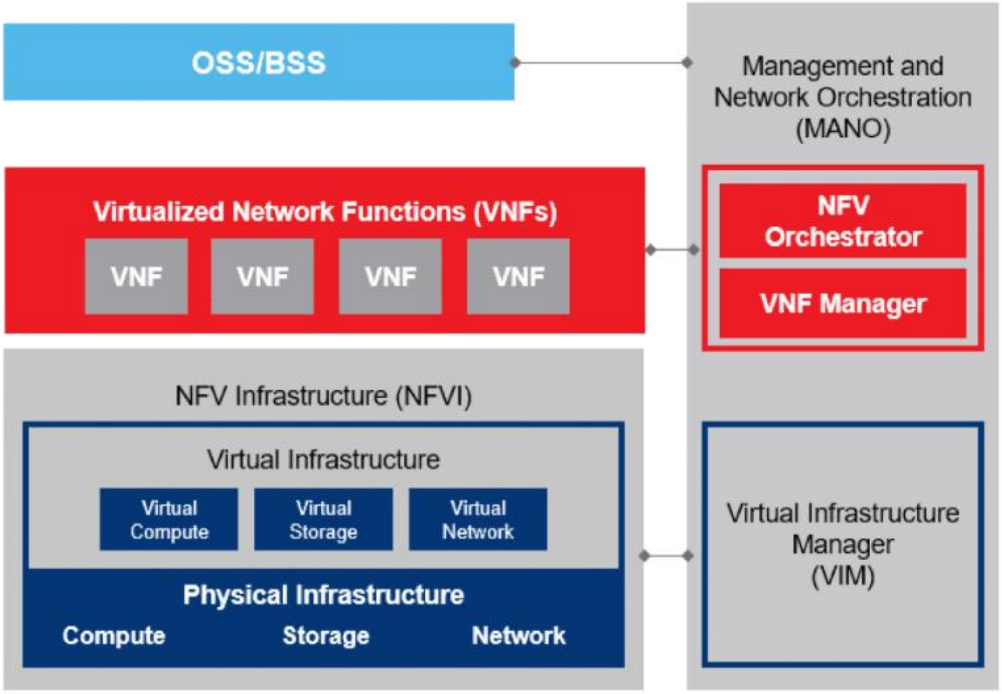


Figure 7: NFV-based virtualized network function architecture

The main benefits of NFV include:

Reduce network service deployment costs: no longer need dedicated hardware equipment

Shorten the time to market for new services: New features can be quickly deployed through software

Improve resource utilization efficiency: hardware can flexibly allocate resources on demand

Promote innovation, NFV architecture is open and programmable (Bradai et al., 2015)

NFV has laid the foundation for the shift of network functions to software and virtualization, bringing a huge impact to traditional dedicated hardware equipment suppliers and also giving cloud computing infrastructure network wings.

Compared with SDN technology, NFV focuses more on the virtualization of network functions. The two can complement each other to achieve end-to-end network service orchestration. Therefore, many operators advocate the integrated deployment of SDN and NFV to maximize benefits.

However, NFV also faces some challenges in application:

VNF performance and its decoupling from hardware

Virtualization Overhead and Resource Management

Complexity of multi-VNF collaborative orchestration

Interoperability with existing legacy networks

In general, SDN and NFV have led the trend of network infrastructure towards software, automation and virtualization, indicating that the future network architecture will be more open and programmable, supporting cloud and on-demand deployment. The successful deployment and development of the two will profoundly reshape the network operation model.

Impact of emerging network paradigms on network architecture

With the rise of emerging network paradigms such as cloud computing, the Internet of Things, and edge computing, traditional network architecture is facing unprecedented challenges. These new paradigms have put forward higher requirements on network capabilities and service quality, prompting network architecture to develop in a more flexible, intelligent, and distributed direction (Sim, 2020) .

Cloud computing promotes network architecture

Cloud computing provides IT resources on demand as a service through the network. Its business model and operation logic put forward new requirements for network infrastructure:

Highly flexible and dynamic network: supports on-demand resource scheduling, automatic expansion and reduction, etc.

End-to-end resource orchestration capability: Ability to seamlessly allocate computing, storage, and network resources across data centers.

Multi-tenant network isolation: Meet the security and QoS requirements of different users and applications.

WAN optimization and acceleration: Solve problems such as high latency and bandwidth limitations caused by cross-domain deployment of cloud resources.

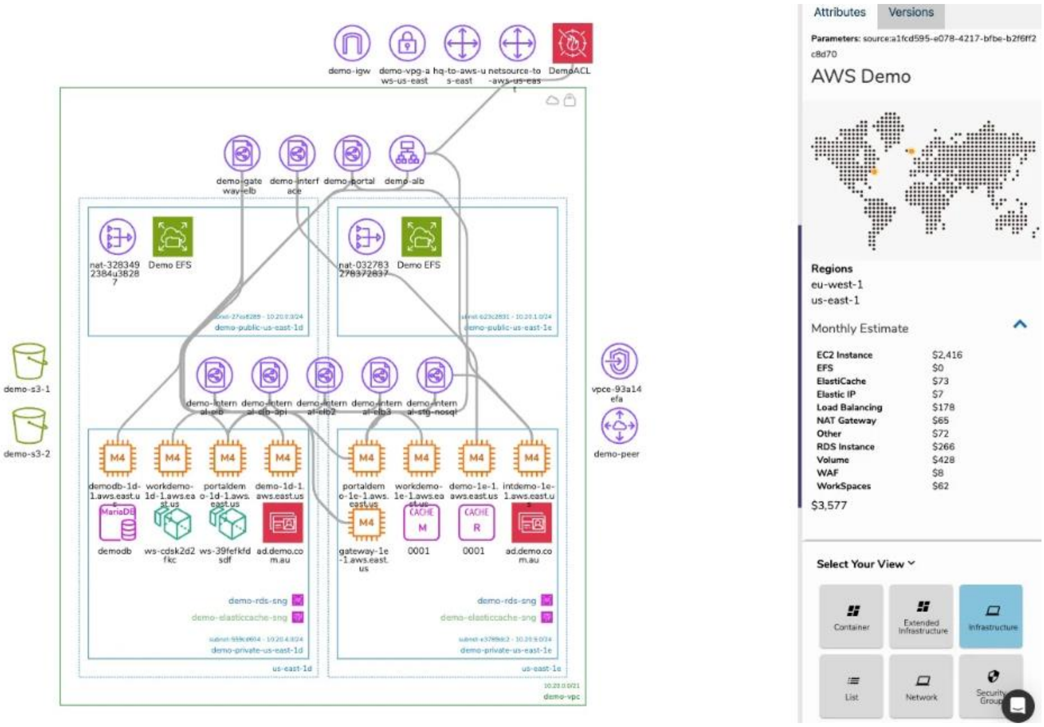
To meet the above requirements, cloud data center networks have adopted new architectures such as virtual overlay networks and software-defined networks:

Virtual overlay networks achieve dynamic resource orchestration, tenant isolation, and service programming through virtualization mechanisms.

SDN improves configuration automation, programmability, and centralized resource management and control.

In addition, cloud service providers have also extensively adopted virtualization technologies such as VXLAN and NVGRE, as well as WAN optimization solutions such as MPLS VPN and EVN to build a flexible and scalable cloud network architecture.

Taking Amazon AWS as an example, its cloud network architecture is shown in Figure 8:



Parameters: source:a1fcd595-e078-4217-bfbe-b2f6ff2c8d70

AWS Demo

Regions
eu-west-1
us-east-1

Monthly Estimate

EC2 Instance	$2,416
EFS	$0
ElastiCache	$73
Elastic IP	$7
Load Balancing	$178
NAT Gateway	$65
Other	$72
RDS Instance	$266
Volume	$428
WAF	$8
WorkSpaces	$62

$3,577

Figure 8: Amazon AWS cloud network architecture diagram

AWS achieves logical isolation through virtual private cloud (VPC), and provides flexible and programmable resource orchestration, connection and security management mechanisms to support large-scale cloud service deployment. This design concept has a profound impact on network architecture.

New Requirements for Network Architecture from Edge Computing and Fog Computing

Compared with cloud computing, which deploys resources centrally in data centers, edge computing and fog computing emphasize sinking computing and storage resources to the edge of the network, close to mobile terminals and IoT devices, thereby reducing latency and network pressure (Huston, 2001) .

This emerging computing paradigm places the following key demands on network architecture:

Distributed computing platform: realizing collaborative orchestration of computing and network

Lightweight and efficient transmission: Supporting large-scale IoT device interconnection

Network intelligent routing: Optimize paths to reduce end-to-end latency

Secure isolation and mobility support: ensuring seamless connections and services

To meet the above needs, some innovative network architectures and technologies have gradually emerged:

(1) Intelligent edge network architecture This architecture introduces network function virtualization (NFV) and software defined network (SDN) technologies into edge nodes, making the edge network flexible and intelligent. For example, the Fog Networking architecture uses SDN and NFV to achieve collaborative orchestration of computing and networks, and supports on-demand deployment of network services. Figure 9 shows the basic architecture of Fog Networking:

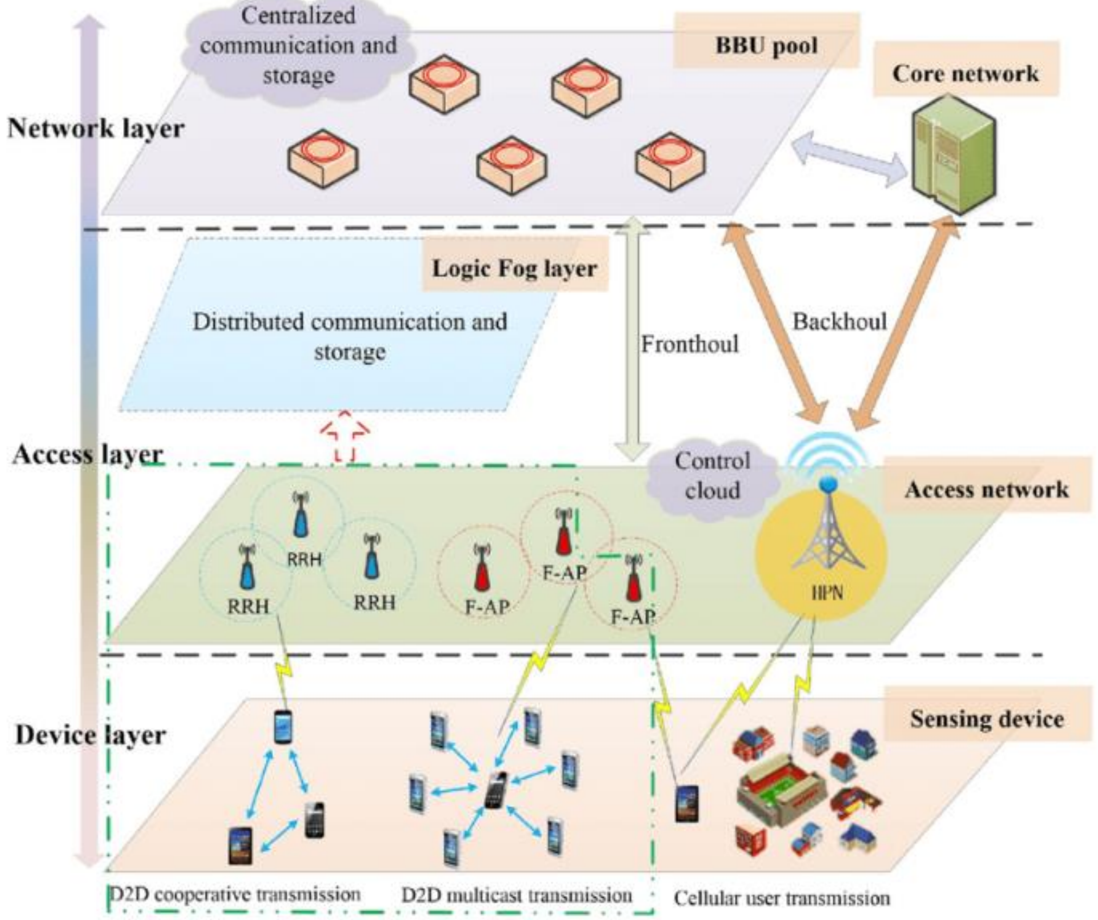


Figure 9: Fog Networking edge network architecture

(2) Low-power wide area network (LPWAN) technology LPWAN focuses on the wide-area interconnection of low-power IoT devices. Its main features include ultra-long battery life, high connection density, and low cost. The current mainstream LPWAN technologies include LoRaWAN, NB-IoT, and Sigfox. These technologies achieve low-power wide-area transmission through self-organizing topology and special modulation and coding methods.
(3) Software Defined Radio (SDR) and Reconfigurable Radio (CR) SDR and CR are committed to breaking through the limitations of proprietary hardware wireless devices and providing flexible and reconfigurable wireless access capabilities through software-defined or reconfigurable wireless protocol stacks, Air interfaces, etc. This openness and flexibility is conducive to protocol innovation in edge computing environments.
(4) Information-Centric Network (ICN) ICN inherits the concept of content-centric networking, takes content as the focus, and improves the efficiency of content distribution in edge environments through mechanisms such as name-based routing and caching. Named Data Networking (NDN), which is suitable for IoT and edge computing scenarios, is an example of ICN in edge environments.

In summary, with the increasing popularity of cloud-edge-end computing models, network architecture is also facing new demands for distributed, intelligent, efficient and low-latency interconnection. By adopting technical means such as software, virtualization, and wireless innovation, future networks will better meet the needs of distributed computing and achieve ubiquitous interconnection and collaborative orchestration.

Future network architecture development trends and challenges

With the continuous innovation of emerging technologies, network architecture is facing an unprecedented opportunity for change. The introduction of cutting-edge technologies such as artificial intelligence (AI) and blockchain will profoundly reshape the future of the network and give rise to a new architectural paradigm. At the same time, the network will also face more new challenges such as security and autonomy (Kleinrock, 2010) .

Application of Artificial Intelligence and Machine Learning in Networks

Artificial intelligence and machine learning technologies have great potential in the field of networking, and their potential applications mainly include:

(1) Intelligent network control and management uses machine learning algorithms to model and analyze network status data, which can realize intelligent network resource management, routing selection, traffic engineering and other functions based on environment perception, thereby improving the automation and optimization level of network operation and maintenance.

(2) Autonomous network systems Through machine learning and artificial intelligence technologies, network systems are expected to achieve advanced intelligence such as autonomous configuration, autonomous optimization, and autonomous repair, thereby reducing operation and maintenance costs and improving the automation and autonomy of the network.

(3) Cognitive network architecture Cognitive networks use machine learning to build models that understand user needs and environmental changes, and optimize the configuration of network resources and services. This cognitive architecture is expected to enable the network to respond to changes more proactively and provide a better service quality experience.

(4) Intelligent machine learning for security defense can be used to detect security threats such as abnormal network behavior and intrusion attempts, and to respond and defend effectively. This will greatly improve the initiative and accuracy of network security management.

Figure 10 shows an example of an AI-based cognitive network architecture.

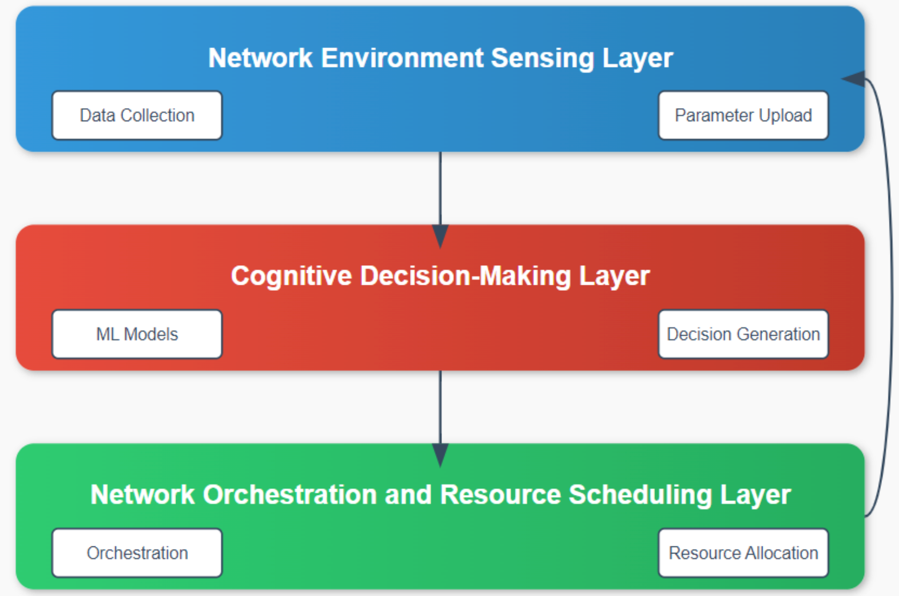


Figure 10: Example of AI-based cognitive network architecture

In this architecture, the network environment perception layer collects key network parameters and uploads them to the cognitive decision-making layer, which runs the machine learning model to generate optimization decisions and guides the network orchestration and resource scheduling of the lower layer to form an autonomous closed loop.

Although the combination of AI and the Internet is promising, it also faces some major challenges:

Standardized data acquisition and processing mechanisms

AI system performance, stability and reliability

Huge computing power and storage requirements

How to prevent AI systems from being attacked or abused

Privacy and ethical risk avoidance

Therefore, the effective integration of AI and the Internet still requires efforts such as theoretical innovation, technological breakthroughs and comprehensive standardization.

The potential of blockchain technology in network architecture

Blockchain technology relies on cryptography to ensure the consistency and immutability of distributed ledgers. Its unique advantages such as decentralization, security and reliability make it also have great application space in network architecture. The main potential includes:

(1) Distributed network architecture based on blockchain Blockchain can build a new decentralized network architecture, where each node is a routing core and no centralized control entity is required. Each node collaborates through the blockchain P2P network to form a network system with stress resistance.

(2) Autonomous management of network resources With the help of the smart contract function of blockchain, network resources such as bandwidth, computing power, storage space, etc. can be described as digital assets, and automated allocation and on-demand use can be achieved. This decentralized resource autonomy mechanism helps improve resource utilization efficiency.

(3) Network service authorization and billing Users can obtain network services through smart contracts. The relevant fees and rules are agreed upon in advance in the contract, thus realizing an automated, auditable and traceable service authorization and billing process. This will simplify the billing management of network operators.

(4) Network security and trust transfer The immutability of the blockchain distributed ledger can be used to maintain the identity and trust relationship of network entities through the network, forming a new authoritative authentication mechanism. On the other hand, the cryptographic principles of blockchain also provide new protection means for network security.

In view of the above potential application scenarios, both academia and industry have actively explored and proposed architectural concepts such as blockchain networks (BlockNetworks). The blockchain network architecture is shown in Figure 11:

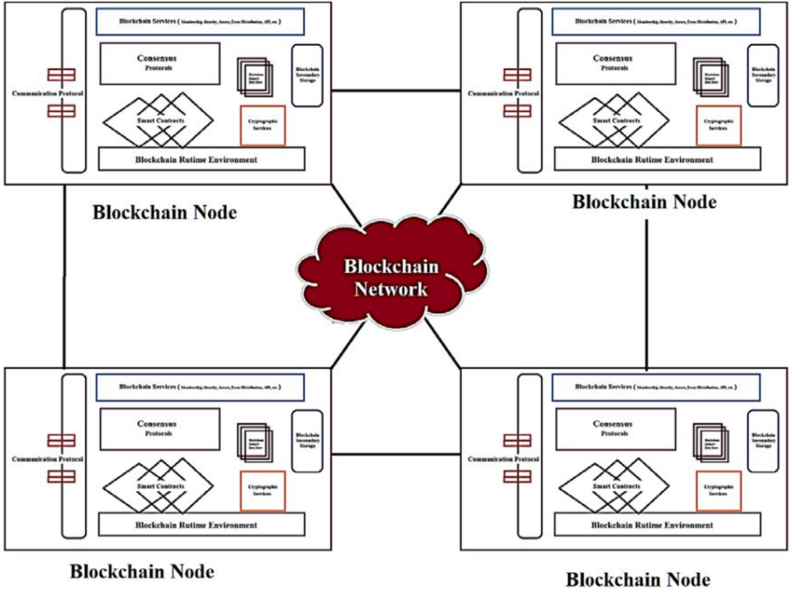


Figure 11: Blockchain network architecture diagram

In a blockchain network, each network node is both a router and a ledger recorder, without the need for any centralized management entity. Functions such as routing and resource management are achieved through distributed collaboration through consensus mechanisms and smart contracts (Kreutz et al., 2015) . Blockchain technology brings great potential to network architecture, but it also faces some challenges:

Performance and scalability issues of blockchain

Efficiency of consensus-reaching mechanisms

Computing power and storage requirements on the device side

Specific path for smooth transition and integration with existing networks

Lack of unified standards and best practices

Only by solving these key problems can blockchain technology truly play an important role in future network architecture.

Network Autonomy and Security Challenges

In addition to the impact of new technologies, future network architectures will also face some unprecedented security and autonomy challenges:

(1) Evolution of cyber threats and attack forms With the rise of new network applications such as the Internet of Things and the Internet of Vehicles, the attack surface will increase significantly. In addition, new technologies such as AI may also be abused to launch more intelligent and covert cyber attacks.

(2) The increasing complexity of network security management In a heterogeneous network environment, it is extremely challenging to achieve unified and efficient security management and access control. At the same time, real-time detection and analysis of large-scale network traffic is also a daunting task.
(3) Reliability of autonomous network systems As networks become increasingly autonomous and intelligent, the reliability and robustness of their behaviors and decisions will become of paramount importance. Any slight mistake may lead to catastrophic consequences.

(4) Network privacy and ethical risks The acquisition and application of massive amounts of privacy data brings huge risks of data abuse; AI algorithms may also have unfair phenomena such as racial and gender discrimination, which will become major ethical challenges in network architecture design.
(5) Lag of laws and regulations. Internet-related laws and regulations often fail to keep pace with the development of new technologies. The serious lag in management and regulatory measures may bring about a series of social and economic risks.

In the face of the above security and autonomy challenges, future network architectures need to take corresponding countermeasures in design:

Strengthen the overall consideration of security in the network system, implement the theory of trusted distributed systems, and adopt a safe and controllable design.

Establish a multi-level security protection mechanism, such as hardware root trust, software isolation, encryption authentication, etc., to achieve the depth and breadth of defense.

Strengthen the real-time detection and online repair capabilities of abnormal behaviors, and improve the system's self-repair and self-immunity levels.

Establish a strict artificial intelligence governance system to ensure the fairness, transparency and explainability of algorithms, and prevent algorithmic ethical risks.

Establish corresponding laws, regulations, systems and standards to clarify the norms and boundaries of network behavior and ensure a balance between technological development and social needs.

In general, the development trend of future network architecture is to evolve towards intelligence, autonomy, and distribution. Emerging cutting-edge technologies such as artificial intelligence and blockchain will have a profound impact on network architecture. At the same time, the network will also face unprecedented security and autonomy challenges. Therefore, the future network architecture not only needs to have excellent performance and functions, but also needs a high degree of security, reliability, and controllability, and comply with the bottom line of moral ethics. Only in this way can the innovation of network architecture truly benefit society and promote the sustainable development of human civilization (Naughton, 2016) .

Summary and Outlook

This article systematically reviews and analyzes the evolution of computer network architecture, and explains its internal development logic and deep-seated driving force. We analyze the trajectory of the continuous innovation of network architecture step by step, from the initial packet switching concept and ARPANET, to the establishment of the TCP/IP protocol architecture, and then to the formation of the Internet layered architecture model (Naughton, 2016) .

The paper then explores the concept of next-generation Internet architectures such as active networks and content-centric networks, and reviews their motivations and limitations in responding to new requirements. We also focus on emerging architectural models such as software-defined networking (SDN) and network function virtualization (NFV) that are reshaping the way network infrastructure is deployed and operated.

In addition, the paper also analyzes the new requirements for network architecture from emerging network paradigms such as cloud computing and edge computing, as well as the role of some innovative technologies such as LPWAN and ICN in meeting these requirements. Finally, we prospectively look forward to the application prospects of cutting-edge technologies such as artificial intelligence and blockchain in network architecture, and point out major challenges that must be addressed in the future, such as network autonomy and security.

In summary, the development of network architecture contains the inherent logic of continuous innovation and reform. Every technological breakthrough and paradigm shift is a pursuit and response to higher efficiency and richer needs. From packet switching to TCP/IP, and then to SDN/NFV, network architecture has gradually evolved towards software, intelligence and virtualization, showing increasingly advanced and open characteristics.

In the future, the deep integration of cutting-edge technologies such as artificial intelligence and blockchain will surely bring new revolutionary changes to network architecture. At the same time, issues such as network security, reliability, and autonomy will become increasingly prominent. Therefore, the innovation of network architecture requires both the promotion of technological innovation and the norms and constraints of ethics and rule of law, so as to truly benefit society and serve the sustainable development of human civilization.

Future Research Directions

Based on the above summary, the author believes that the development of future network architecture should at least focus on the following directions:

Innovations in the integration of artificial intelligence and the network include intelligent network management, cognitive network systems, AI security defense, etc., which require in-depth research in algorithms, system architecture, standards and specifications.

Distributed Autonomous System Architecture Decentralized technologies such as blockchain have brought new ideas for building distributed autonomous system architectures that do not require central management, and their potential is worth exploring in depth.

Research on network autonomy and reliability assurance mechanisms is a major challenge in ensuring the security, robustness and controllability of network decisions and behaviors as the network becomes increasingly intelligent.

Unified security protection system in heterogeneous network environments Heterogeneous network environments such as the Internet of Things and edge computing have brought new challenges to network security protection, and it is necessary to establish an effective unified protection mechanism.

Network privacy protection and algorithm fairness research: Personal privacy protection issues in the big data environment, as well as potential biases in artificial intelligence algorithms, all need to be paid attention to and avoided.

The organic integration of network technology and social ethics and rule of law strengthens the organic combination of technological innovation and social needs, establishes corresponding laws, regulations and ethical standards, and makes the development of new technologies follow rules.

The evolution of network architecture is an endless process, and every innovation will trigger new demands and challenges. Only by maintaining continuous efforts and innovative spirit can network architecture keep pace with the times and provide a more solid foundation for the development of human society.

CONCLUSION

Looking back at the development of network architecture over the past 100 years, we have seen the power of technological innovation to foster change. The idea of packet switching pioneered the modern network, the TCP/IP architecture laid the foundation for the Internet, and software-defined networking will drive the next leap in network architecture.

In the future, the addition of disruptive technologies such as artificial intelligence and blockchain will surely reshape the face of network architecture. But at the same time, new challenges such as network autonomy and security will also emerge. Therefore, the future network architecture should not stop at the technical level, but should focus on the organic integration with social development and seek a balance between efficiency, innovation and security.

Only in this way can the development of network architecture keep pace with the times and continue to give wings to human civilization and social progress. Let us look forward to and work hard to create a bright future of network architecture innovation!

REFERENCES

Abbate, J. (2000). Inventing the internet . MIT press.

Abbasi, AA, Abbasi, A., Shamshirband, S., Chronopoulos, AT, Persico, V., & Pescapè, A. (2019). Software-defined cloud computing: A systematic review on latest trends and developments. IEEE Access , 7 , 93294-93314.

Sim, K. M. (2020). Intelligent resource management in intercloud, fog, and edge: Tutorial and new directions. IEEE Transactions on Services Computing, 15(2), 1157-1174.

Campbell, A. T., De Meer, H. G., Kounavis, M. E., Miki, K., Vicente, J. B., & Villela, D. (1999). A survey of programmable networks. ACM SIGCOMM Computer Communication Review, 29(2), 7-23.

Ahmad, I., Namal, S., Ylianttila, M., & Gurtov, A. (2015, July). Towards software defined cognitive networking. In 2015 7th international conference on new technologies, mobility and security (NTMS) (pp. 1-5). IEEE.

Cisco Systems. (2020). Cisco Annual Internet Report (2018–2023) White Paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Donahoo, M. J., & Calvert, K. L. (2009). TCP/IP sockets in C: practical guide for programmers. Morgan Kaufmann.

Huston, G. (2001). Analyzing the Internet's BGP routing table. The Internet Protocol Journal, 4(1), 2-15.

International Telecommunication Union (ITU). (2022). Measuring digital development Facts and figures 2022. https://www.itu.int/itu-d/reports/statistics/facts-figures-2022/

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., & Braynard, R. L. (2009). Networking named content. Proceedings of the 5th international conference on Emerging networking experiments and technologies, 1-12. https://doi.org/10.1145/1658939.1658941

Kleinrock, L. (2010). An early history of the internet [History of Communications]. IEEE Communications Magazine, 48(8), 26-36.https://doi.org/10.1109/MCOM.2010.5534584

Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14-76. https://doi.org/10.1109/JPROC.2014.2371999

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. Journal of Cyber Policy, 1(1), 5-28. https://doi.org/10.1080/23738871.2016.1157619

Panwar, S. S., Towsley, D., & Wolf, J. K. (1988). Optimal scheduling policies for a class of queues with customer deadlines to the beginning of service. Journal of the ACM (JACM), 35(4), 832-844.

Saltzer, J. H., Reed, D. P., & Clark, D. D. (1984). End-to-end arguments in system design. ACM Transactions on Computer Systems (TOCS), 2(4), 277-288. https://doi.org/10.1145/357401.357402

Xylomenos, G., Ververidis, C. N., Siris, V. A., Fotiou, N., Tsilopoulos, C., Vasilakos, X., ... & Polyzos, G. C. (2014). A survey of information-centric networking research. IEEE Communications Surveys & Tutorials, 16(2), 1024-1049. https://doi.org/10.1109/SURV.2013.070813.00063

Chataut, R., & Akl, R. (2020). Massive MIMO systems for 5G and beyond networks—overview, recent trends, challenges, and future research direction. Sensors, 20(10), 2753.

Zimmermann, H. (1980). OSI reference model--The ISO model of architecture for open systems interconnection. IEEE Transactions on communications, 28(4), 425-432. https://doi.org/10.1109/TCOM.1980.1094702

Ahad, A., Tahir, M., & Yau, K. L. A. (2019). 5G-based smart healthcare network: architecture, taxonomy, challenges and future research directions. IEEE access, 7, 100747-100762.