SDN and NFV Overview



Huawei Technologies Co., Ltd.

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  **Trademarks and Permissions**  HW_POS_RBG_Vertical-150ppi.png and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com/> |

**Huawei Certification System**

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.



Contents

[1 SDN and NFV Overview 1](#_Toc59717207)

[1.1 Foreword 1](#_Toc59717208)

[1.2 Objectives 1](#_Toc59717209)

[1.3 SDN Overview 1](#_Toc59717210)

[1.3.1 Evolution of the Computer Era 1](#_Toc59717211)

[1.3.2 Network Industry Development: Implications from the IT Industry 2](#_Toc59717212)

[1.3.3 Current Situation of the Network Industry: Typical IP Network - Distributed Network 3](#_Toc59717213)

[1.3.4 Thinking in the Network Field: Problems Faced by Typical Networks 4](#_Toc59717214)

[1.3.5 Frequent Network Congestion 4](#_Toc59717215)

[1.3.6 Complex Network Technologies 5](#_Toc59717216)

[1.3.7 Difficulty in Locating and Analyzing Network Faults 5](#_Toc59717217)

[1.3.8 Slow Network Service Deployment 6](#_Toc59717218)

[1.3.9 SDN Origin 7](#_Toc59717219)

[1.3.10 Basic Concepts of OpenFlow 7](#_Toc59717220)

[1.3.11 Flow Table Overview 8](#_Toc59717221)

[1.3.12 Comparison between Forwarding Modes 9](#_Toc59717222)

[1.3.13 Essential Requirements of SDN 10](#_Toc59717223)

[1.3.14 SDN Network Architecture 10](#_Toc59717224)

[1.3.15 Huawei SDN Network Architecture 11](#_Toc59717225)

[1.3.16 Huawei SDN Solution - Integrating Management, Control, and Analysis to Build an Intent-Driven Network 12](#_Toc59717226)

[1.3.17 Introduction to iMaster NCE 12](#_Toc59717227)

[1.3.18 Huawei CloudFabric DCN Autonomous Driving Network Solution 13](#_Toc59717228)

[1.3.19 Huawei CloudCampus Autonomous Driving Network Solution 16](#_Toc59717229)

[1.4 NFV Overview 21](#_Toc59717230)

[1.4.1 NFV Background: Thinking from IT Industry Transformation 21](#_Toc59717231)

[1.4.2 Origin of NFV 22](#_Toc59717232)

[1.4.3 NFV Value 22](#_Toc59717233)

[1.4.4 Key NFV Technologies 23](#_Toc59717234)

[1.4.5 Introduction to the NFV Architecture 24](#_Toc59717235)

[1.4.6 Standard NFV Architecture 25](#_Toc59717236)

[1.4.7 Functional Modules of the NFV Architecture 26](#_Toc59717237)

[1.4.8 NFV Architecture Interfaces 26](#_Toc59717238)

[1.4.9 Huawei's NFV Solution 27](#_Toc59717239)

[1.5 FAQ 28](#_Toc59717240)

[1.6 Quiz 28](#_Toc59717241)

[1.7 Summary 29](#_Toc59717242)

# SDN and NFV Overview

## Foreword

The open ecosystem of the computing industry brings booming development of multiple fields, such as Commercial Off-the-Shelf (COTS), operating system, virtualization, middleware, cloud computing, and software applications. The network industry is also seeking transformation and development. Software Defined Networking (SDN) and Network Functions Virtualization (NFV) are mainly used.

This course aims to help engineers understand the development of SDN and NFV and introduce Huawei SDN and NFV solutions.

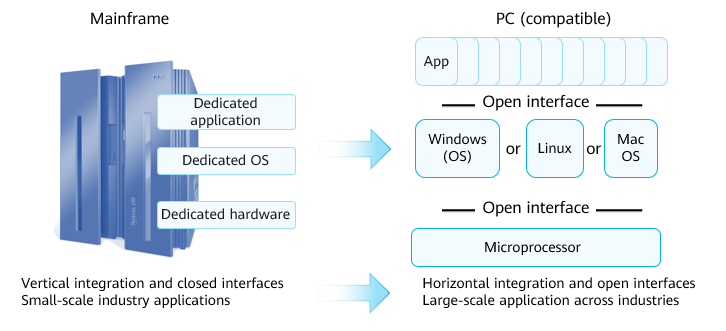
## Objectives

On completion of this course, you will be able to:

* Describe the development of SDN and NFV.
* Understand basic principles of OpenFlow.
* Understand Huawei SDN solution.
* Understand the standard NFV architecture.
* Understand Huawei NFV solution.

## SDN Overview

### Evolution of the Computer Era



Evolution of the Computer Era

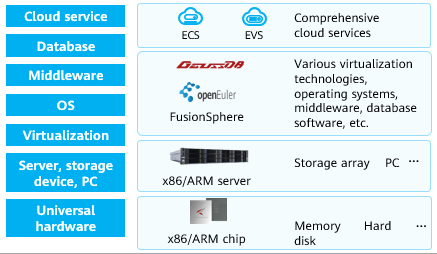
In 1964, IBM spent US$5 billion on developing IBM System/360 (S/360), which started the history of mainframes. Mainframes typically use the centralized architecture. The architecture features excellent I/O processing capability and is the most suitable for processing large-scale transaction data. Compared with PCs, mainframes have dedicated hardware, operating systems, and applications.

PCs have undergone multiple innovations from hardware, operating systems, to applications. Every innovation has brought about great changes and development. The following three factors support rapid innovation of the entire PC ecosystem:

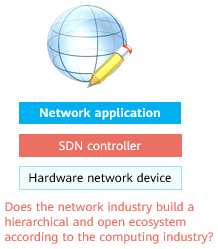
* Hardware substrate: The PC industry has adapted a simple and universal hardware base, x86 instruction set.
* Software-defined: The upper-layer applications and lower-layer basic software (OS and virtualization) are greatly innovated.
* Open-source: The flourishing development of Linux has verified the correctness of open source and bazaar model. Thousands of developers can quickly formulate standards to accelerate innovation.

### Network Industry Development: Implications from the IT Industry

The transformation of the IT industry has triggered the thinking of the network industry. The industry has proposed the SDN concept and has made attempts to put SDN into commercial use, aiming to make networks more open, flexible, and simple.



Computing Industry Openness Promotes Ecosystem Development

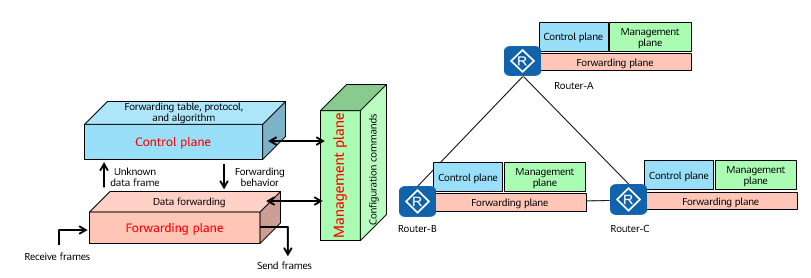


What about Network Industry Changes

### Current Situation of the Network Industry: Typical IP Network - Distributed Network

The typical IP network is a distributed network with peer-to-peer control. Each network device has independent forwarding, control, and management planes. The control plane of a network device exchanges packets of a routing protocol to generate an independent data plane to guide packet forwarding.

The advantage of a typical IP network is that network devices are decoupled from protocols, devices from different vendors are compatible with each other, and network convergence is ensured in fault scenarios.



Distributed Network

The switch is used as an example to describe the forwarding plane, control plane, and management plane.

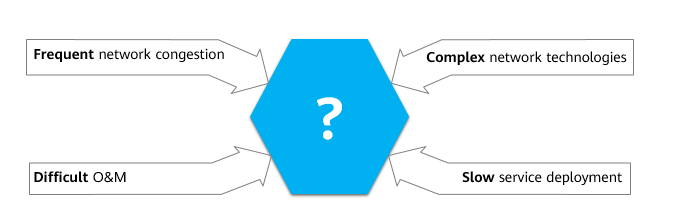
Forwarding plane: provides high-speed, non-blocking data channels for service switching between service modules. The basic task of a switch is to process and forward various types of data on its interfaces. Specific data processing and forwarding, such as Layer 2, Layer 3, ACL, QoS, multicast, and security protection, occur on the forwarding plane.

Control plane: provides functions such as protocol processing, service processing, route calculation, forwarding control, service scheduling, traffic statistics collection, and system security. The control plane of a switch is used to control and manage the running of all network protocols. The control plane provides various network information and forwarding query entries required for data processing and forwarding on the data plane.

Management plane: provides functions such as system monitoring, environment monitoring, log and alarm processing, system software loading, and system upgrade. The management plane of a switch provides network management personnel with Telnet, web, SSH, SNMP, and RMON to manage devices, and supports, parses, and executes the commands for setting network protocols. On the management plane, parameters related to various protocols on the control plane must be pre-configured, and the running of the control plane can be intervened if necessary.

Some Huawei series products are divided into the data plane, management plane, and monitoring plane.

### Thinking in the Network Field: Problems Faced by Typical Networks

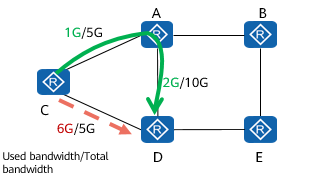


Problems Faced by Typical Networks

### Frequent Network Congestion

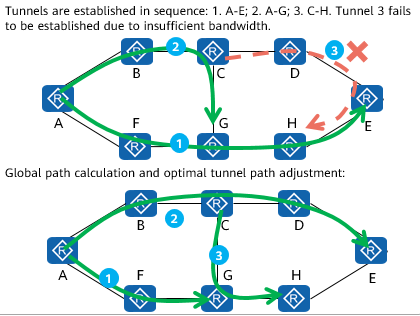
Problem and Solution of Bandwidth-based Route Selection：

* The network computes forwarding paths based on bandwidth. The link from router C to router D is the shortest forwarding path. The volume of service traffic from router C to router D exceeds the bandwidth, causing packet loss. Although other links are idle, the algorithm still selects the shortest path for forwarding. The optimal traffic forwarding path is C-A-D.



Problem and Solution of Bandwidth-based Route Selection

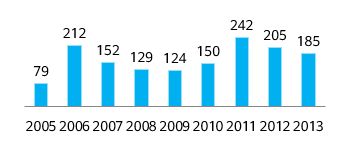
Problem and Solution of Tunnel Establishment Based on Fixed Sequence：



Problem and Solution of Tunnel Establishment Based on Fixed Sequence

### Complex Network Technologies

**Many network protocols:** Network technology experts need to learn many RFCs related to network devices. Understanding the RFCs takes a long time, and the number of RFCs is still increasing.



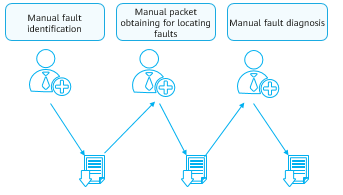
RFC increase trends

**Difficult network configuration:** To be familiar with devices of a specific vendor, you need to master tens of thousands of commands. Additionally, the number of commands is still increasing.

### Difficulty in Locating and Analyzing Network Faults

Difficult to Spot Faults

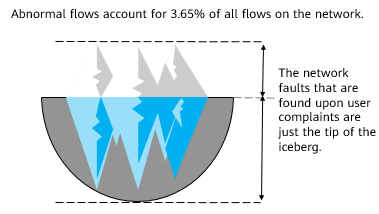
* Traditional O&M networks rely on manual fault identification, location, and diagnosis.
* More than 85% of network faults are found only after service complaints. Problems cannot be proactively identified or analyzed.



Difficult to Spot Faults

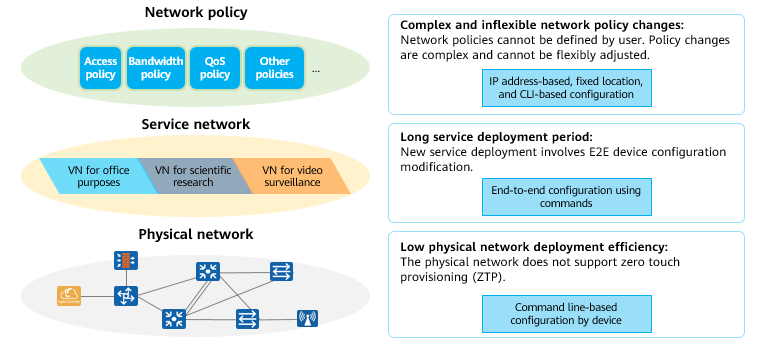
Difficult to Locate Faults

* Traditional O&M only monitors device indicators. Some indicators are normal, but user experience is poor. There is no correlated analysis of users and networks.
* According to data center network (DCN) statistics, it takes 76 minutes to locate a fault on average.



Difficult to Locate Faults

### Slow Network Service Deployment



Slow Network Service Deployment

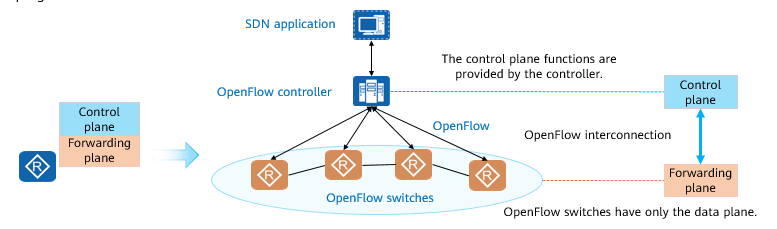
Vision of network service deployment:

* Free mobility based on network policies, regardless of physical locations
* Quick deployment of new service
* ZTP deployment on the physical network
* Plug-and-play of devices

### SDN Origin

SDN was developed by the Clean Slate Program at Stanford University as an innovative new network architecture. The core of SDN is to separate the control plane from the data plane of network devices to implement centralized control of the network control plane and provide good support for network application innovation.

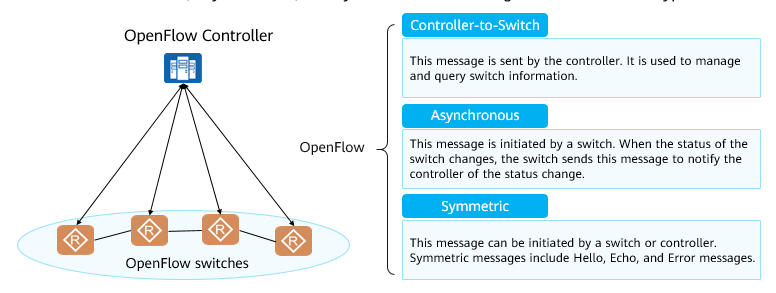
SDN has three characteristics in initial phase: forwarding-control separation, centralized control, and open programmable interfaces.



SDN Origin

### Basic Concepts of OpenFlow

OpenFlow is an SBI protocol between a controller and a switch. It defines three types of messages: Controller-to-Switch, Asynchronous, and Symmetric. Each message contains more subtypes.



OpenFlow

Controller-to-Switch messages:

* Features message: After an SSL/TCP session is established, the controller sends Features messages to a switch to request switch information. The switch must send a response, including the interface name, MAC address, and interface rate.
* Configuration message: The controller can set or query the switch status.
* Modify-State message: The controller sends this message to a switch to manage the switch status, that is, to add, delete, or modify the flow table and set interface attributes of the switch.
* Read-State message: The controller sends this message to collect statistics on the switch.
* Send-Packet message: The controller sends the message to a specific interface of the switch.

Asynchronous messages:

* Packet-in message: If no matching entry exists in the flow table or the action "send-to-controller" is matched, the switch sends a packet-in message to the controller.
* Packet-out message: The controller sends this message to respond to a switch.
* Flow-Removed message: When an entry is added to a switch, the timeout interval is set. When the timeout interval is reached, the entry is deleted. The switch then sends a Flow-Removed message to the controller. When an entry in the flow table needs to be deleted, the switch also sends this message to the controller.
* Port-status message: A switch sends this message to notify the controller when the interface configuration or state changes.

Symmetric messages:

* Hello message: When an OpenFlow connection is established, the controller and switch immediately send an OFPT\_HELLO message to each other. The version field in the message is filled with the latest OpenFlow version supported by the sender. After receiving the message, the receiver calculates the protocol version number, that is, selects the smaller one between the versions supported by the sender and the receiver. If the receiver supports the version, connection requests are processed until the connection is successful. Otherwise, the receiver replies with an OFPT\_ERROR message, in which the type field is filled with ofp\_error\_type.OFPET\_HELLO\_FAILED.
* Echo message: Either a switch or controller can send an Echo Request message, but the receiver must reply with an Echo Reply message. This message can be used to measure the latency and connectivity between the controller and switch. That is, Echo messages are heartbeat messages.
* Error message: When a switch needs to notify the controller of a fault or error, the switch sends an Error message to the controller.

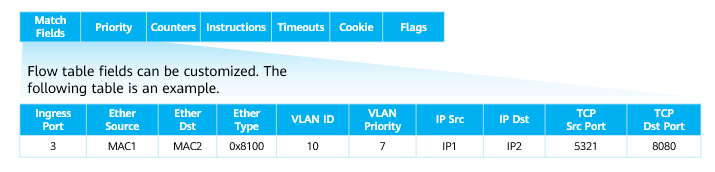
The OpenFlow protocol is still being updated. For more message types, see the OpenFlow Switch Specification released by Open Networking Foundation (ONF).

### Flow Table Overview

OpenFlow switches forward packets based on flow tables.

Each flow entry includes the Match Fields, Priority, Counters, Instructions, Timeouts, Cookie, and Flags. The Match Fields and Instructions are key fields for packet forwarding.

* The Match Fields is a field against which a packet is matched and can be customized.
* The Instructions field indicates OpenFlow processing when a packet matches a flow entry.



Flow Table

Match Fields: a field against which a packet is matched. (OpenFlow 1.5.1 supports 45 options). It can contain the inbound interface, inter-flow table data, Layer 2 packet header, Layer 3 packet header, and Layer 4 port number.

Priority: matching sequence of a flow entry. The flow entry with a higher priority is matched first.

Counters: number of packets and bytes that match a flow entry.

Instructions: OpenFlow processing when a packet matches a flow entry. When a packet matches a flow entry, an action defined in the Instructions field of each flow entry is executed. The Instructions field affects packets, action sets, and pipeline processing.

Timeouts: aging time of flow entries, including Idle Time and Hard Time.

* Idle Time: If no packet matches a flow entry after Idle Time expires, the flow entry is deleted.
* Hard Time: After Hard Time expires, a flow entry is deleted regardless of whether a packet matches the flow entry.

Cookie: identifier of a flow entry delivered by the controller.

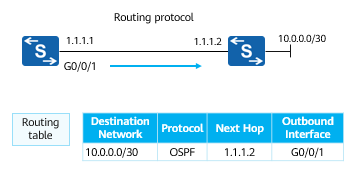
Flags: This field changes the management mode of flow entries.

### Comparison between Forwarding Modes

Typical Routing Protocol:

Packet Forwarding Based on Routing Tables

* In typical cases, network devices query routing tables to guide traffic forwarding.
* Entries in a routing table are calculated by running a routing protocol between network devices.
* The length of the routing table is fixed. Network devices forward packets based on the longest match rule. A network device has only one routing table.

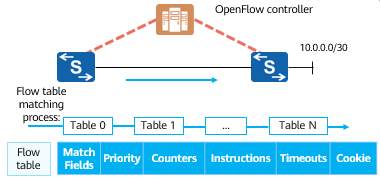


Typical Routing Protocol

OpenFlow:

Packet Forwarding Based on Flow Tables

* OpenFlow is a network protocol. Switches running OpenFlow forward traffic based on flow tables.
* Flow tables are calculated by the OpenFlow controller and then delivered to switches.
* A flow table has variable length and defines various matching and forwarding rules. A network device has multiple flow tables.



OpenFlow

For tables 0-255, table 0 is first matched. In a flow table, flow entries are matched by priority. The flow entry with a higher priority is matched first.

Currently, OpenFlow is mainly used on software switches, such as OVSs and CE1800Vs, in DCs, but not on physical switches to separate forwarding and control planes.

### Essential Requirements of SDN

The essence of SDN is to make networks more open, flexible, and simple. It builds a centralized brain for a network and implements fast service deployment, traffic optimization, or network service openness through centralized control in the global view.

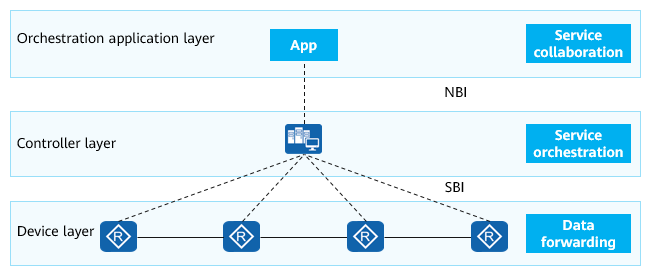
SDN has the following benefits:

* Provides centralized management, simplifying network management and O&M.
* Shields technical differences, simplifies network configuration, and reduces O&M costs.
* Offers automatic optimization, improving network utilization.
* Deploys services rapidly, shortening the service rollout time.
* Builds an open network, supporting open and programmable third-party applications.

Forwarding-control separation is a method to implement SDN.

### SDN Network Architecture

The SDN network architecture consists of the orchestration application layer, controller layer, and device layer. Different layers are connected through open interfaces. From the perspective of the controller layer, SBIs oriented to the device layer and NBIs oriented to the orchestration application layer are distinguished. OpenFlow is one of SBI protocols.



SDN Network Architecture

Orchestration application layer: provides various upper-layer applications for service intents, such as OSS and OpenStack. The OSS is responsible for service orchestration of the entire network, and OpenStack is used for service orchestration of network, compute, and storage resources in a DC. There are other orchestration-layer applications. For example, a user wants to deploy a security app. The security app is irrelevant to the user host location but invokes NBIs of the controller. Then the controller delivers instructions to each network device. The command varies according to the SBI protocol.

Controller layer: The SDN controller is deployed at this layer, which is the core of the SDN network architecture. The controller layer is the brain of the SDN system, and its core function is to implement network service orchestration.

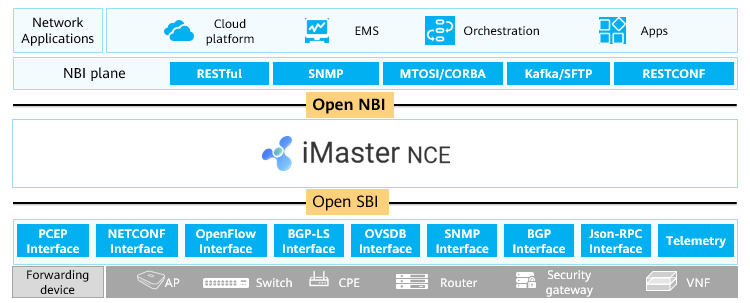
Device layer: A network device receives instructions from the controller and performs forwarding.

NBI: NBIs are used by the controller to interconnect with the orchestration application layer, mainly RESTful.

SBI: SBIs used by the controller to interact with devices through protocols such as NETCONF, SNMP, OpenFlow, and OVSDB.

### Huawei SDN Network Architecture

Huawei SDN network architecture supports various SBIs and NBIs, including OpenFlow, OVSDB, NETCONF, PCEP, RESTful, SNMP, BGP, JSON-RPC, and RESTCONF interfaces.



Huawei SDN Network Architecture

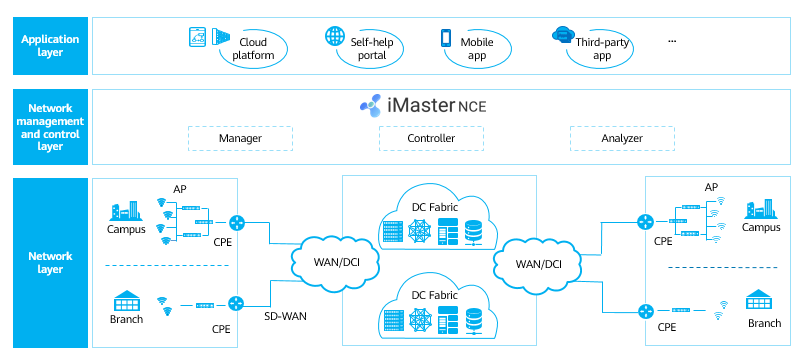
Cloud platform: resource management platform in a cloud DC. The cloud platform manages network, compute, and storage resources. OpenStack is the most mainstream open-source cloud platform.

The Element Management System (EMS) manages one or more telecommunication network elements (NEs) of a specific type.

Orchestration (container orchestration): The container orchestration tool can also provide the network service orchestration function. Kubernetes is a mainstream tool.

MTOSI or CORBA is used to interconnect with the BSS or OSS. Kafka or SFTP can be used to connect to a big data platform.

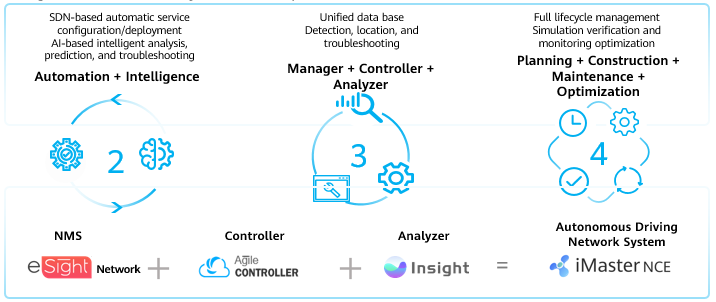
### Huawei SDN Solution - Integrating Management, Control, and Analysis to Build an Intent-Driven Network



Huawei SDN Solution

### Introduction to iMaster NCE

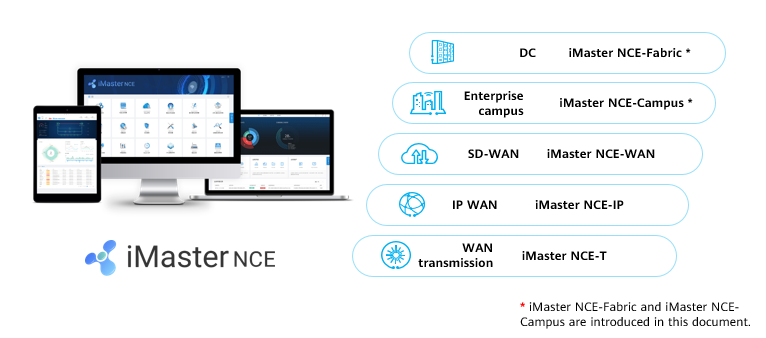
Huawei iMaster NCE is the industry intelligent network automation platform that integrates management, control, analysis, and AI capabilities.



iMaster NCE

iMaster NCE converts service intents into physical network configurations. It manages, controls, and analyzes global networks in a centralized manner in the southbound direction. It enables resource cloudification, full-lifecycle network automation, and intelligent closed-loop driven by data analysis for business and service intents. It provides northbound open APIs for quick integration with IT systems.

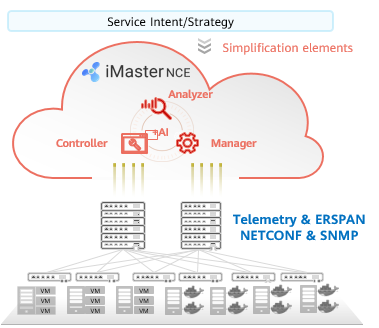
iMaster NCE can be used in the enterprise data center network (DCN), enterprise campus, and enterprise branch interconnection (SD-WAN) scenarios to make enterprise networks simple, smart, open, and secure, accelerating enterprise service transformation and innovation.



iMaster NCE Application

### Huawei CloudFabric DCN Autonomous Driving Network Solution

Based on iMaster NCE-Fabric, DCNs provide full-lifecycle services from planning, construction, O&M, to optimization.



Huawei CloudFabric DCN Autonomous Driving Network Solution

Integrated planning and construction:

* The planning tool interconnects with iMaster NCE-Fabric to implement integrated planning and construction.
* Zero Touch Provisioning (ZTP)

Simplified deployment

* Service intent self-understanding and conversion
* Network change simulation and evaluation, eliminating human errors

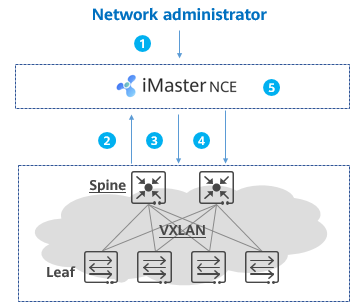
Intelligent O&M:

* Rapid fault detection and location based on knowledge graph and expert experience
* Fast fault rectification based on expert experiences and simulation analysis

Real-time optimization:

* AI-Fabric-oriented local traffic inference and online model training and optimization
* User behavior prediction and resource optimization suggestions

Simplified ZTP Deployment

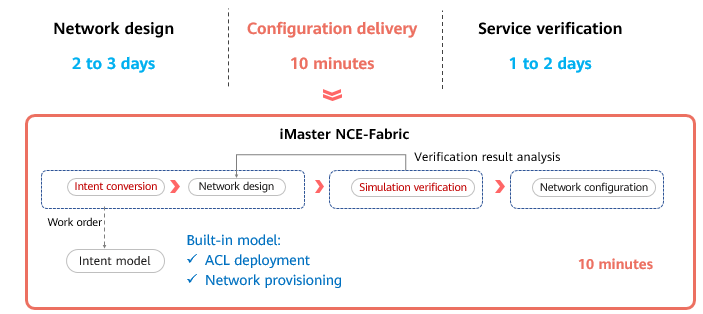


ZTP Deployment

ZTP deployment process:

* The network administrator clicks the icon on iMaster NCE to start the ZTP task.
* A device automatically obtains an IP address to access iMaster NCE.
* iMaster NCE determines the device role (spine or leaf node), delivers configurations such as the management IP address, SNMP configuration, and NETCONF configuration to online devices, and manages the devices through the management IP address.
* iMaster NCE globally delivers interconnection configurations as well as OSPF or BGP configurations.
* The device goes online successfully, and the administrator views network-wide information on iMaster NCE.

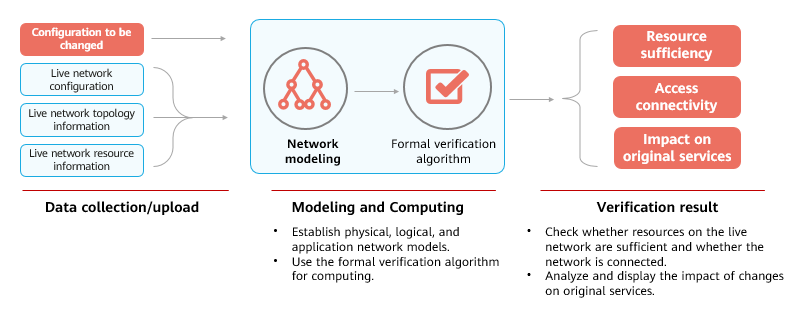
Network Intent Self-understanding and Fast Service Deployment



Network Intent Self-understanding and Fast Service Deployment

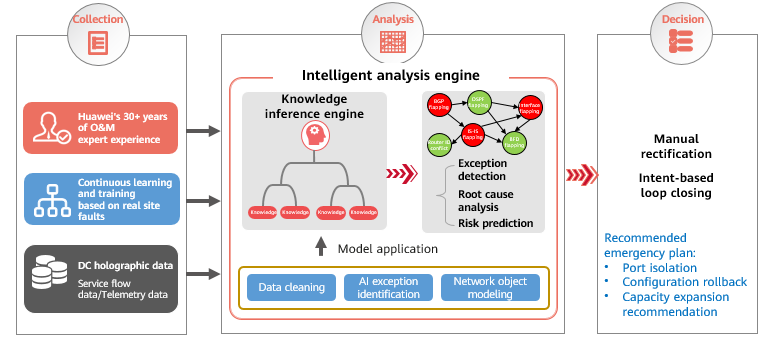
* Huawei iMaster NCE-Fabric supports automatic and fast deployment of virtualization, cloud computing, and container networks.
* iMaster NCE-Fabric can connect to a user's IT system to match the intent model for user intents and deliver configurations to devices through NETCONF to implement fast service deployment.
* iMaster NCE-Fabric can interconnect with the mainstream cloud platform (OpenStack), virtualization platform (vCenter/System Center), and container orchestration platforms (Kubernetes).

Network Change Simulation and Change Risk Prediction



Network Change Simulation and Change Risk Prediction

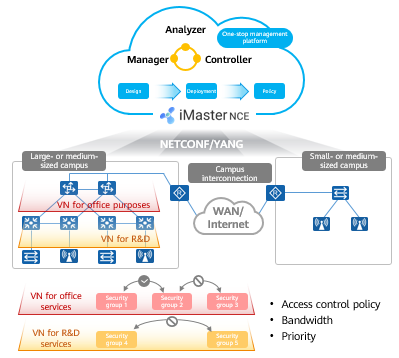
AI-powered Intelligent O&M for DCNs



AI-powered Intelligent O&M for DCNs

* iMaster NCE-FabricInsight provides AI-based intelligent O&M capabilities for DCs.

### Huawei CloudCampus Autonomous Driving Network Solution



Huawei CloudCampus Autonomous Driving Network Solution

Fast network deployment, improving deployment efficiency by 600%

* Device plug-and-play: simplified device deployment, scenario navigation, and template-based configuration
* Simplified network deployment: Network resource pooling, multi-purpose network, and automatic service provisioning

Fast service provisioning, improving user experience by 100%

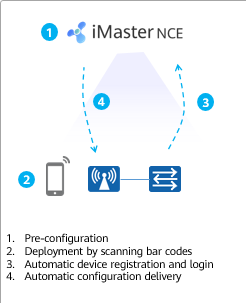
* Free mobility: GUI-based policy configuration, allowing users to access the network anytime and anywhere without changing the roaming permission and user experience
* Intelligent terminal identification: Anti-spoofing for terminal access, with an intelligent terminal identification accuracy of over 95%
* Intelligent HQoS: Application-based scheduling and shaping, and refined bandwidth management, ensuring service experience of key users

Fast intelligent O&M, improving network performance by over 50%

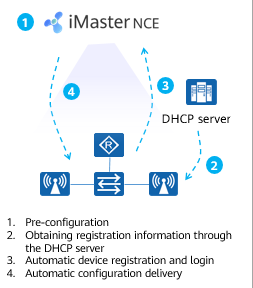
* Real-time experience visualization: Telemetry-based network experience visualization at each moment, for each user, and in each area
* Precise fault analysis: Proactively identifying 85% of typical network issues and providing suggestions, and comparing and analyzing real-time data to predict faults
* Intelligent network optimization: Predictive optimization of wireless networks based on historical data, improving network-wide performance by over 50% (Source: Tolly Certification)

Device Plug-and-Play

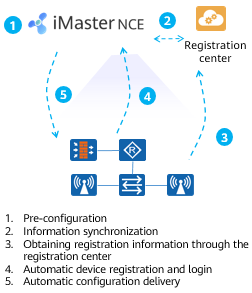
* Device plug-and-play includes but is not limited to deployment by scanning bar codes using an app, DHCP-based deployment, and deployment through the registration query center.
* Registration center: Huawei device registration query center, also called registration center, is one of the main components of Huawei CloudCampus solution. It is used to query the device management mode and registration ownership. A device determines whether to switch to the cloud-based management mode and which cloud management platform to register with based on the query result. The AP is used as an example. Huawei devices that support cloud-based management are pre-configured with the URL (register.naas.huawei.com) and port number (10020) of the Huawei device registration center.



Deployment by Scanning Bar Codes



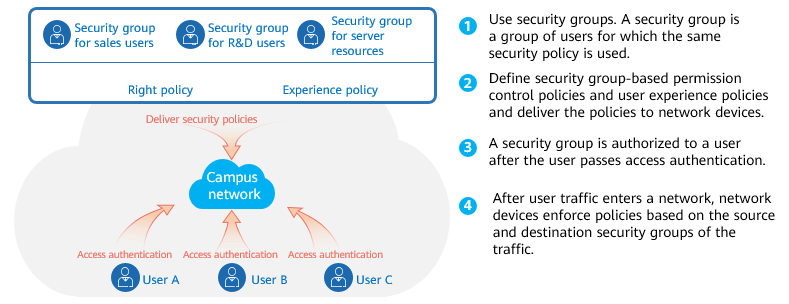
DHCP-based Deployment



Deployment Through the Registration Center

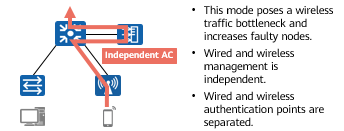
Free Mobility: Policy Management Based on Security Groups

* Free mobility: Enables users to have consistent network rights and security policies regardless of their locations and IP addresses.

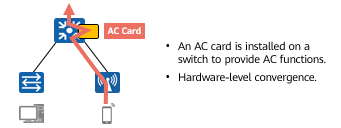


Free Mobility

Wired and Wireless Convergence

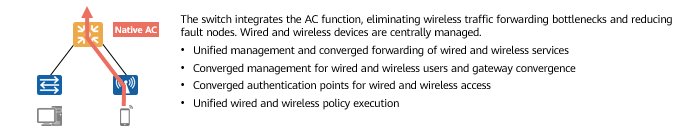


WLAN Construction Mode 1: Standalone AC



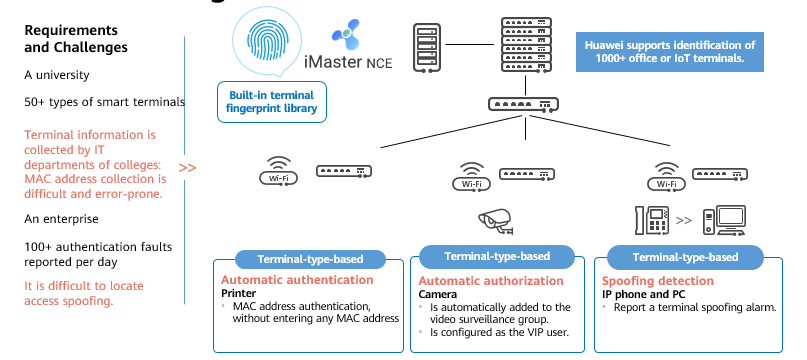
WLAN Construction Mode 2: AC Card

* Wired and wireless authentication point separation, distributed policy control, separation of control and data traffic forwarding, and troubleshooting and management difficulties.



Wired and Wireless Convergence (Native AC)

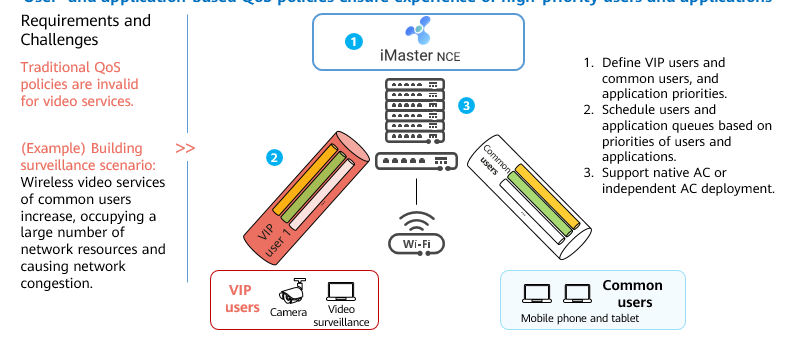
Intelligent Terminal Identification, Ensuring Secure Access



Intelligent Terminal Identification, Ensuring Secure Access

HQoS: User- and Application-based QoS Policy

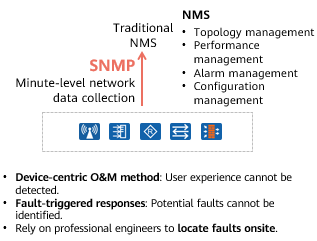
* User- and application-based QoS policies ensure experience of high-priority users and applications



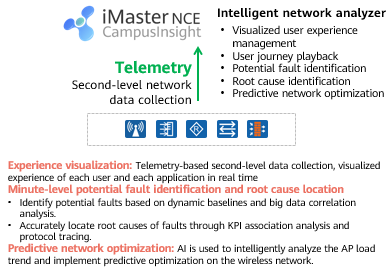
HQoS: User- and Application-based QoS Policy

AI-Powered Intelligent O&M of Campus Networks

* The efficiency is improved by using algorithms. With scenario-based continuous learning and expert experience, intelligent O&M frees O&M personnel from complex alarms and noises, making O&M more automated and intelligent.

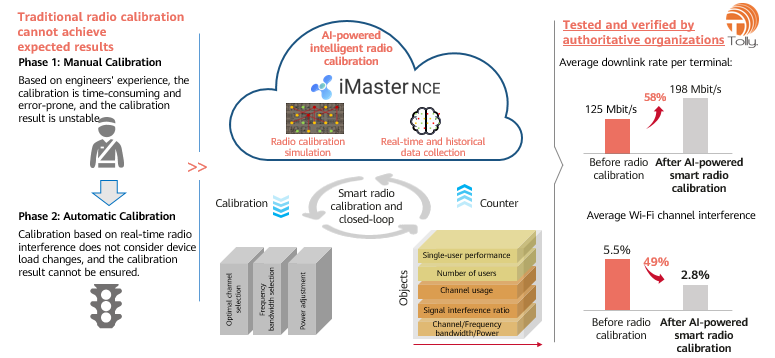


As-Is: Device-Centered Network Management



To-Be: User Experience-Centered AI-Powered Intelligent O&M

AI-Powered Intelligent Radio Calibration



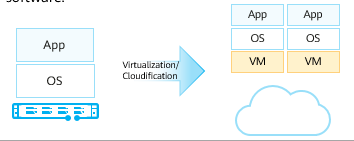
AI-Powered Intelligent Radio Calibration

## NFV Overview

### NFV Background: Thinking from IT Industry Transformation

The IT industry transformation brings thinking on network architecture and device architecture in the network industry. The network architecture layer involves the SDN controller and the device architecture layer involves the device deployment mode.

In recent years, IT technologies such as virtualization and cloud computing have been booming, and applications deployed on hardware have been gradually migrated to the cloud. Applications are deployed on private clouds, public clouds, or hybrid clouds as software.



IT Industry Transformation

Thinking about the network industry: Can network applications be deployed in a software-based manner?

In the context, Network Functions Virtualization (NFV) is introduced.

Virtualized network functions (VNFs) are implemented by virtualizing traditional NEs such as IMSs and CPEs of carriers. After hardware is universalized, traditional NEs are no longer the products with embedded software and hardware. Instead, they are installed on universal hardware (NFVI) as software.

### Origin of NFV

In October 2012, 13 top carriers (including AT&T, Verizon, VDF, DT, T-Mobile, BT, and Telefonica) released the first version of NFV White Paper at the SDN and OpenFlow World Congress. In addition, the Industry Specification Group (ISG) was founded to promote the definition of network virtualization requirements and the formulation of the system architecture.

In 2013, the ETSI NFV ISG conducted the first phase of research and completed the formulation of related standards. The ETSI NFV ISG defined NFV requirements and architecture and sorts out the standardization processes of different interfaces.

In 2015, NFV research entered the second phase. The main research objective is to build an interoperable NFV ecosystem, promote wider industry participation, and ensure that the requirements defined in phase 1 are met. In addition, the ETSI NFV ISG specified the collaboration relationships between NFV and SDN standards and open source projects. Five working groups are involved in NFV phase 2: IFA (architecture and interface), EVE (ecosystem), REL (reliability), SEC (security), and TST (test, execution, and open source). Each working group mainly discusses the deliverable document framework and delivery plan.

The ETSI NFV standard organization cooperates with the Linux Foundation to start the open source project OPNFV (NFV open source project, providing an integrated and open reference platform), integrate resources in the industry, and actively build the NFV industry ecosystem. In 2015, OPNFV released the first version, further promoting NFV commercial deployment.

NFV-related standard organizations include:

* ETSI NFV ISG: formulates NFV requirements and functional frameworks.
* 3GPP SA5 working group: focuses on technical standards and specifications of 3GPP NE virtualization management (MANO-related).
* OPNFV: provides an open-source platform project that accelerates NFV marketization.

### NFV Value

NFV aims to address issues such as complex deployment and O&M and service innovation difficulties due to large numbers of telecom network hardware devices. NFV brings the following benefits to carriers while reconstructing telecom networks:

* Shortened service rollout time
* Reduced network construction cost
* Improved network O&M efficiency
* Open ecosystem

Shortened service rollout time: In the NFV architecture, adding new service nodes becomes simple. No complex site survey or hardware installation is required. For service deployment, you only need to request virtual resources (compute, storage, and network resources) and software loading, simplifying network deployment. To update service logic, you simply need to add new software or load new service modules to complete service orchestration. Service innovations become simple.

Reduced network construction cost: Virtualized NEs can be integrated into COTS devices to reduce the cost. Enhancing network resource utilization and lowering power consumption can lower overall network costs. NFV uses cloud computing technologies and universal hardware to build a unified resource pool. Resources are dynamically allocated on demand based on service requirements, implementing resource sharing and improving resource utilization. For example, automatic scale-in and scale-out can be used to solve the resource usage problem in the tidal effect.

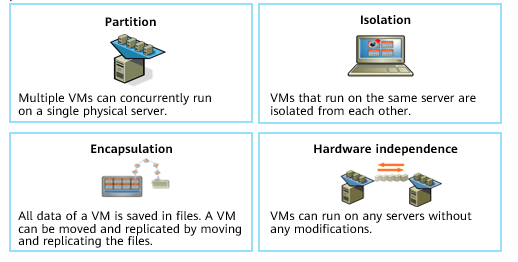
Enhanced network O&M efficiency: Automated and centralized management improves the operation efficiency and reduces the O&M cost. Automation includes DC-based hardware unit management automation, MANO application service life management automation, NFV- or SDN-based coordinated network automation.

Open ecosystem: The legacy telecom network exclusive software/hardware model defines a closed system. NFV-based telecom networks use an architecture based on standard hardware platforms and virtual software. The architecture easily provides open platforms and open interfaces for third-party developers, and allows carriers to build open ecosystems together with third-party partners.

### Key NFV Technologies

Virtualization

* Virtualization is the foundation of NFV, and cloudification is the key.
* On traditional telecom networks, each NE is implemented by dedicated hardware, resulting in high costs and difficult O&M. Virtualization features partition, isolation, encapsulation, and independence from hardware, which can meet NFV requirements. Carriers use virtualization to run software-based NEs on universal infrastructures.
* On traditional telecom networks, each NE is implemented by dedicated hardware. A large number of hardware interoperability tests, installation, and configuration are required during network construction, which is time-consuming and labor-consuming. In addition, service innovation depends on the implementation of hardware vendors, which is time-consuming and cannot meet carriers' service innovation requirements. In this context, carriers want to introduce the virtualization mode to provide software NEs and run them on universal infrastructures (including universal servers, storage devices, and switches).
* Using universal hardware helps carriers reduce the cost of purchasing dedicated hardware. Service software can be rapidly developed through iteration, which enables carriers to innovate services quickly and improve their competitiveness. By dong this, carriers can enter the cloud computing market.



Virtualization

Cloudification

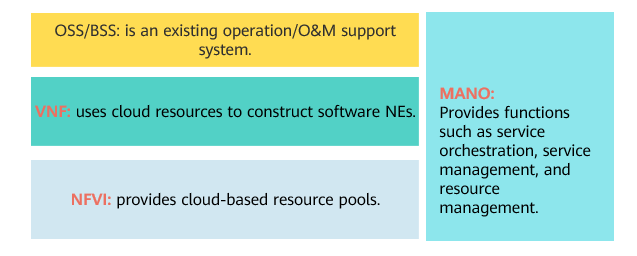
* As defined by the National Institute of Standards and Technology (NIST), cloud computing is a model that allows users to obtain resources (for example, networks, servers, storage devices, applications, services) in a shared compute resource pool based on their needs anytime, anywhere. This model enables fast resource provisioning and release, and minimizes the resource management workload and interactions with service providers.
* Cloud computing has many advantages. Cloudification of network functions on carriers' networks mainly uses resource pooling and rapid elastic scaling.
* According to the NIST, cloud computing services have the following characteristics:
  + On-demand self-service: Cloud computing implements on-demand self-service of IT resources. Resources cna be requested and released without intervention of IT administrators.
  + Broad network access: Users can access networks anytime and anywhere.
  + Resource pooling: Resources including networks, servers, and storage devices in a resource pool can be provided for users.
  + Rapid elasticity: Resources can be quickly provisioned and released. The resource can be used immediately after being requested, and can be reclaimed immediately after being released.
  + Measured service: The charging basis is that used resources are measurable. For example, charging is based on the number of CPUs, storage space, and network bandwidth.



Characteristics of Cloud Computing

### Introduction to the NFV Architecture

The NFV architecture includes the network functions virtualization infrastructure (NFVI), a virtualized network function (VNF), and management and orchestration (MANO). In addition, the NFV architecture needs to support the existing business support system (BSS) or operations support system (OSS).



NFV Architecture

Each layer of the NFV architecture can be provided by different vendors, which improves system development but increases system integration complexity.

NFV implements efficient resource utilization through device normalization and software and hardware decoupling, reducing carriers' TCO, shortening service rollout time, and building an open industry ecosystem.

The NFVI consists of the hardware layer and virtualization layer, which are also called COTS and CloudOS in the industry.

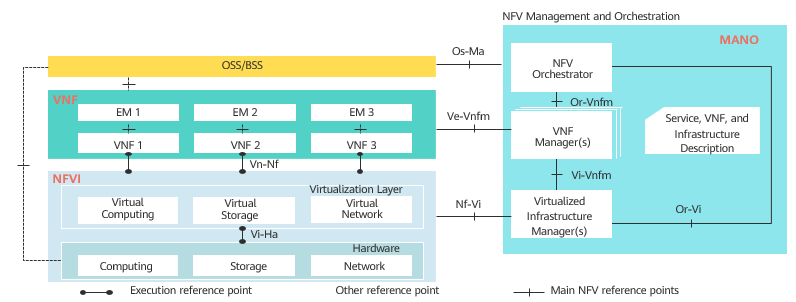
* COTS: universal hardware, focusing on availability and universality, for example, Huawei FusionServer series hardware server.
* CloudOS: cloud-based platform software, which can be regarded as the operating system of the telecom industry. CloudOS virtualizes physical compute, storage, and network resources into virtual resources for upper-layer software to use, for example, Huawei FusionSphere.

VNF: A VNF can be considered as an app with different network functions and is implemented by software of traditional NEs (such as IMS, EPC, BRAS, and CPE) of carriers.

MANO: MANO is introduced to provision network services in the NFV multi-CT or multi-IT vendor environment, including allocating physical and virtual resources, vertically streamlining management layers, and quickly adapting to and interconnecting with new vendors' NEs. The MANO includes the Network Functions Virtualization Orchestrator (NFVO, responsible for lifecycle management of network services), Virtualized Network Function Manager (VNFM, responsible for lifecycle management of VNFs), and Virtualized Infrastructure Manager (VIM, responsible for resource management of the NFVI).

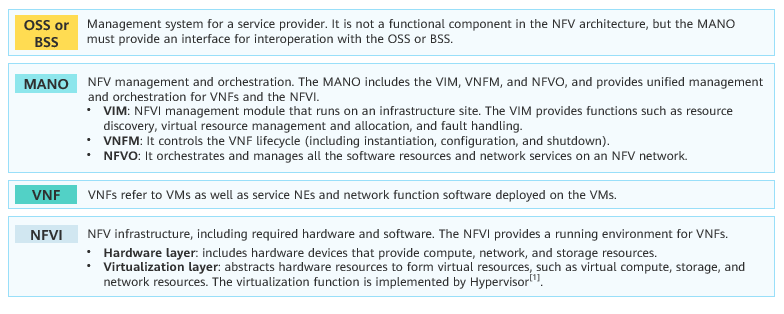
### Standard NFV Architecture

ETSI defines the standard NFV architecture, which consists of the NFVI, VNF, and MANO. The NFVI includes the universal hardware layer and virtualization layer. The VNF is implemented using software, and the MANO implements management and orchestration of an NFV architecture.



Standard NFV Architecture

### Functional Modules of the NFV Architecture



Main functional modules defined in the standard NFV architecture

BSS: business support system

OSS: operation support system

A hypervisor is a software layer between physical servers and OSs. It allows multiple OSs and applications to share the same set of physical hardware. It can be regarded as a meta operating system in the virtual environment, and can coordinate all physical resources and VMs on the server. It is also called virtual machine monitor (VMM). The hypervisor is the core of all virtualization technologies. Mainstream hypervisors include KVM, VMWare ESXi, Xen, and Hyper-V.

### NFV Architecture Interfaces

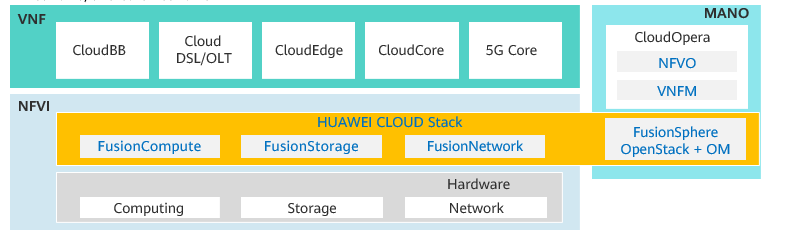
Main interfaces of the standard NFV architecture

|  |  |
| --- | --- |
| Interface | Description |
| Vi-Ha | Is used between the virtualization layer and hardware layer. The virtualization layer meets basic hardware compatibility requirements. |
| Vn-Nf | Is used between a VM and the NFVI. It ensures that VMs can be deployed on the NFVI to meet performance, reliability, and scalability requirements. The NFVI meets VMs' OS compatibility requirements. |
| Nf-Vi | Is used between the virtualization layer management software and NFVI. It provides management of virtual computing, storage, and network systems of NFVI, virtual infrastructure configuration and connections, as well as system usage, performance monitoring, and fault management. |
| Ve-Vnfm | Is used between the VNFM and a VNF, implementing VNF lifecycle management, VNF configuration, VNF performance, and fault management. |
| OS-Ma | Manages lifecycles of network services and VNFs. |
| Vi-Vnfm | Is used for interaction between the service application management system or service orchestration system and virtualization layer management software. |
| Or-Vnfm | Sends configuration information to the VNFM, configures the VNFM, and connects the orchestrator and VNFM. It exchanges information with the NFVI resources allocated to VNFs and information between VNFs. |
| Or-Vi | Is used to send resource reservation and resource allocation requests required by the orchestrator and exchange virtual hardware resource configurations and status information. |

### Huawei's NFV Solution

In the Huawei NFV architecture, functions of the virtualization layer and VIM are implemented by the HUAWEI CLOUD Stack NFVI platform. HUAWEI CLOUD Stack can virtualize compute, storage, and network resources and centrally manage, monitor, and optimize physical virtualization resources.

Huawei provides cloud-based solutions for carriers' wireless networks, bearer networks, transport networks, access networks, and core networks.



Huawei's NFV Solution

DSL: Digital Subscriber Line

OLT: Optical Line Terminal

## FAQ

Q1: What is the relationship between SDN and NFV in the industry?

A: Both SDN and NFV involve network transformation and the NFV concept was proposed at the SDN and OpenFlow World Congress. However, they are independent of each other. SDN mainly affects the network architecture, and NFV mainly affects the NE deployment mode.

Q2: What is the relationship between SDN and NFV in Huawei solutions?

A: Huawei provides different solutions for SDN and NFV, but they are associated. Huawei NFVI solution is provided by HUAWEI CLOUD Stack.

## Quiz

1. (Single) Which of the following statements about OpenFlow is incorrect? ( )
2. OpenFlow is a protocol used to configure network switches. The process is similar to the application programming interface (API).
3. OpenFlow is an open source protocol.
4. OpenFlow switches forward packets based on flow tables.
5. OpenFlow is implemented through XML.
6. (Multiple) OpenFlow matches and processes network packets based on user-defined or preset rules. Which of the following are the components of an OpenFlow rule? ( )
7. Match Fields
8. Priority
9. Processing instructions
10. Statistics (such as Counters)
11. (Multiple) Which of the following statements about the key features of Network Functions Virtualization (NFV) is false? ( )
12. Centralized control and global efficiency optimization
13. Open interfaces and accelerate service rollout
14. Cloud-based upper-layer services and standard underlying hardware
15. Hierarchical operation, accelerating service rollout and innovation
16. (Multiple) In the SDN network architecture, which of the following belong to the application layer? ( )
17. Openstack
18. Third-party app platform
19. Server
20. Switch
21. (Multiple) Huawei SDN network architecture supports various southbound and northbound interfaces, including OpenFlow, OVSDB, NETCONF, PCEP, RESTful, SNMP, BGP, JsonRPC, and RESTCONF. ( )
22. True
23. False
24. (Multiple) Which of the following statements about Huawei SDN solution are true? ( )
25. The solution supports various SBI protocols, such as RESTful, NETCONF, and OVSDB.
26. OpenFlow can be used as the SBI protocol.
27. The solution integrates management, control, and analysis to build a simplified network.
28. The solution provides open and programmable network interfaces to support third-party application development and system interconnection.
29. Please briefly describe the benefits of NFV.

## Summary

With the transformation and development of the network industry, SDN and NFV are proposed.

SDN is an innovation of network architecture. It uses a controller to make networks more open, flexible, and simple.

NFV is an innovation in the deployment of telecom network devices. Based on virtualization and cloud computing, NFV helps reconstruct telecom networks.