



5G SLICING
ASSOCIATION



中国移动
China Mobile

研究院
CMRI



HUAWEI

Tencent 腾讯



国家电网
STATE GRID

中国电力科学研究院有限公司
CHINA ELECTRIC POWER RESEARCH INSTITUTE



DIGITAL DOMAIN
数字王国

Categories and Service Levels of Network Slicing White Paper

March 2020

Contents

1 Introduction

2 Principle and Methodology for Network Slicing Levels

3 Solution for Network Slicing Levels

3.1 5G Network Slicing and Isolation Capability

3.1.1 RAN Slice Isolation Solution

3.1.2 Transport Network Slice Isolation Solution

3.1.3 Core Network Slice Isolation Solution

3.2 Security Capabilities of 5G Network Slices

3.3 O&M Models

4 Suggestions on Typical Case Categories

4.1 Public Network Slicing Cases

4.1.1 Scenarios and Requirements of Public Network Slicing

4.1.2 Network Slicing Solution for Cloud Games

4.2 Industry Network Slicing Cases

4.2.1 Scenarios and Requirements of Industry Network Slicing

4.2.2 Network Slicing Solution for UHD Live Broadcast Backhaul

4.3 Network Slicing Cases for Special Industries

4.3.1 Network Slicing Scenarios and Requirements in Special Industries

4.3.2 Network Slicing Solution for Power Grids

5 Cost Analysis

6 Industry Application Suggestions

7 Summary and Prospect

8 Appendixes

5G is an upgraded generation of wireless technologies that also revolutionizes the network service architecture. Network slicing is one key technology that tells 5G apart from 4G, where a slice itself forms a logical private network. Targeted at vertical industries, network slicing is a powerful enabler for telecom operators to develop industry customers, incubate new services, and improve network value. Industry partners from such as electric power, media, banking, factory, and transportation fields are taking a close interest in network slicing in the hope to cultivate novel services and upgrade industries.

3GPP as the dominant standards developing organization (SDO) of 5G standards had preliminarily defined in Release 15 (frozen in June 2019) the basic functions and procedures of network slicing, laying a solid foundation for the first wave of 5G deployment and commercial adoption of network slicing services. However, a slice as a customized end-to-end logical network requires support from across the radio access network (RAN), transport network, core network, and management system. If sorted and then combined based on these domains' capabilities, the slice options will be too many. In early commercial adoption, letting industries clearly know what a slice can do and narrowing down to an optimal slice solution that fits most industry applications have become an urgent issue.

This document elaborates on the 5G Network Slicing levels. It defines five capability levels of 5G end-to-end Network Slicing, holistically considering current standard definition, product implementation progress in industries in early commercial adoption, and requirements and practices of vertical industries. The document then dives into different capability levels of the RAN, transport network, and core network as well as important factors that affect slice levels, such as security and operation capabilities. Based on the aforesaid capabilities and slice levels, this document further analyzes costs and provides price references for slices of different levels. Based on typical application scenarios in vertical industries, this document also summarizes the requirements of vertical industries for 5G networks and slices, and suggests corresponding slice levels as a reference for customized services in industry applications. Finally, this document discusses the maturity of 5G network slicing in industries and looks into application trends.

In conclusion, the classification of 5G Network Slicing levels is significant for vertical industries to select desired slice solutions. Categories and service levels of Network Slicing are prerequisite for introducing network slicing to vertical industries. Only with a clear view of the Network Slicing capabilities can the application and development of slicing technologies be promoted in various industries and more tailored logical private networks and services be developed for vertical industries.

2 Principle and Methodology for Network Slicing Levels

Unlike a traditional 4G network that works in "one pipe and best effort" mode, a 5G network in combination with slicing aims to provide various end-to-end logical private networks that run on a shared infrastructure and a shared network to cater for the specific requirements of vertical industries. Based on analytics of performance counters, function differences, network requirements, and O&M modes, requirements for 5G fall into two types:

- **Public network users**

The services that 4G networks provide for individuals are all retained in 5G at a consistent or even better user experience.

- **Industrial network users**

- Common industries

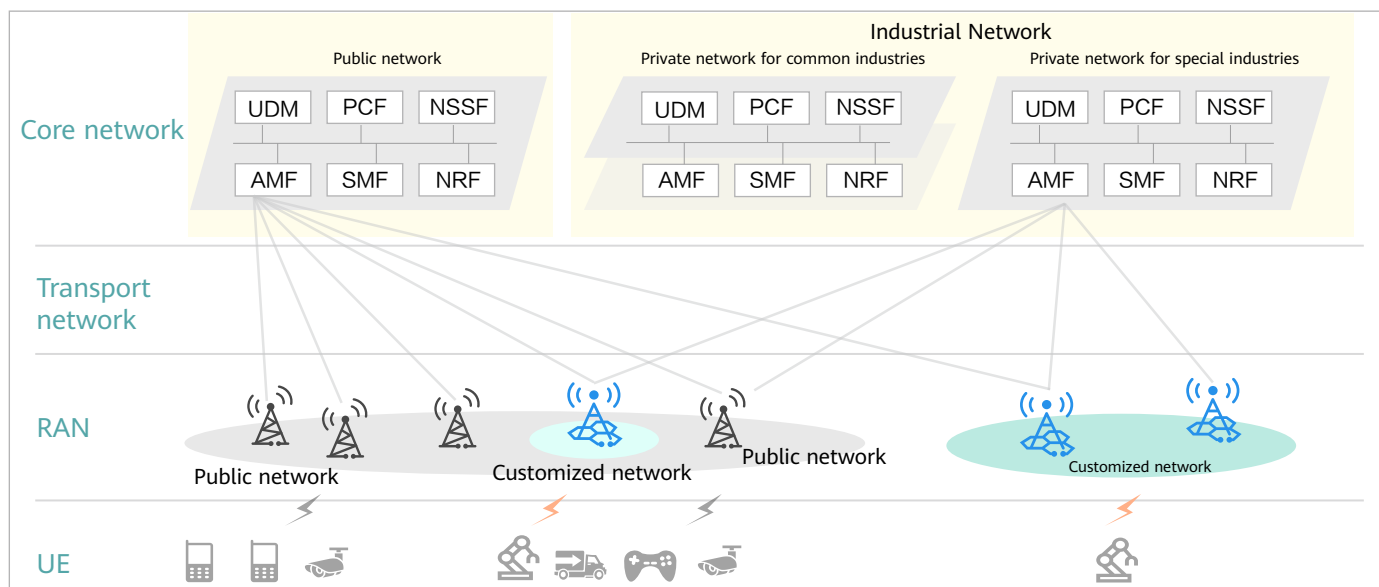
Common industry users have requirements for service isolation and quality, and may call for differentiation in customization in terms of such as connection management.

- Special industries

Users who have specific requirements (for example, high isolation or high service quality assurance) demand extremely high security, such as power grids, government, and army.

Public networks and industry networks share core network hardware, transmission resources, and radio resources. This sharing mechanism gives full play to network scale effect. IoT numbers and public network numbers are used to separate UEs on different networks, and NEs, resources, and base stations can be exclusively used by different networks, enabling flexible architectures and configuration modes.

Figure 2-1 Architecture of Public networks and industry networks



To meet these 5G network slicing requirements and those concerning isolation, deployment, and operation, two relatively independent 5G Network Slicing slices are available: public network slices, industrial Network Slicing. This document defines multi-level slices with varying capabilities to meet corresponding requirements of 5G users.

Depending on the existing network capabilities, the RAN, transport network, core network, security, and operation capabilities are holistically considered for different slice levels to match the most possible network deployment policies. A total of five slice capability levels are provided to meet the three types of 5G requirements, as shown in the following figure.

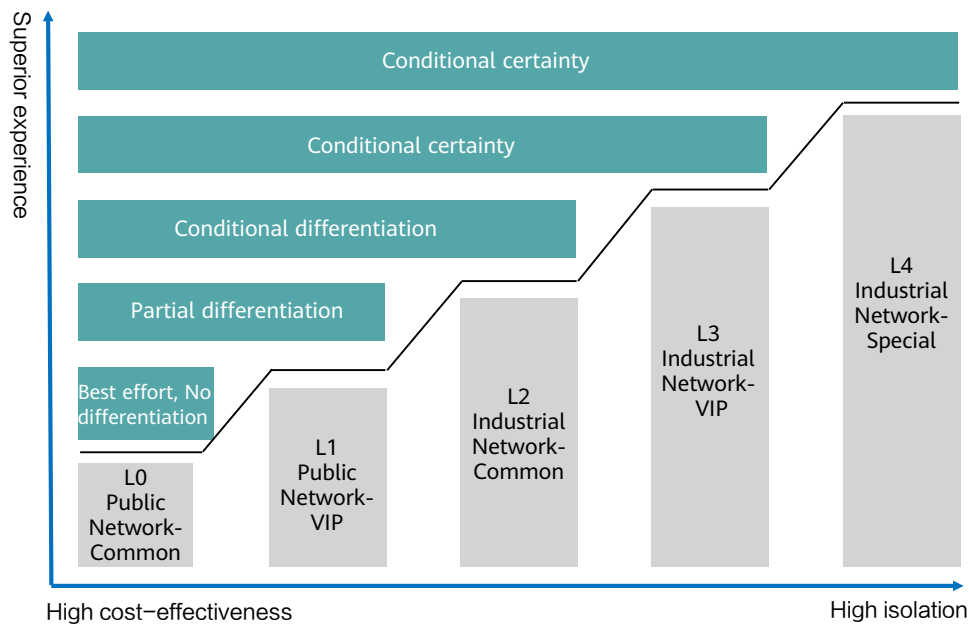


Figure 2-2 Slice capability levels

Table 2-1 describes Network Slicing levels.

| Slice Level | | L0 | L1 | L2 | L3 | L4 |
|------------------------|--------------------|---|---|--|--|--|
| Network Type | | Public network | | Industrial network | | |
| Level Classification | | Common | VIP | Common | VIP | Special |
| Definition | | Built on 5G public network infrastructure, with no special requirements | Built on 5G public network infrastructure, with tailored requirements | Built on 5G industry network infrastructure, with value-added services | Built on 5G industry network infrastructure, with specific resources exclusively used and advanced services provided | Built on 5G industry private network infrastructure, with all resources exclusively used and reliability services provided |
| Resource Customization | Resource Isolation | Complete sharing | Complete sharing (or partially exclusive) | Complete sharing (or partially exclusive) | Partially exclusive | Completely independent |
| Service Experience | Security | Basic security | eMBB enhanced security | Service feature security | High-level service feature security | High-level security |
| | O&M | None | None | Visualization | Manageability | Manageability |
| | Customized Service | Default | Customization | Customization | Customization | Customization |

- **Slice level**
Five slice levels, including L0 to L4, are defined.
- **Network type**
Two network types, including public network and industrial network, are available.
- **Level classification**
Public networks have two levels: common and VIP. Industrial networks have three levels: common, VIP, and special.
- **Slice level definition**
It defines each slice level.
- **Resource customization**
Three options are available, including fully shared, partially exclusive, and completely independent. In initial construction, public networks and industry networks are separated, delivering natural isolation. Resource customization refers to the degree of resource isolation among the RAN, transport network, and core network. For details, see section 3.1 "5G Network Slicing and Isolation Capability."

- **Service experience**

- **Security**

Five options are available, including basic security, enhanced Mobile Broadband (eMBB) enhanced security, service feature security, high-level service feature security, and high-level security. Security capabilities vary with slice levels and network types. For details, see section 3.2 3.2 "Security Capabilities of 5G Network Slicing."

- **O&M modes**

Three options are available, including no O&M, industry visualization, and industry manageability. For details, see section 3.3 "O&M Models."

- **Customized service**

Except common users on public networks that have no special requirements, L1 to L4 require different assurance capabilities which are to be tailored to specific scenarios and requirements.

In addition to the aforementioned basic network capabilities (network resources, isolation, O&M, security, and customized services), different vertical industries have their own customization requirements. Network slicing needs to provide customization capabilities, such as support for non-IP transmission, clock synchronization, and high-speed device processing, and such capabilities can be added to each of capability levels.

This white paper focuses on eMBB and low-latency slices. In the future, levels will be optimized with standard improvement and live network maturity in ultra-reliable low-latency communication (URLLC) and Massive Machine-Type Communications (mMTC) scenarios.

3 Solution for Network Slicing Levels

This chapter provides detailed solutions to the aforementioned five capability levels in terms of RAN, transport network, core network, and management system in the preceding dimensions.

3.1 5G Network Slicing and Isolation Capability

3.1.1 RAN Slice Isolation Solution

Currently, the RAN has Four groups of combination capabilities, which are mapped based on slice level classification principles. The following are the grouping and mapping principles regarding RAN.

The RAN slice isolation solution aims to isolate and guarantee resources for network slices on new radio (NR) RAN. Slice-specific QoS assurance, air interface dynamic RB resource sharing, and static RB resource reservation are available, differentiating in service latency, reliability, and isolation requirements.

The following table provides suggestions on typical RAN slice levels tailored to specific requirements in different service scenarios, and the typical industries and service scenarios specific to each isolation level.

Table 3-1 Suggestions on 5G RAN slice levels

| Slice Level | RAN Slice Type | Air Interface | Industry |
|----------------------|--|---|--|
| L0 L1 L2 | Combination 1: RB resource sharing and QoS-specific slice | QoS priority-based assurance | Enterprise broadband |
| L3/L4 (On demand) | Combination 2: partially reserved RB resources and dynamically shared slices | Dynamic RB resource sharing | Basic service assurance is required. Example services include smart grid inspection and media live broadcast. |
| | Combination 3: resource-exclusive slice | Static RB resource reservation | High requirements are posed on service isolation and bandwidth. Examples include power grid distribution automation, government, and public security private networks. |
| | Combination 4: carrier-exclusive slice | Use network slicing on the dedicated network with exclusive carrier frequencies | This level is applicable to mining, manufacturing, and departments with high security requirements (such as government security departments) |

In air interface assurance, most services are guaranteed by setting differentiated QoS priorities, thereby improving the efficiency of scarce resources such as spectrums. However, as 5G gradually penetrates into the production and management processes in various industries, different levels of assurance need to be provided on the RAN.

Scheduling air interface resources can involve QoS (5QI, short for 5G QoS Identifier) priorities and RB resource reservation, and carrier isolation.

- **QoS-based scheduling**

When resources are insufficient, on-demand customization provides network services with differentiated QoS through service scheduling weights, admission thresholds, and queue management thresholds. Regarding resource preemption, air interface resources are preferentially scheduled for high-priority services. Under resource congestion, high-priority services may be affected.

- **RB resource reservation**

Multiple slices can share RB resources of one cell. RB resources are reserved and allocated to a specific slice based on resource requirements. RB reservation is classified into static reservation and dynamic sharing.

- Dynamic sharing

Resources reserved for a specific slice can be reused by other slices to a certain extent. When the slice does not need to use the reserved RB resources, the reserved RB resources can be partially or completely used for data transmission of other slices. During uplink and downlink data transmission, required resources can be allocated in time.

- Static reservation

Resources reserved for a specific slice cannot be allocated to any other slice at any time. This mode ensures that sufficient resources are always available.

- **Carrier isolation**

Different slices run on different carrier-served cells. Each slice uses only the air interface resources of a corresponding cell. Slices are strictly distinguished to guarantee their own resources.

3.1.2 Transport Network Slicing Isolation Solution

The isolation on mobile transport networks between RANs and CNs can be hard isolation or soft isolation, depending on slice security and reliability requirements. The isolation technology can be FlexE/MTN interface isolation, MTN cross-connection isolation, or VPN+QoS isolation, depending on the isolation, latency, and availability requirements.

- **Hard Isolation Technology**

- FlexE/MTN Interface Isolation

With FlexE/MTN Interface, multiple elastic Ethernet hard pipes can be created on one physical port. Services can achieve time slot isolation at the interfaces and achieve statistical multiplexing within the devices.

- MTN Cross-Connection Isolation

Based on the Ethernet 64/66B code block-based cross-connection technology, TDM (Time Division Multiplexing) time slot isolation is achieved, thereby achieving extremely low forwarding delay and isolation effects. The forwarding delay of a single hop ranges from 5 μ s to 10 μ s, which is much lower than that of traditional packet switching devices.

The FlexE/MTN interface isolation technology can be used together with the MTN cross-connection isolation technology or packet forwarding technology for packet transmission.

- **Soft Isolation Technology**

VPN+QoS isolation: Services on a physical network can be isolated using VPN. VPN+QoS software isolation cannot achieve timeslot-level isolation as in physical isolation.

Currently, the transport side can provide Four groups of channels, which are mapped to slice levels, as shown in Table 3-2.

Table 3-2 Suggestions on 5G transport Network Slicing levels

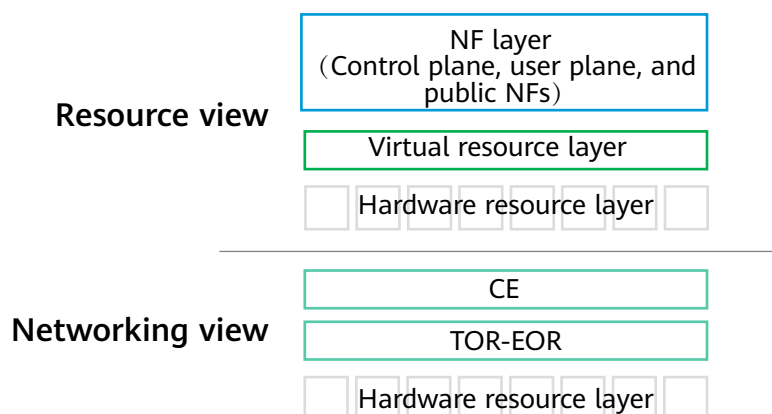
| Slice Level | Slice Type | Service | Industry |
|-------------|--|---|---|
| L0 | VPN sharing+QoS scheduling | 5G 2C personal data plans | Internet access and OTT video |
| L1 | VPN sharing + FlexE/MTN interface isolation (tunnel isolation) | 5G 2C games, cloud VR data plans, and industry applications requiring mobile access | Cloud gaming, home cloud VR, and industry applications such as mobile rescue, drones, and mobile surveillance |
| L2 | VPN isolation + FlexE/MTN interface isolation (tunnel isolation) | 5G 2B vertical industry production services with fixed access | Power grid, manufacturing, healthcare, mining, port, and IoV |
| L3 | VPN isolation + FlexE/MTN interface isolation (tunnel isolation) or E2E MTN channel (MTN interface isolation +MTN cross-connection,E2E physical isolation) | 5G 2B vertical industry life services with fixed access | Government and enterprise private line, meter reading and collection, video surveillance, and live broadcast |
| L4 | E2E MTN channel(MTN interface isolation +MTN cross-connection, E2E physical isolation) | Fixed 2B platinum private line service (one-hop transmission) | Private lines for government, finance, securities, and power grid customers |

- 1. VPN sharing+QoS scheduling:** IP packet forwarding is performed, and traffic is involved in QoS scheduling.
- 2. VPN sharing+ FlexE/MTN interface isolation:** FlexE/MTN interfaces and QoS are combined. Timeslot isolation is performed for service access, and IP forwarding is performed. VPN sharing enables QoS scheduling for traffic. The isolation is better than that of traditional packet switching devices, but is weaker than that of MTN cross-connection forwarding.
- 3. VPN isolation+FlexE/MTN interface isolation:** FlexE/MTN interfaces and QoS scheduling are combined. Timeslot isolation is performed for service access, and IP forwarding is performed. VPN isolation is performed. QoS scheduling is performed for traffic. The isolation is better than that of traditional packet switching devices, but is weaker than that of MTN cross-connection forwarding.
- 4. E2E MTN channel:** The MTN interfaces and MTN cross-connection isolation technologies are combined. Timeslot isolation is performed for service access, and MTN cross-connection is used in forwarding. Service isolation is physical isolation. The forwarding delay of a single hop ranges from 5 μ s to 10 μ s, which is much lower than that of traditional packet switching devices.

3.1.3 Core Network Slicing Isolation Solution

The core Network Slicing isolation solution helps isolate 5GC Network Slicing resources from the networking and guarantee the SLA. The resource view mainly shows the 5GC hardware resource layer, virtual resource layer, and NF layer allocated for slice isolation. The networking view mainly shows the isolation of switches or routers in the 5GC DCs.

Figure 3-1 Layered separation of 5GC Network Slicing



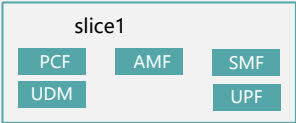
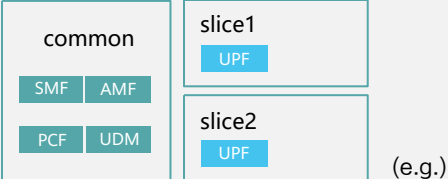
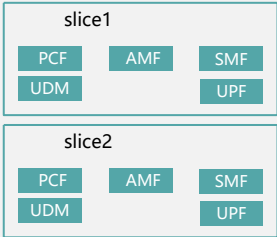
The resource view and networking view as well as the diverse isolation requirements in different service scenarios help make suggestions on typical isolation levels, as described in the following table. This table also describes the typical industries and service scenarios for each isolation level.

Table 3-3 Suggestions on 5GC Network Slicing levels

| Slice Level | 5GC Network Slicing Type | Key Isolation Technology | | | | Involved Industry | Typical Service Scenario |
|-------------|------------------------------|----------------------------|------------------------|----------|-----------------------|---------------------------------------|--|
| | | Hardware Resource Layer | Virtual Resource Layer | NF Layer | Intra-DC Transmission | | |
| L0 | Public network - common | Fully shared | | | | NA | Basic B2C services by default (Internet access and video best-effort services) |
| L1 | Public network - VIP | Shared or partially shared | | | | NA | Preferential services for the public network: carrier-operated game acceleration and video acceleration services |
| L2 | Industrial network - common | Shared or partially shared | | | | Game, video, and education | Game acceleration, 4K/AR/VR live broadcast, and AR/VR education |
| L3 | Industrial network - VIP | Shared or partially shared | | | | Healthcare and industry manufacturing | Local networks of hospitals and industrial parks |
| L4 | Industrial network - special | Independent on demand | | | | Public security and electric power | Public security emergency network and power grid |

1. The hardware resource layer refers to a variety of x86/Arm-based servers. The hardware resource layer can work in either shared or independent isolation mode. The independent mode is also referred to as physical isolation.
2. The virtual resource pool is also called network function virtualization infrastructure (NFVI). It uses virtualization technologies (such as VM and container) to process software of traditional communications devices carried on COTS hardware, implementing fast development, deployment, and elastic scaling of new services. A virtual resource pool can also work in either shared or independent isolation mode. The independent mode is also referred to as logical isolation.
3. The NF layer is based on the network functionfunctions virtualization (NFV) and service based architecture (SBA) defined in 3GPP specifications. The network function/virtual network function layer (NF/VNF) of the 5GC also supports on-demand isolation at different layers, which ensures service independence between different slices.
 - A. The fully shared mode is equivalent to the best-effort mode on the basis of one transmission path on 2G/3G/4G networks. This mode is used for common consumer services of public networks and has no special requirements for security isolation.
 - B. The partially shared mode achieves the optimal balance between security isolation and costs, because it takes industry requirements into consideration, with most of NFs shared and a few NFs independently deployed. This mode meets the Network Slicing level requirements of most common industries.
 - C. The fully independent mode is equivalent to building a complete industry-dedicated core network, resulting in the optimal security isolation but the highest construction and operation costs. Therefore, this mode is only used for special industries that require ultra-high security isolation and are not cost-sensitive.

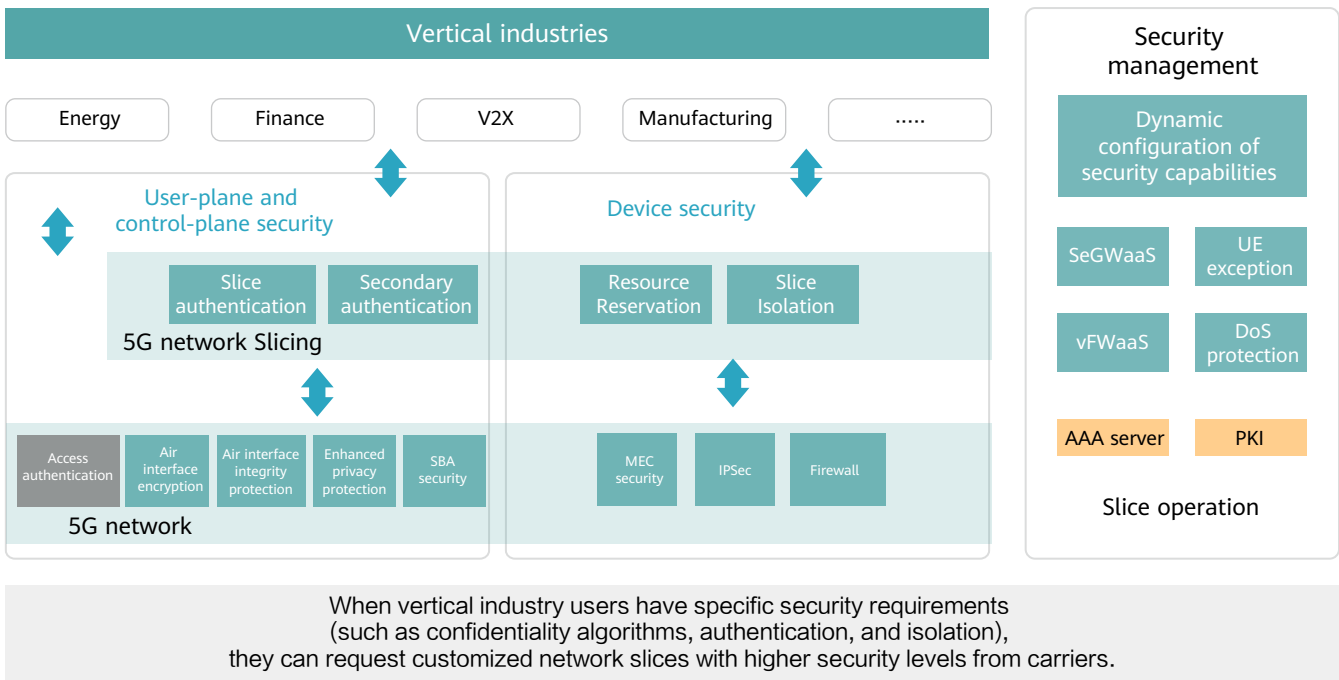
Table 3-4 Isolation modes for the 5GC NF layer

| Fully Shared Mode | Partially Shared | Fully Independent Mode |
|---|--|---|
|  | <p>Some NFs are independently deployed as required. For example, the UPF is independently deployed, or the SMF and UPF are independently deployed.</p>  |  |

3.2 Security Capabilities of 5G Network Slicing

To support E2E security protection for different services, flexible security architecture is required to provide multi-level slice security assurance. When vertical industry users have specific security requirements, they can request customized Network Slicing with different security protection levels from carriers. Differentiated security capabilities include security management capabilities Security capabilities of network protocols and network device resource security capabilities, as shown in the following figure.

Figure 3-2 Security capabilities of 5G Network Slicing



1. Security management capabilities

(1) Visualized 5G network security situation: 5G system provides visualized monitoring of application layer security, infrastructure security, and user-plane/control-plane/management-plane security. It helps implement quick response and closed-loop management based on both manual and automated processing. This ensures that carrier networks and data are not intruded or damaged by external and internal users. In addition, misoperations and unauthorized operations of internal personnel can be audited and monitored, which serves as a reliable source of evidence for post-incident tracing. A slice security situation awareness portal can be provided for industry customers.

(2) Security service: Network Slicing provide hierarchical security O&M capabilities and security services based on differentiated security requirements of users in different industries. For example, enterprises can use the capability of detecting abnormal terminals to provide network traffic cleansing, malicious website detection, and network blocking services. In addition, security services, such as security test, security training, code audit, graded protection evaluation, and security integration, can be provided if required by customers.

2. Security capabilities of network protocols

(1) Access authentication: 5G Network Slicing can use basic authentication capabilities, that is, primary authentication and unified authentication framework (default capabilities), provided by the 5G system to authenticate subscribers during network access and establish a unified key hierarchy that is independent from the access technology. The 5G system also provides optional slice authentication and secondary authentication mechanisms to flexibly support identity authentication in a variety of application scenarios.

(2) Control plane and user plane protection: Mandatory integrity protection and optional encryption protection are provided for signaling exchanged between UEs and gNodeBs, as well as between UEs and AMFs. Encryption protection and integrity protection are optional for subscriber data. User-plane integrity protection is disabled over the air interface for voice, video, and common subscriber data, but is enabled over the air interface for IoT data services and special data services that have high reliability requirements.

(3) Privacy protection: 5G globally unique temporary identities (5G-GUTIs) or 5G temporary mobile subscriber identities (5G-TMSIs) are used to replace subscription permanent identifiers (SUPIs) for protection. To prevent the disclosure of subscriber information in initial access messages of UEs, enhanced air interface privacy protection, that is, an SUPI encryption (SUCI) mechanism can be used.

(4) SBA security: The NRF-based discovery and authorization service can be used between 5GC NFs. HTTPS can be optionally used to protect information security, and TLS bidirectional identity authentication is used to prevent spoofing NFs from accessing the network, ensuring the security of the SBA architecture.

3. Device resource security capability

In addition to effective isolation and resource reservation of compute resources, storage resources, wireless network resources, and transport network resources, 5G slicing also enhances security mechanisms to meet hierarchical security requirements.

(1) Transmission security: The transmission security of the N2/N3 interface between the (R)AN and core network, the N6 interface between the UPF and enterprise cloud, and the Xn interface between base stations inherits the 4G IPsec security protection solution to prevent data leakage and unauthorized tampering attacks on the transport network.

(2) Access security of external network devices: A virtual firewall or physical firewall is deployed between the NFs in the slice and the external network devices to ensure the security of the slice internal network and external network. Enterprises can also deploy intelligent firewalls to intelligently analyze and identify N4 and O&M messages. Only related data traffic can flow in and out.

(3) Edge computing security: When the UPF is deployed in the campus of industry users, the edge computing platform security, communications security, control, and supervision can be provided. High-level security can provide edge computing data security and capability exposure security as well as other security measures.

Based on the service security requirements and network structure of end users and vertical industries, slices of different levels should have different security capability combinations. The following table lists the security levels.

Table 3-5 Suggestions on 5G slice security levels

| Slice Level | Slice Security Level | Slice Security Capability (Classification Basis) | Management Security Capability | Network Protocol Security Capability | Device Resource Security Capability |
|-------------|------------------------------|---|---|--|---|
| L0 | Public network - common | Basic 5G network security | Carrier view: The security situation of the E2E 5G network is visible, and end users are unaware of it. | 3GPP basic authentication Basic privacy protection Signaling integrity protection | Resource sharing security |
| L1 | Public network - VIP | eMBB dedicated security capabilities | | 3GPP basic authentication Basic privacy protection Enhanced privacy protection over the air interface Signaling integrity protection User-plane encryption protection SBA security Slice transmission security | Resource sharing security Extranet device access security |
| L2 | Industrial network - common | Basic industry security requirements | Slice security situation awareness portal | 3GPP basic authentication Basic privacy protection Signaling integrity protection Encryption and integrity protection on the user plane | Resource reservation and sharing security Access security of external network devices Edge computing security |
| L3 | Industrial network - VIP | Advanced industry security requirements, and optional access control capabilities | Slice security situation awareness portal Security services | 3GPP basic authentication Basic privacy protection Enhanced privacy protection over the air interface Encryption and integrity protection Slice authentication/secondary authentication SBA security Slice transmission security | Resource reservation and security sharing Enterprise intelligent firewall High-level edge computing security |
| L4 | Industrial network - Special | High-level private network isolation + encryption & data processing in campuses | Slice security situation awareness portal Edge computing security Security services | 3GPP basic authentication Basic privacy protection Enhanced privacy protection over the air interface Encryption and integrity protection Slice authentication/secondary authentication SBA security Slice transmission security | Resource sharing Enterprise intelligent firewall IPsec encryption Edge computing security |

3.3 O&M Models

O&M models for Network Slicing can be divided into two scenarios based on the O&M difficulties and system openness. The following table describes the two scenarios.

Table 3-6 Network Slicing O&M scenarios

| Slice Level | Scenario | Capability Exposure Degree | Monitoring | Management |
|-------------|------------------------------|--|---|---|
| L2 | Industrial network - common | Self-service portal (KPI visualization) | View the slice status, UE information, bills, and SLA reports on the self-service portal. | N/A |
| L3 | Industrial network - VIP | Self-service portal (KPI visualization + self-service) | View the slice status, UE information, bills, and SLA reports on the self-service portal. | Self-service portal: 1. Service subscription, modification, and termination. 2. UE life cycle management (UE registration and deregistration, suspension, and resumption). 3. Simple fault diagnosis, such as real-time diagnosis, historical information association diagnosis (non-real-time diagnosis), and location service. |
| L4 | Industrial network - special | API capability exposure (KPI visualization + self-service) | Tenants use apps to monitor slice services through open APIs. | Tenants use apps to manage slice services through open APIs. |

The tenant self-service portal provides the following functions:

- 1. Network Slicing service monitoring:** The tenant self-operation portal allows tenants to monitor and view slice-related information, including:
 - Slice service information query: slice status query, slice SLA report, and other functions.
 - Slice bill query: slice bill information.
 - UE basic information query: UE status query, UE life cycle information query, UE package service query, UE group information query, and other functions.
- 2. Network Slicing service handling** The tenant self-operation portal allows tenants to perform self-service operations, including:
 - Self-service slice service handling: For example, apply for provisioning a new slice service, adjust the package content in the provisioned slice, or apply for suspending or stopping the slice service.
 - UE life cycle management: includes UE registration and deregistration, suspension and resumption, and UE service package modification.
 - Automatic service policy management: Tenants can set self-service processing policies, including message notification, service change, and data collection setting.
- 3. Network Slicing service assurance:** The tenant self-operation portal allows tenants to perform simple fault diagnosis, including:
 - Real-time diagnosis: UE information can be viewed online, and slice service faults can be diagnosed based on the real-time UE status.
 - Non-real-time diagnosis: Associated query of historical information such as UE status information and 5GC NF (for example, UDM) exposure is supported for comprehensive fault cause evaluation. Note: The specific assurance capability depends on the actual support capability of the carrier's BSS or CSMF system.
 - Location information service: The locations of UEs or UE groups can be viewed to facilitate fault diagnosis.
- 4. Network Slicing API capability exposure:** Tenants who want to develop apps by themselves can invoke the capability exposure API of the CSMF to implement all the preceding operations capabilities.
 - Monitoring capability: includes operations capability exposure and slice network data exposure. The network capabilities required by tenants can be provided by the CSMF.
 - Service handling capability: includes APIs required by tenant self-service.

Note: Suggestions on tenant selection: For small- and medium-scale tenants who want to focus on slice usage but do not want to make too much O&M investment, it is recommended that the tenant self-operation portal be preferentially selected to complete self-service or operations. For large-scale tenants who want to have more knowledge about slice services and have a large O&M budget, they can use the slice APIs to expose their own apps.

Current Network Slicing capability exposure mainly includes slice monitoring, management, and subscription. More capabilities of Network Slicing capability exposure are still under further planning and will be further enhanced based on the needs of slice tenants.

4 Suggestions on Typical Case Categories

4.1 Public Network Slicing Cases

4.1.1 Scenarios and Requirements of Public Network Slicing

In the first wave of 5G commercial use, voice and wireless Internet access are still typical user requirements. In terms of resource requirements and service assurance, these services are basically the same as 4G services. Public network common slicing can be used for deployment. In addition, new 5G consumer applications will also become prominent. According to IHS Markit, the global mobile game market will reach US\$83 billion by 2022, and cloud games may be provided to users. Cloud games have many advantages, such as a low terminal admission threshold, free from download or installation, cross-platform or cross-OS, free from terminal adaptation and optimization, and a short R&D period. Thanks to these advantages, cloud games have attracted attention from platform providers such as Microsoft, Google, Tencent, and Apple.

A prerequisite for cloud game deployment is to deliver user experience comparable to that of host games. This requires that ultra-high definition (UHD) images and videos collected on mobile phones, PCs (with 5G chips), iPad or TV screens be promptly uploaded to the game server in the cloud, and data results of computing and rendering in the cloud be pushed to mobile phones in real time. According to the following analysis, cloud games do not need to be isolated from common public network services, but have lots of customization requirements on low latency and user experience. Therefore, it is recommended that public network VIP slicing be used for deployment.

[Network requirements on network slicing for games]: Research shows that the terminal rate of HD/UHD games can reach 12.5–25 Mbit/s, and the latency of multiplayer online battle arenas (MOBAs), the latency is < 80 ms in the 4G environment, and the optimum latency is < 50 ms; in the 5G environment, the operating frame rate can be improved by relying on lower latency, so the latency requirement is lower. VR interactive games have more stringent requirements on bandwidth and latency. According to IHS Markit, VR games with 8K resolution and limited interactivity require 40–60 Mbit/s bandwidth and 20–30 ms latency.

Table 4-1 Network requirements for VR game experience (source: IHS Markit)

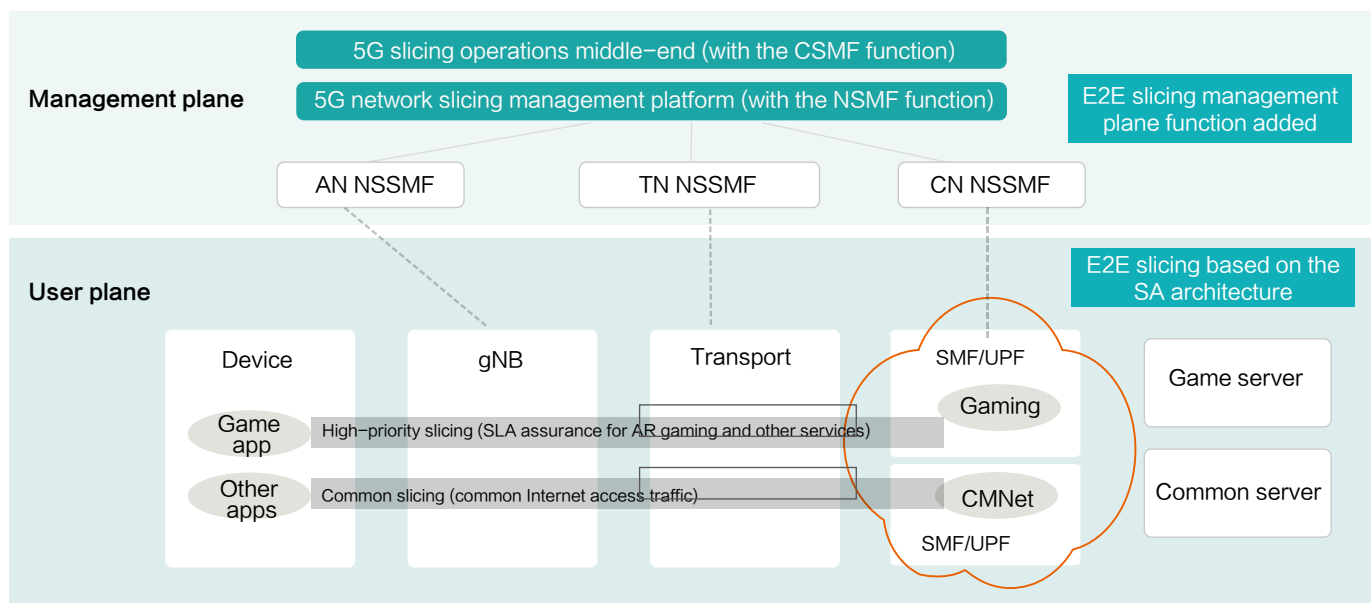
| | Basic VR Experience (Limited Interactivity) | Advanced VR Experience (Limited Interactivity) | Basic VR Experience (High Interactivity) | Advanced VR Experience (High Interactivity) |
|-----------------------|--|---|---|--|
| Resolution /Mode | 8K, 2D, 3D | 12K, 3D | 8K, 2D, 3D | 12K, 3D |
| Bandwidth required | 40– 60 Mbps | 340 Mbps | 120 – 200 Mbps | 1.4 Gbps |
| Latency required | 20 – 30 ms | 20 ms | 10 ms | 5 ms |

[Security requirements on network slicing for games]: With regard to security, the major requirements on network slicing for game acceleration are user identification and authentication.

A unique slice identifier is used to distinguish a game application from other services such as Internet access, video, and voice chat. Functional NEs are selected through 5G network slicing to selectively receive desired slicing services.

In addition to the authentication system based on the SIM card credentials of terminals, Internet entertainment applications usually have a set of user identification and authentication systems so that users can connect to service networks and the applications can be decoupled from terminals.

Figure 4-1 Slicing test networking in the 2C game scenario



4.1.2 Network Slicing Solution for Cloud Games

The 5G network slicing classification capability provides cloud game users with game acceleration services different from common Internet access services, including:

- The RAN side uses the QoS priority assurance solution to provide high-level services for game players. For professional players and esports players, RB resource reservation technology can be used to further shorten latency and improve deterministic assurance of games.
- To ensure low latency for games, the core network side can provide exclusive UPFs for game players to improve service forwarding efficiency and shorten latency.

4.2 Industry Network Slicing Cases

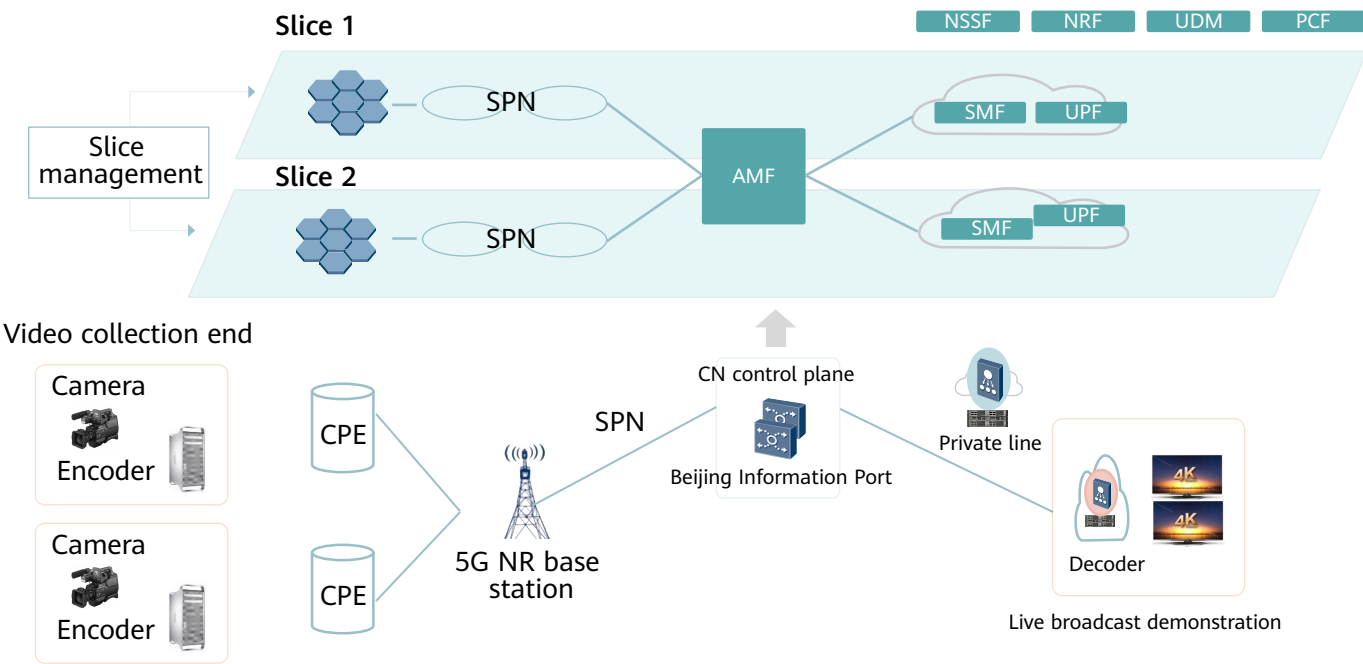
4.2.1 Scenarios and Requirements of Industry Network Slicing

Compared with common public network services, enterprise communications services have distinct industry characteristics. However, it is infeasible for many enterprises to build their own private networks. First, they lack infrastructure, capital, and frequency bands required for building private networks. Second, private networks can hardly meet continuous network coverage requirements of Internet of Vehicles (IoV) and UHD videos in a short period of time. Therefore, common industry slicing based on carriers' public networks will play an important role in future commercial use of 5G. The following uses UHD videos as an example to describe typical common industry slicing deployment.

Typical 4K UHD videos feature 3840x2160 resolution, high frame rate, high color depth, wide color gamut (WCG), high dynamic range (HDR), and panoramic sound, bringing immersive experience to audience. Video backhaul is a key part of UHD live content production. The bandwidth and frame rate of 4K videos are usually higher than 40 Mbit/s and 50 frames per second (FPS) respectively, posing higher requirements on the backhaul rate, latency, and jitter. Currently, satellite and Internet private lines can basically meet the transmission of one-channel 4K signals. However, 4K/8K videos (> 100 FPS) or backhaul of multi-channel UHD signals requires ultra-high bandwidth and VIP slicing solutions with better assurance.

UHD live broadcast will also stimulate the innovation of media operations modes such as VR "secondary site". According to IHS Markit, China's VR "secondary site" market will reach US\$1.8 billion by 2025. However, it is time-consuming and labor-intensive to deploy a private network for the secondary site, and the network utilization is low during non-performance periods. Therefore, it is more suitable to use common industry slicing. VR content has higher requirements on transmission bandwidth. E2E latency must be strictly controlled for the secondary site with bidirectional interactions. Therefore, network slicing must be deployed close to the site. In terms of service operations, secondary site slice tenants require flexible configuration and automatic provisioning to cover markets such as sports events, commercial performance, and entertainment themes if possible.

4.2.2 Network Slicing Solution for UHD Live Broadcast Backhaul



- With network slicing for UHD live broadcast, QoS priority scheduling can be performed based on service requirements on the RAN side to ensure the quality of backhaul signals. In some major national events, large celebrations, and sports events, RB resources need to be reserved to ensure the transmission quality of 4K/8K live broadcast signals.
- On the transport network side, channelized sub-interfaces with HQoS scheduling or packet switching can ensure uninterrupted transmission of live broadcast signals.
- The core network side can also allocate logically exclusive SMFs and UPFs for UHD live broadcast channels.

4.3 Network Slicing Cases for Special Industries

4.3.1 Network Slicing Scenarios and Requirements in Special Industries

The deployment of an intelligent power grid with green, secure, reliable, and efficient as the targets involves multiple 5G slicing service scenarios, including:

eMBB services implement monitoring of transmission lines, substations, and emergency sites in real time through HD videos. In these scenarios, multiple channels are required.

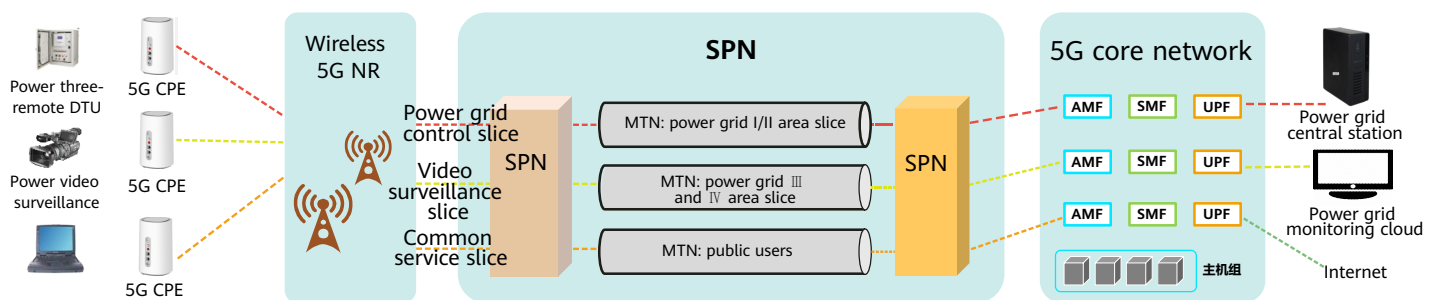
URLLC services, which are mainly power grid control services, include relay protection, precise load control, three remotes (remote monitoring, remote communication, and remote control), synchronous phasor measurement, and other latency-sensitive services.

mMTC services, including power consumption information collection and advanced metering, use numerous electric measurement terminals to collect power consumption information in minutes to meet the requirements for intelligent power consumption and service customization.

To handle the preceding customized services and meet the special requirements of the power grid for security, data isolation, and service control, it is recommended that network slicing be deployed for special industries.

4.3.2 Network Slicing Solution for Power Grids

Figure 4-3 Network slicing solution for power grids










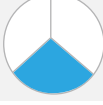

This figure shows a three-layer network solution for power grid slicing. The control slice carries the power production service, such as differential protection, precision load control, and three remotes (remote monitoring, remote communication, and remote control). The power terminal device accesses the 5G network through 5G CPEs. The egress switch of the 5G core network is configured to connect the switch to the master station system of power distribution automation. Network slicing is used for E2E isolation between control services, information collection services (power III/IV area services) services, and mobile application services.

- Slice access subnet: Scheduling priorities are configured based on slices and 5QI values. For the control services' slice, the 5QI value is X. For the information collection services' slice, the 5QI value is Y. For the mobile application services' slice, the 5QI value is Z. With the ever-increasing power control requirements, independent frequencies can be assigned to ensure the power distribution service.
- Slice transport subnet: Three FlexE pipes are configured on the transmission side. Slice identifiers are mapped to VLANs to transmit data over different FlexE pipes.
- Core network slicing: Three slices are allocated with independent AMF, UPF, and SMF to achieve complete isolation.

5 Cost Analysis

The following table describes the cost analysis for 5G network slicing from the perspectives of SLA assurance, exclusive resource use, and tenant self-operations based on differentiated requirements of various industries and users.

Table 5-1 Network Slicing cost analysis

| Slice Level | Name | Network Slicing SLA | Exclusive Resource Use | Tenant Self-Service OAM | Overall Cost |
|-------------|------------------------------|---|---|---|---|
| L0 | Public network - common | NA | NA | NA | NA |
| L1 | Public network - VIP |  | NA | NA |  |
| L2 | Industrial network - common |  |  |  |  |
| L3 | Industrial network - VIP |  |  |  |  |
| L4 | Industrial network - Special |  |  |  |  |

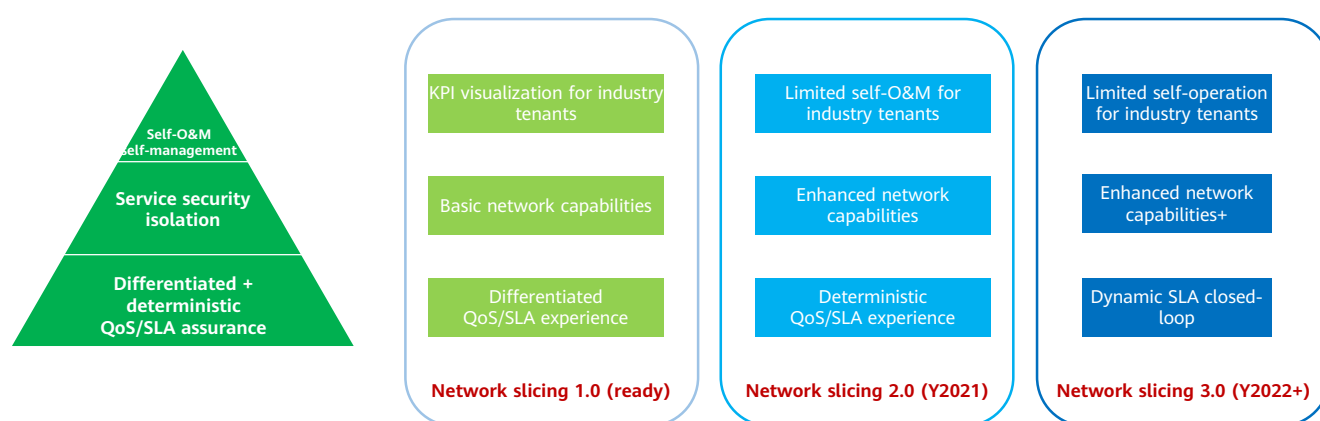
The overall costs are illustrated based on the proportions of different Network Slicing levels. It can be seen that the network costs of an operator are increased each time a network capability is added, which greatly affects the final pricing of a Network Slicing.

6 Industry Application Suggestions

Similar to the evolution of 3GPP Release 15, Release 16, and Release 17, the E2E network slicing solution cannot be achieved overnight. Instead, it is iterative and stepwise. In addition, different Network Slicing provide different service levels and cause different network costs. Therefore, it is wise for customers in different industries to customize the most appropriate Network Slicing based on their application scenarios and requirements. Operators should avoid excessive demand for the highest level of service.

Based on the three core capabilities (isolation, SLA/QoS assurance, and slice OAM of 5G Network Slicing) and the matching between standard technology readiness and the original requirements of industry customers, 5G network slicing goes through the following phases in the industry.

Figure 6-1 5G Network Slicing phases in the industry



Phase 1 (ready): As mentioned above, the 5G transport network and 5G core network support different software-based and hardware-based isolation solutions. On the 5G NR side, 5QIs (QoS scheduling mechanism) are mainly used to achieve software-based isolation in WAN scenarios. Alternatively, campus-specific 5G NR (including micro base stations and indoor distributed base stations) is used to implement hardware-based isolation in LAN scenarios. In terms of service experience assurance, 5QIs are used to implement differentiated SLA assurance between slices. In terms of slice OAM capabilities, E2E KPIs can be managed in a visualized manner. This means that from 2020 on, Huawei is ready to deliver commercial use of E2E slicing for common customers and VIP customers of the public network and common customer of general industries (such as UHD live broadcast and AR advertisement).

Phase 2 (to be ready in 2021): In terms of isolation, the 5G NR side supports the wireless RB resource reservation technology (including the static reservation and dynamic reservation modes) to implement E2E network resource isolation and slicing in WAN scenarios. In terms of service experience assurance, features such as 5G LAN and 5G TSN are enhanced to implement differentiated and deterministic SLA assurance between different slices. In terms of slice OAM, on the basis of tenant-level KPI visualization, the limited self-service of the industry for rented slices can be further supported. In this phase, operators can serve VIP customers in common industries (such as AR/VR cloud games and drone inspection), dedicated industry customers (such as electric power management information region, medical hospital campus, and industrial campus), and dedicated industry customers (such as electric power production control region and public security).

Phase 3 (to be ready after 2022): In this phase, 5G network slicing supports real dynamic closed-loop SLAs based on AI and negative feedback mechanism, implementing network self-optimization and better serving industries (such as 5G V2X) with high requirements on mobility, roaming, and service continuity. In addition, industry-oriented comprehensive service capabilities will be further enhanced and evolved.

7 Summary and Prospect

Network slicing is a landmark 5G technology. It provides differentiated network capabilities to meet different network requirements of public networks and industry users. It provides different combinations of network capabilities for different industries and scenarios. Therefore, it is critical for network slicing service providers and consumers to unify the classifications and definitions of network capabilities and resource capabilities at different levels.

This white paper defines five Network Slicing levels based on the analysis of different capabilities of the wireless, transport, and core networks, as well as security and operation capabilities. The five Network Slicing levels correspond to different application scenarios of public networks, common industries, and dedicated industries. This white paper provides cost analysis in terms of quality assurance, resource occupation, and network O&M. In this way, the network slicing technology can be more intuitively understood and used by public network customers, vertical industry customers, operators, and device vendors. These Network Slicing levels can be used as a basic template for operators to design and package Network Slicing offerings. In addition, the overall view of Network Slicing offerings and the comparison between Network Slicing can be provided for users, promoting the commercialization of the Network Slicing industry and providing reliable reference for Network Slicing application and promotion.

8 Appendixes

Appendix: Acronyms and Abbreviations

NFV: network functions virtualization

SBA: service based architecture

NFVI: network functions virtualization infrastructure

NF/VNF: network functions/virtual network functions

AMF: access and mobility function

SMF: session management function

UPF: user plane function

UDM: unified data management

PCF: policy control function

NSMF: Network Slicing management function

O&M: operation and maintenance

SPN: Slicing Packet Network

MTN: Metro Transport Network