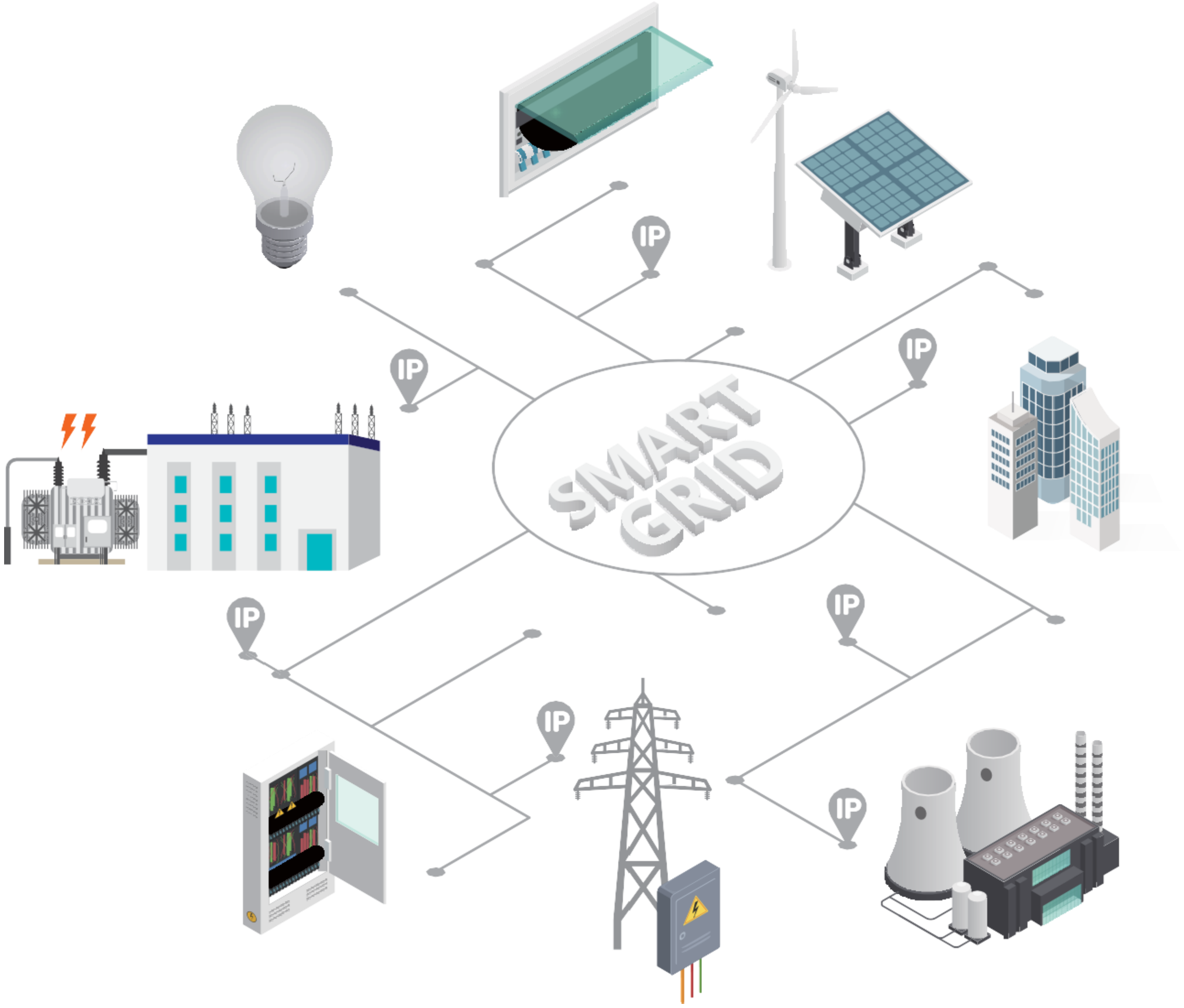
Technical White Paper on the FlexE-based Relay Protection Service Bearer Solution



HUAWEI TECHNOLOGIES CO., LTD.

About This Document

This document describes how to use the innovative FlexE technology to transmit relay protection services (mission-critical services in power grids) and meet the requirements of low latency, low jitter, and two-way latency consistency during the IP-based evolution of smart grids. Through analysis, modeling, and testing, this document fully demonstrates how FlexE provides independent hard pipes for relay protection services and solves the problem that the latency and jitter in case of blocking caused by long packets do not meet service requirements when the traditional hierarchical quality of service (HQoS) technology is used. The FlexE technology fully meets the bearer requirements of relay protection services and paves the way for the evolution of smart grids from traditional SDH to all-IP, ensuring grid security and reducing power outage risks.

Authors:

Ma Li:
Huawei Utility Industry Datacom
System Architect

Zou Yuquan:
Huawei Utility Industry Solution
Planning Expert

Zhou Yun:
Huawei Utility Industry Datacom
System Architect

Li Yu:
Huawei Utility Industry Datacom
System Architect

Contents

01 Smart Grid Development Towards IP

Smart grids have become a focal point for the development of the electric power industry. As such, countries around the world are formulating plans and policies to accelerate the development of smart grid technologies and the industry. Leveraging advanced ICT technologies, smart grids build reliable, high-speed, and two-way communication channels. Smart grids also employ sensing and measurement technologies and devices, as well as control methods, to ensure secure, economical, efficient, and eco-friendly operations.

With the construction of smart grids and digital substations, services, such as supervisory control and data acquisition (SCADA) and dispatch phone services are gradually becoming IP-based. As well as this, new services, such as wide area measurement system (WAMS) and wide area protection services are being continuously introduced. At the same time, power grids are seeing the large-scale emergence of new energy services, such as distributed power generation, energy storage, and charging pile services, while high-bandwidth services such as video surveillance continue to grow. With so many evolving and newly emerging technologies, traditional communication networks are unable to meet the requirements of smart grids. Instead, intelligent IP networks are required. Intelligent IP networks, unlike traditional communication networks, can provide a reliable, flexible, and simple connection platform for smart grids, and have now become the ideal choice for electric power enterprises during the construction of next-generation electric power communication networks.

Traditional services, including relay protection, SCADA, electric energy metering, and dispatch phone services, require low bandwidth, high reliability, and real-time performance. Traditional communication networks are constructed mainly based on circuit switching SDH technologies. When an electric power company evolves the network to IP, the IP network must be intelligent and able to reliably carry mission-critical services, such as relay protection and SCADA services. In particular, relay protection services, especially the optical fiber differential protection services for power transmission lines, have high requirements on the communication latency, jitter, and two-way latency variation. Intelligent IP networks must be able to reliably bear the optical fiber differential protection services for power transmission lines.

02 Requirements of Relay Protection Services for Communication Networks

2.1 Introduction to Relay Protection Services

Power systems consist of power generation, transformation, transmission, distribution, and consumption. With power supply covering all aspects of social production and life, the security and reliability of power grids are critical. And the 'aorta' of power grids is formed by high-voltage power transmission lines linking power generation, transformation, distribution, and consumption. These lines cover a wide range of areas, such as cities, mountains, rivers, and straits. Such wide-spread distribution means that they are vulnerable to natural disasters, human activities, and harsh weather conditions and environments, which may lead to faults. Fast fault detection and automatic fault isolation are implemented using relay protection, which acts as the power system's first line of defense. Relay protection is used to ensure power grid security and limit the scope of the fault.

Relay protection includes power transmission line protection and primary device (such as generators, transformers, and busbars) protection. Primary device protection is intra-substation protection in which only local collection and calculation are required and there is no requirement for long-distance communication. Power transmission line protection, on the other hand, can be further broken down into overcurrent protection and pilot protection based on protection rules. Examples of pilot protection include distance protection and optical fiber differential protection, with the latter featuring short operation time, accurate fault determination, small protection dead zone, and effective protection against incorrect tripping. Optical fiber differential protection meets the requirements of relay protection for being fast in operation, efficient, and sensitive. As long as there are optical fiber communication channels available, optical fiber differential protection is recommended as the primary protection for power transmission lines. According to Kirchhoff's law, optical fiber differential protection for power transmission lines requires that protection relays at both ends of the lines transmit synchronous sampling data to each other and determine the current difference between the two ends in real time. Given this, it has especially high requirements for real-time and reliable communication. Taking all of this into account, this document mainly analyzes and verifies the feasibility of using IP networks to carry services of optical fiber differential protection for power transmission lines.

2.2 Network Requirements of Relay Protection Services

Optical fiber differential protection for power transmission lines (hereinafter referred to as relay protection) is implemented by directly connecting optical fibers or using a communication network. The communication network used to carry relay protection services has very high requirements on the latency, jitter, and two-way latency consistency.

Protection relays connect to the communication network through low-speed interfaces, such as C37.94, G.703 64K, and X.21 interfaces. Currently, most network vendors use pulse code modulation (PCM) converters to convert these low-speed interfaces into E1 interfaces for network access, or integrate these low-speed interfaces into network devices.

Protection relays at both ends of a power transmission line need to synchronously sample their current values. Currently, there are two mainstream synchronous sampling solutions. External clock solution: Protection relays at both ends access the same high-precision external clock source (such as the GPS clock or IEEE 1588v2 network clock source) to implement synchronous sampling. The disadvantage of this solution is that relay protection depends on the reliability of the clock source, and therefore a clock system fault may present system risks. Internal clock solution: The clock of the protection relay on one side of the power transmission line is used as the reference. The protection relay on the other side uses the ping-pong algorithm (shown in Figure 2-1) to determine the channel latency and uses the internal latency compensation mechanism to implement synchronous sampling.

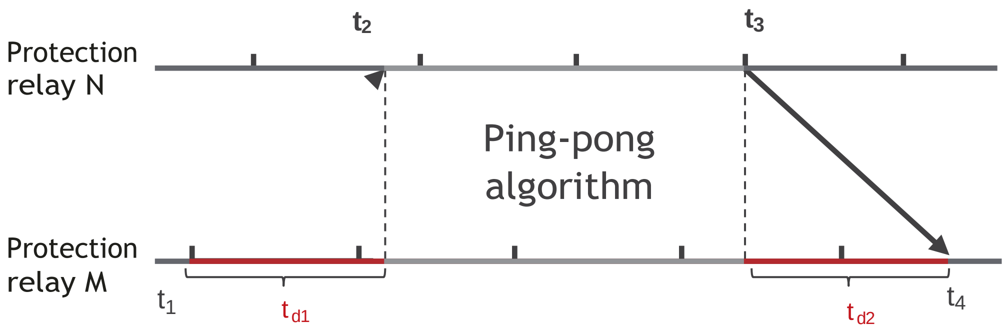


Figure 2-1 Fundamentals of the ping-pong algorithm

Protection relay M sends a data packet with the current timestamp t_1 to protection relay N, which receives the data packet at t_2. After performing data processing, protection relay N sends a data packet with t_2, t_3, and t_1 to protection relay M. After receiving the data packet at t_4, protection relay M calculates the path latency using the following formula:

$$T\_latency = (t_{d1} + t_{d2}) = (t_2 - t_1)+(t_4 - t_3)$$

The ping-pong algorithm considers that the two-way latencies are the same by default, and there are therefore strict requirements on the network jitter and two-way latency variation. When the system frequency is 50 Hz and the power cycle is 20 ms, the phase angle difference ω corresponding to 1 ms is 18°. The current value sampling angle difference is calculated as follows:

$$\theta = \omega \triangle t = \omega \text{ x } \frac{t_{d2} - t_{d1}}{2}$$

The error current generated by the current value sampling angle difference is set to I_d. The current sampling values on protection relays M and N are set to I. The current sampling value difference of relay protection services is calculated as follows:

$$\frac{I_d}{I} = 2 \text{ x } \sin\left(\frac{\theta}{2}\right) = 2 \text{ x } \sin\left(\frac{\omega \triangle t}{2}\right) = 2 \text{ x } \sin\left(\omega \text{ x } \frac{t_{d2} - t_{d1}}{4}\right)$$

The protection setting difference is generally less than 5%, and so the current sampling value difference I_d/I must be less than or equal to 5%. According to the preceding formula, $|t_{d2} - t_{d1}|$ is less than or equal to 318 μs. Given this, the thresholds for the jitter and two-way latency variation of the communication network can be set to 200 μs.

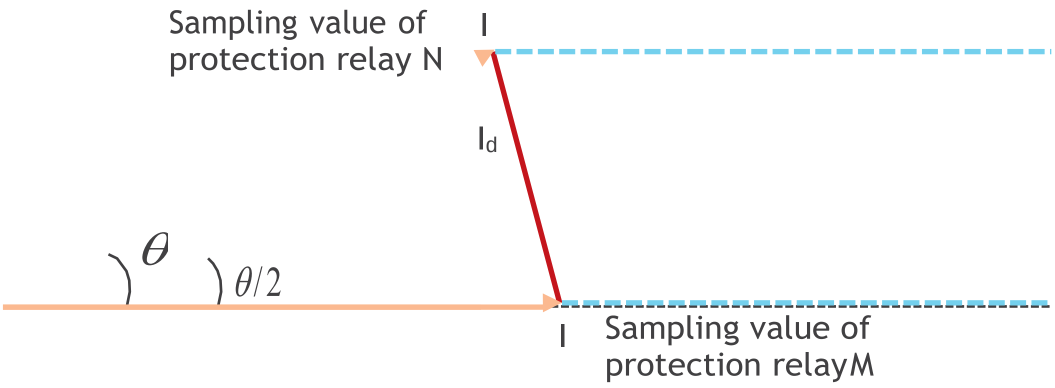


Figure 2-2 Current sampling value difference

The protection relays at both ends perform time compensation on received data packets based on the latency calculated using the ping-pong algorithm, and then compare the corresponding sampling values.

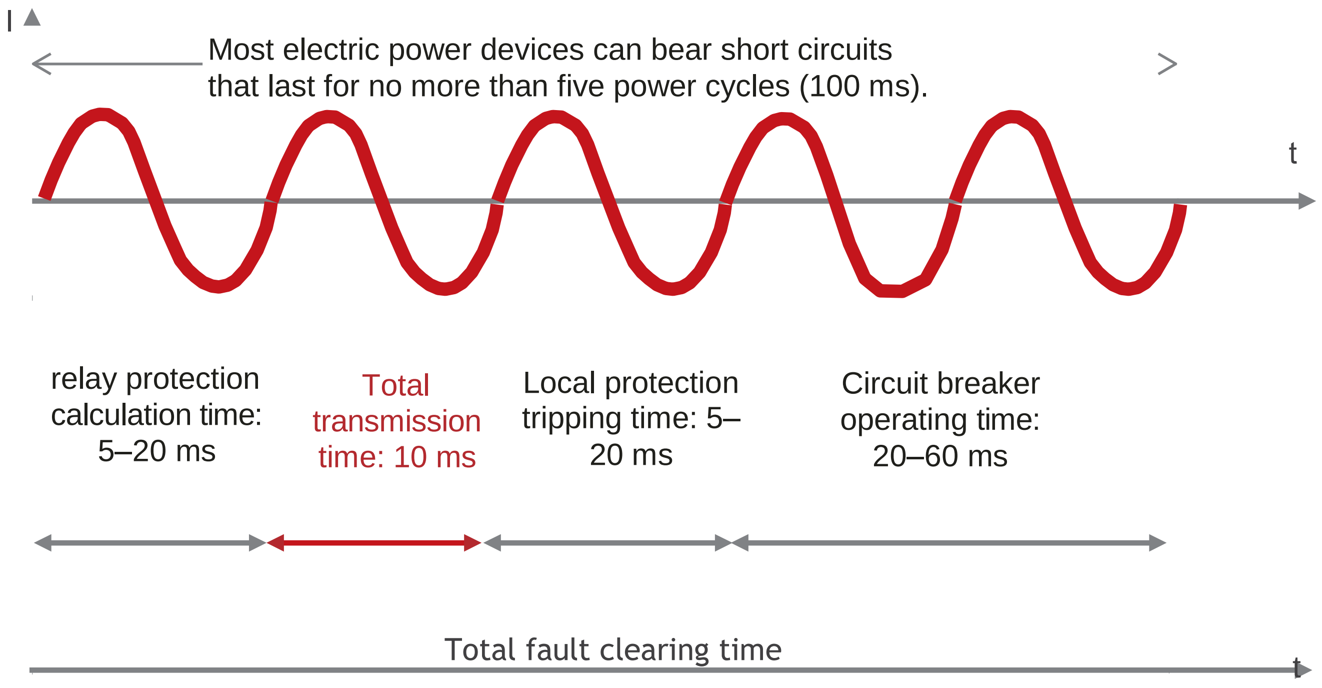

I
Most electric power devices can bear short circuits that last for no more than five power cycles (100 ms).
t
relay protection calculation time: 5–20 ms
Total transmission time: 10 ms
Local protection tripping time: 5–20 ms
Circuit breaker operating time: 20–60 ms
Total fault clearing time
t

Figure 2-3 Latency requirements of relay protection services

In addition, different relay protection vendors and electric power companies have different standards for the end-to-end latency of the communication network to ensure that relay protection is fast in operation. To ensure that faults are cleared on the power transmission line within 100 ms, the total transmission time of the communication network must be within 5 ms to 10 ms (after subtracting the inherent operating time of the circuit breaker and the time for collecting, processing, and determining data of the protection relay). The latency on the communication network affects the time of the relay protection action. Reducing the latency can ensure that relay protection is fast in operation, thereby reducing the fault clearing time of the power system.

Table 2-1 shows the requirements of relay protection services on the latency, jitter, and two-way latency variation of the communication network.

Table 2-1 Requirements of relay protection services for communication networks

Communication Latency	Jitter	Two-Way Latency Variation
5-10 ms	≤ 200 μs	≤ 200 μs

03 Challenges Facing Traditional IP Networks in Carrying Relay Protection Services

3.1 Current IP Bearer Solution for Relay Protection Services

Protection relays require low-speed interfaces, such as C37.94, G.703 64K, and X.21 interfaces on the communication network. Traditionally, PCM converters are used to convert low-speed interfaces into E1 interfaces for relay protection services to access the communication network. Currently, Huawei intelligent IP network supports multiple relay protection service interfaces. Without external PCM converters, relay protection services can directly access the intelligent IP network. Figure 3-1 shows the networking for relay protection services carried on an IP network.

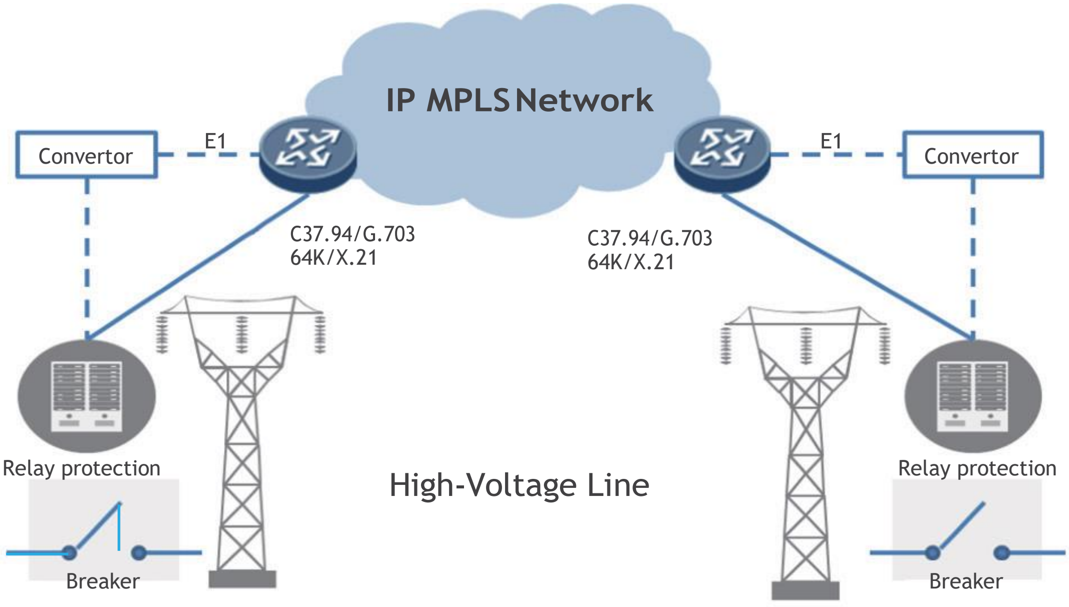


Figure 3-1 Networking for relay protection services carried on an IP network

3.1.1 Relay Protection Service Emulation

Currently, relay protection services are mainly carried on TDM networks, which transmit data flows. In contrast, IP networks transmit data packets. For this reason, TDM services must be first emulated as IP packets before being transmitted over an IP network. To achieve this, the time division multiplexing over packet switched network (TDMoPSN) technology must be used. TDMoPSN supports two mainstream protocols: Structure-Agnos tic Time Division Multiplexing over Packet (SAToP) and Structure-Aware TDM Circuit Emulation Service over Packet Switched Network (CESoPSN). Figure 3-2 shows the TDMoPSN frame format.

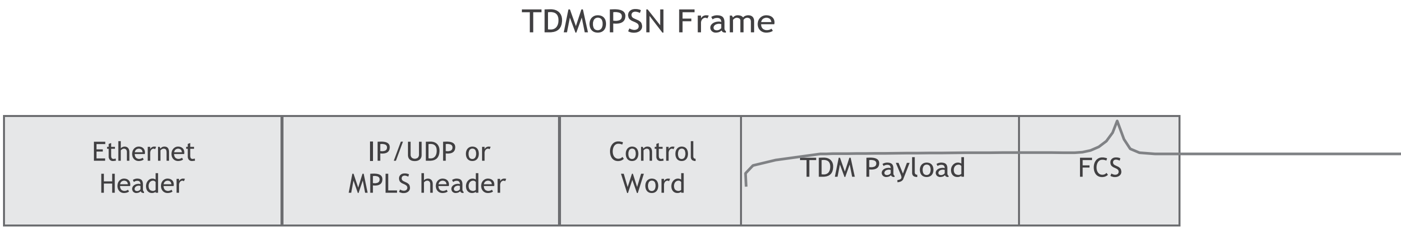


Figure 3-2 TDMoPSN frame format

SAToP implements emulation for low-speed plesiochronous digital hierarchy (PDH) circuit services. Specifically, it transmits structure-agnostic or unframed E1, T1, E3, and T3 services by segmenting TDM services into serial bit streams, encapsulating the bit streams, and transmitting the bit streams on Pseudowire Emulation Edge-to-Edge (PWE3) channels. PWE3 is a Layer 2 service bearer technology that emulates Ethernet, TDM, and ATM services on a PSN. With PWE3, various Layer 2 services on customer edges (CEs) are emulated and transparently transmitted over the PSN through PWE3 channels between provider edges (PEs). CESoPSN implements emulation for low-speed PDH circuit services, such as E1 services. Where CESoPSN differs from SAToP is that it provides structure-aware emulation and transmission of TDM services. That is, framed services and signaling in the TDM frame can be identified and transmitted.

After receiving a relay protection (TDM) data flow, an ingress PE on an IP MPLS network encapsulates the data flow as IP data packets, and transmits these data packets to an egress PE through a PWE3 channel. After receiving the IP data packets, the egress PE converts them back to the TDM data flow. Due to network jitter, the packets sent to the egress PE over the PSN may arrive out of order. To address this issue, the jitter buffer technology can be used to regulate the arrival intervals of PWE3 packets and rearrange out-of-order packets, thereby ensuring that the TDM data flow can be rebuilt on the egress PE. A large-capacity jitter buffer can compensate for significant jitter, but this may lead to high latency. Therefore, a jitter buffer of 1000 μs to 2000 μs is recommended.

When relay protection services are rebuilt, clock synchronization must be ensured for input/output services on uplink and downlink devices. This is because relay protection services require data to be transmitted at a constant speed. The clock source of a protection relay can be an external or internal clock, while an external clock is generally used to obtain frequency synchronization information from the network side.

3.1.2 Static Bidirectional Co-Routed LSP

The ping-pong algorithm is used to calculate the link latency for relay protection services. By default, the algorithm considers the latencies in two directions to be the same, whereas, in actual fact, they differ. To ensure low latency variation in two directions, you can use static bidirectional co-routed LSPs of MPLS TE tunnels to ensure consistent round-trip paths.

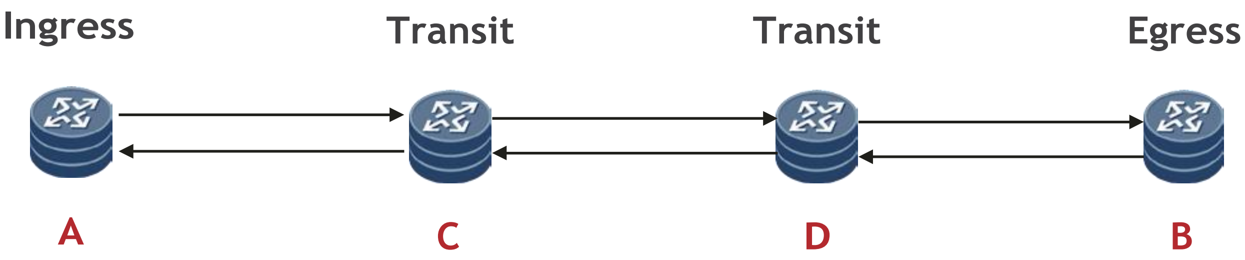


Figure 3-3 Networking for static bidirectional co-routed LSPs

In Figure 3-3, T_latency (A-B) is the latency in transmitting packets from A to B, and T_latency (B-A) is the latency in transmitting packets from B to A. The latencies in the two directions are calculated as follows:

T_latency (A-B) = Ingress_latency (A) + Transit_latency (A, C, D, B) + Egress _latency (B)

T_latency (B-A) = Ingress_latency (B) + Transit_latency (B, D, C, A) + Egress_latency (A)

The encapsulation interval on the ingress is configurable, with a minimum value of 125 μs. Given this, the difference between Ingress_latency (A) and Ingress_latency (B) can be controlled. Egress_latency (A) and Egress_latency (B) can also be set to the same value. As the ingress and egress latencies are configurable, the final two-way latency variation is mostly subject to Transit_latency (A, C, D, B) and Transit_latency (B, D, C, A). That is, the variation depends on the packet forwarding latency difference (jitter) of all hops. Static bidirectional co-routed LSPs of MPLS TE tunnels can be used to prevent the two-way latency variation that occurs when round-trip paths are different.

3.2 Challenges Faced by the Current IP Bearer Solution

In the traditional IP bearer solution, HQoS is used to ensure that high-priority services such as relay protection services are preferentially forwarded on the network. As long as the network is lightly loaded, the service priority can be ensured. However, if network congestion occurs, there may be severe network latency and two-way latency variation, failing to meet the requirements of relay protection services.

IP networks forward services using the statistical multiplexing technology with higher efficiency, which is vastly different from the time division multiplexing technology used by the SDH network. With the statistical multiplexing technology, a deterministic latency in service transmission becomes a random latency. Also, high- and low-priority services share the same physical outbound interface on a router. So, when a low-priority packet is being transmitted by the outbound interface, high-priority packets need to wait until it is transmitted. This is called head-of-line (HOL) blocking, and it leads to a randomness in waiting time, which in turn causes different latency variations for different nodes. In this case, even if label switching-based Layer 2.5 packet switching is used, the synchronization of the services at the transmit and receive ends cannot be ensured when the path is determined.

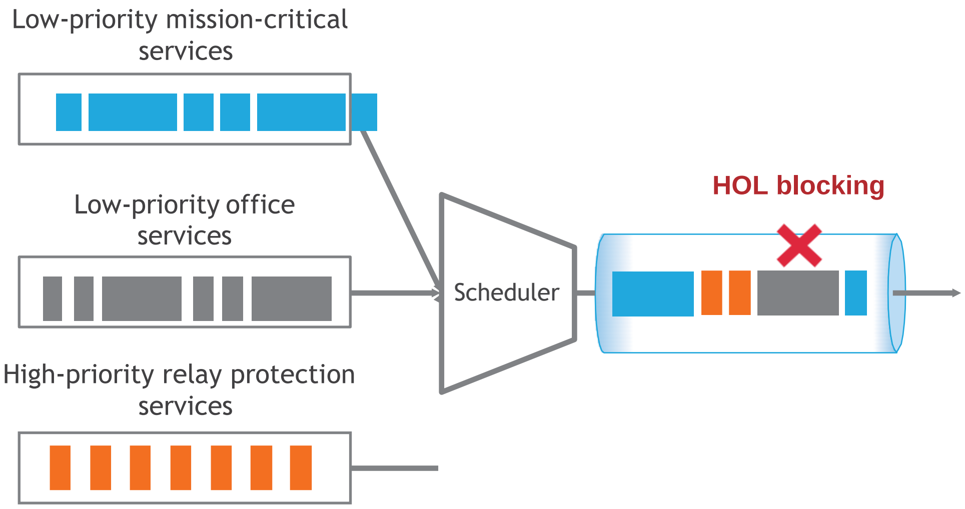

Low-priority mission-critical services
Low-priority office services
High-priority relay protection services
Scheduler
HOL blocking

Figure 3-4 HOL blocking

To resolve the problem that the two-way latency variation of relay protection services is excessively large due to the jitter on the packet network, the asymmetric latency compensation technology has been developed. This technology can be used to adjust the two-way latency variation of the relay protection services by collecting and adjusting the dwell time of packets in the jitter buffer on the egress, and is suitable for the scenario where the network is lightly loaded and the average latencies of bidirectional service packets are similar. However, adjusting the jitter buffer is not a feasible way to adjust the two-way latency variation if the network is congested, especially if bidirectional congestion is inconsistent (for example, the network is lightly loaded in one direction and congested in the other direction, resulting in inconsistent average latencies of bidirectional service packets). As a result, the asymmetric latency compensation technology cannot ensure that the two-way latency variation meets the requirements of relay protection services in this case.

04 FlexE Technology Overview

4.1 Background

Based on high-speed Ethernet interfaces, Flexible Ethernet (FlexE) is a cost-efficient carrier-grade interface technology that provides high reliability and dynamic configuration through decoupling of the Ethernet Media Access Control (MAC) and physical (PHY) layers. Leveraging the most widely used and powerful Ethernet ecosystem, FlexE addresses the challenges in developing services such as video streaming, cloud computing, and 5G, drawing wide attention from the industry since it was first proposed in 2015.

With the rise of cloud computing, video, and mobile communication services, requirements on IP networks are no longer focused on bandwidth. Instead, the focus has shifted to service experience, service quality, and networking efficiency. Given this, Ethernet, as the underlying connection technology, needs to maintain its existing advantages of cost-efficiency, high reliability, and easy O&M, in addition to developing new capabilities such as multi-granularity rate and flexible bandwidth adjustment, as well as enhanced QoS capabilities for multi-service bearing. The end goal for high-speed Ethernet technologies is to enhance user experience in multi-service bearer scenarios. One way to achieve this i s for Ethernet to provide channelized hardware isolation on physical-layer interfaces, thereby allowing services to be isolated by slicing at the physical layer. In addition, in combination with high-performance programmable forwarding and HQoS scheduling, Ethernet can work with upper-layer networks or applications to enhance QoS capabilities in multi-service bearer scenarios. To achieve this, FlexE was developed.

4.2 Technical Implementation of FlexE

Based on IEEE 802.3, FlexE introduces the FlexE shim layer to decouple the MAC and PHY layers (as shown in Figure 4-1), achieving flexible rate matching.

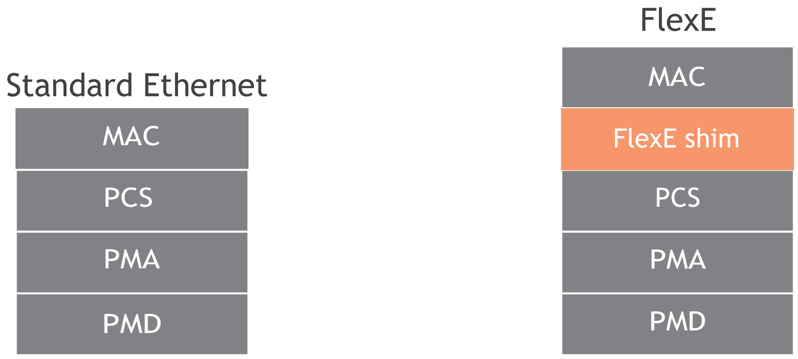


Figure 4-1 Structures of standard Ethernet and FlexE

FlexE uses the client/group architecture, in which multiple FlexE clients can be mapped to a FlexE group for transmission, implementing bonding, channelization, sub-rating, and other functions. The following describes the related concepts:

- FlexE client: an Ethernet data flow based on a MAC data rate that may or may not correspond to any Ethernet PHY rate. FlexE clients correspond to various user interfaces that function in the same way as traditional service interfaces on existing IP/Ethernet networks. FlexE clients can be configured flexibly to meet specific bandwidth requirements. They support Ethernet MAC data flows of various rates (including 10 Gbit/s, 40 Gbit/s, N x 25 Gbit/s, and even non-standard rates), and the Ethernet MAC data flows are transmitted to the FlexE shim layer as 64B-/66B-encoded bit streams.
- FlexE shim: a layer that maps or demaps the FlexE clients carried over a FlexE group. It decouples the MAC and PHY layers and implements key functions of FlexE through the calendar slot distribution mechanism.
- FlexE group: a group composed of IEEE 802.3-defined Ethernet PHYs. Because FlexE inherits IEEE 802.3-defined Ethernet technology, the FlexE architecture provides enhanced functions based on exist- ing Ethernet MAC and PHY rates.

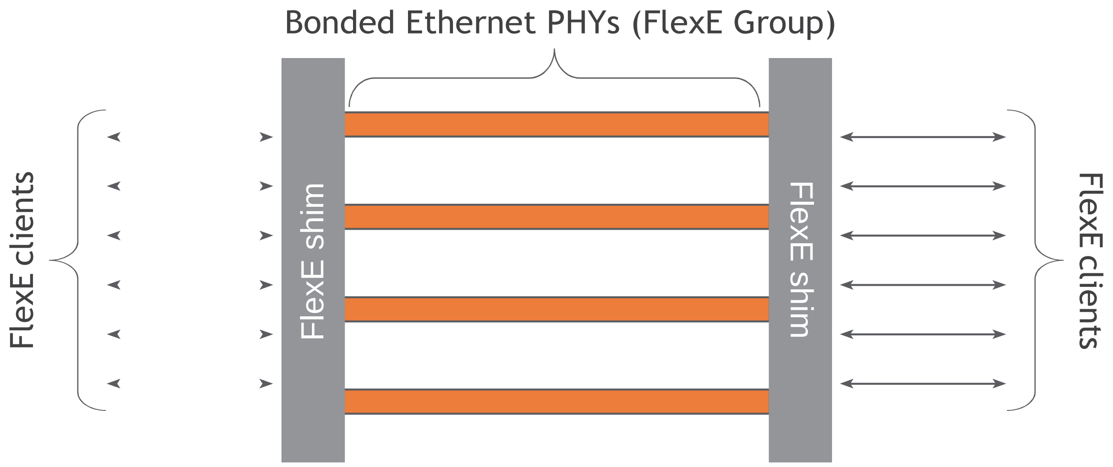


Figure 4-2 General architecture of FlexE

The FlexE shim layer implements the core functions of FlexE. It partitions each 100-Gbit/s PHY in a FlexE group into a group, called a sub-calendar, of 20-slot data channels. The sub-calendar provides 5-Gbit/s bandwidth per slot. Ethernet frames of FlexE clients are partitioned into 64B/66B blocks, which are distributed to multiple PHYs of a FlexE group based on slots through the FlexE shim layer.

According to Optical Interworking Forum (OIF) FlexE standards, the bandwidth of each FlexE client can be set to 10 Gbit/s, 40 Gbit/s, or N x 25 Gbit/s. The bandwidth of each slot of a 100GE PHY in a FlexE group is 5 Gbit/s, and a FlexE client can theoretically support multiple rates through different combinations of these slots.

The calendar mechanism enables the FlexE shim to map and carry FlexE clients with different rates in a FlexE group and to allocate bandwidth to these clients. Depending on the bandwidth required by each FlexE client and the distribution of slots in each PHY, FlexE allocates available slots in a FlexE group, mapping each client to one or more slots. FlexE then uses the calendar mechanism to enable a FlexE group to carry one or more FlexE clients. Each 64B-/66B-encoded block in a FlexE client is carried over a slot (a basic logical unit carrying the 64B/66B block), as shown in Figure 4-3. In the calendar mechanism, FlexE uses every 20 blocks (slots 0 to 19) as a logical unit. In addition, it uses the 1023 repetitions of the calendar between blocks as a calendar component. The calendar components are distributed into slots in a specified order to form a data bearer channel with a granularity of 5 Gbit/s.

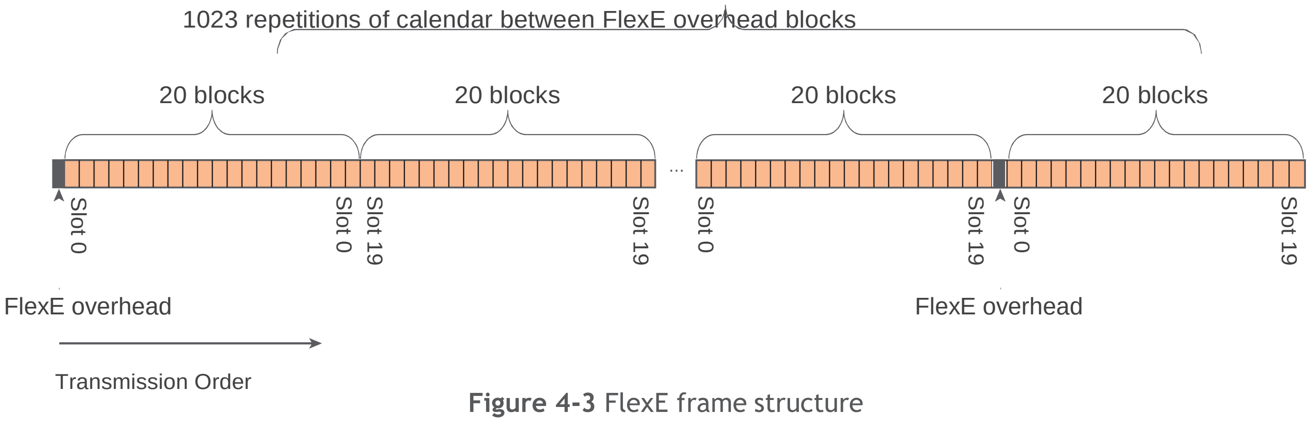


Figure 4-3 FlexE frame structure

Overhead frames and multiframes are defined for the FlexE shim layer to represent slot mappings and implement the calendar mechanism. The FlexE shim layer provides inband management channels through overhead, allowing configuration and management information to be transmitted between two interconnected FlexE interfaces to automatically set up links through autonegotiation. Specifically, one overhead multiframe consists of 32 overhead frames, each of which contains eight overhead slots, depicted by black blocks in Figure 4-3. After every 1023 repetitions of 20 blocks, there is an overhead slot, which is a 64B/66B block. Overhead slots have different fields, and an ordered set with block type code 0x4B and O code 0x5 marks the first block of an overhead frame. During information transmission, the first overhead frame is determined between two interconnected FlexE interfaces by matching a control character and an "O Code" character. In this way, the two interfaces establish a management information channel independent of a data channel of the green slot in Figure 4-4 and are then able to implement for the transmission configuration information. For example, after a FlexE client's information (such as the slot mapping and position information of a data channel in the FlexE shim or group) is sent, the receive end can restore the FlexE client based on this information. FlexE inband management also allows interconnected interfaces to exchange link state information and OAM information, such as remote PHY fault (RPF) information.

FlexE also achieves dynamic bandwidth adjustment for clients by allowing slot/calendar configurations to be modified. To reflect FlexE client mappings in a FlexE group, interconnected interfaces use an overhead management channel to transmit two types of calendar configurations (A and B configurations, represented by "0" and "1", respectively), which can be dynamically switched between one another to achieve bandwidth adjustment. Because a FlexE client may have different bandwidth values in A and B calendar configurations, configuration type switching can work with system application control, implementing seamless bandwidth adjustment. The overhead management channel provides a request/acknowledge mechanism for switching between the two configuration types.

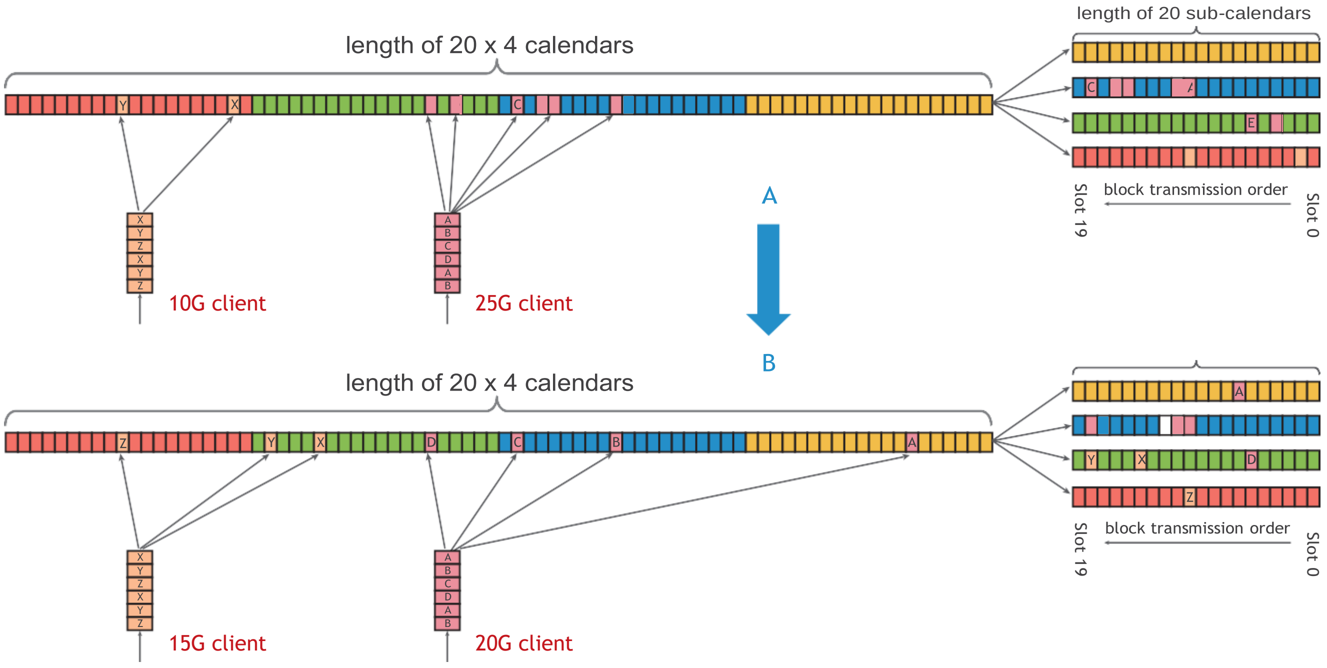


Figure 4-4 Bandwidth adjustment through FlexE calendar configuration switching

4.3 FlexE Technology Standards Progress and Application Cases

4.3.1 FlexE Standardization and Technology Development

The OIF launched the FlexE standard in early 2015 and released FlexE IA 1.0 in 2016. Attracting wide attention since its release, this standard is the first FlexE standard in the industry and defines support for 100GE PHYs. The OIF later went on to release FlexE IA 2.0, which augments FlexE IA 1.0 by providing support for 200GE/400GE PHYs. It does this while maintaining the multiplexing frame format compatible with FlexE IA 1.0 and the padding mechanism for 100/200/400GE PHY rate adaptation. Additionally, FlexE IA 2.0 supports IEEE 1588v2 time synchronization in mobile backhaul application scenarios.

In addition to the OIF, standards organizations such as the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), Internet Engineering Task Force (IETF), and Broadband Forum (BBF) have started FlexE standardization.

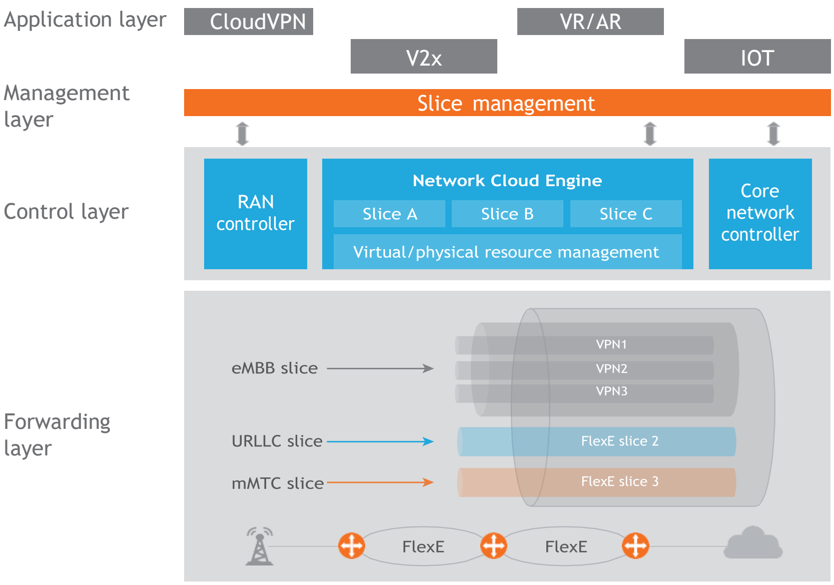
- The ITU-T Q11/15 and Q13/15 work groups are currently defining the mapping of the FlexE unaware, terminate, and aware modes on OTNs, with these definitions due to be released through a supplementary version of the G.709 standard. The mapping of the FlexE unaware mode references the PCS codeword transparent transmission mode of 100GBASE-R on OTNs. In terminate mode, the existing transmission devices carry Ethernet data, and the idle/padding mechanism can be used to adjust transmission rates. The mapping of the aware mode on OTNs is implemented through the latest idle mapping mechanism. The rate of client data flows on the UNI side and the DWDM link rate can be adjusted. In addition, a mechanism for FlexE time and frequency synchronization in the OTN mapping is also being discussed.
- The BBF launched the standards project "Network Services in IP/MPLS Network using Flex Ethernet" in May 2017. The project aims to define how to implement the enhanced QoS function architecture through FlexE interfaces on IP/MPLS networks and how to achieve compatibility with tunneling technologies that support FlexE interfaces on the existing networks, with the aim of better carrying bandwidth-hungry and latency-sensitive services. The BBF conference of 2017 Q3 saw the acceptance of multiple FlexE-based proposals, including technical solutions and architectures for deploying FlexE on IP/MPLS networks, FlexE-based network slicing, and more flexible path provisioning/management based on Segment Routing.
- The IETF has started to formulate the FlexE control plane standard, with the objective of extending FlexE from interface technology to end-to-end technology that leverages IETF's IP/MPLS technology to provide interface-level hardware-based isolation, thereby implementing technical solutions, such as network slicing and VIP private lines. Currently, the IETF focuses on the FlexE framework, mainly involving the architecture and scenarios of the end-to-end FlexE technology, as well as the signaling and routing protocols that need to be improved/extended for implementing end-to-end FlexE paths. The signaling extension focuses on RSVP-TE and Segment Routing, while the routing protocol extension includes the extension of IS-IS, OSPF, and BGP-LS.

With the emergence of new services such as 5G URLLC bearer and time-sensitive applications, deterministic networking was introduced to guarantee worst-case latency on IP/Ethernet networks. The Layer 2 technology IEEE 802.1 TSN and Layer 3 technology IETF DetNet define the congestion management mechanism on IP/Ethernet networks, scheduling algorithm based on latency information, explicit path establishment, and high-reliability redundant link technology. These technologies can work in combination with FlexE technology to provide deterministic service bearers with lower-bounded latency and zero packet loss, and this has also become a research focus.

With the official release of the OIF's FlexE IA 2.0 and FlexE technology's systematic application and architecture expansion in related standards organizations in the data communication field, FlexE technology has attracted much attention within the industry. Chip and device manufacturers are actively engaged in related R&D, product testing, and demonstration, while network operators and large OTT service providers are also actively participating in standards promotion, technical cooperation, and solution verification. Indeed, the related industry chain is starting to form.

4.3.2 FlexE Technology Application Cases

5G network slicing is one possible application of FlexE. Network slicing divides network resources to meet the transport requirements of different services and guarantee SLA compliance (such as satisfying bandwidth and latency requirements). As outlined in NGMN 5G White Paper, network slicing allows an IP network to carry diversified services, such as eMBB, autonomous driving, URLLC, and mMTC services. FlexE channelization provides physical division and isolation between FlexE clients at the interface level and can construct E2E network slices based on the router architecture.



Management layer

» Each slice application has an independent configuration management page.
» Based on the actual requirements, all slices support network function expansion.

Control layer

» Each slice has an independent network topology, resource allocation mode, and even control protocol, and they are controlled by the slice instance.

Forwarding layer

» Based on the FlexE technology, the forwarding layer provides E2E physical service isolation and different SLAs.

Figure 4-5 FlexE-based 5G network

In 2019, Huawei partnered with China Mobile and China Southern Power Grid to complete the world's first 5G differential protection test for power distribution network lines in Shenzhen. This test, which is a phased field test of 5G smart grid applications, was carried out on a real and complex network environment for carrying differential protection services across base stations. In addition, network slicing was used to isolate power grid services from non-power grid services. A service indicator verification showed that 5G meets the millisecond-level latency and microsecond-level precision network timing requirements of power grid control services.

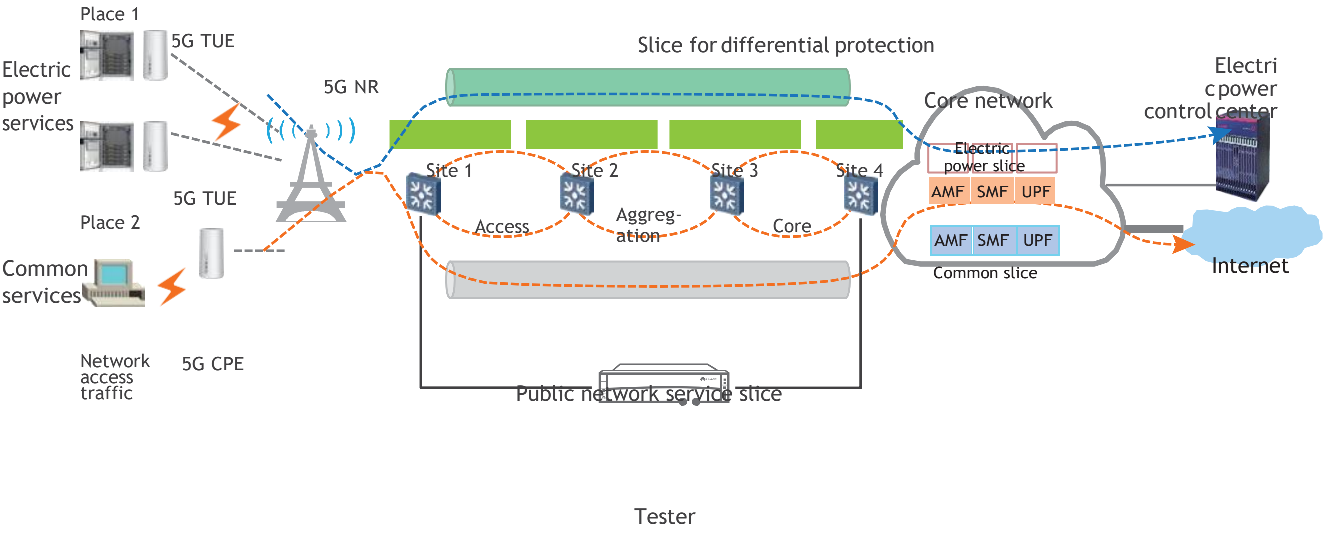


Figure 4-6 Networking diagram for testing differential protection for power distribution network lines

In the test, electric power services and eMBB public network services were carried on different network slices. The test instrument was used to simulate public network traffic congestion and bursts on the live network, with the aim of testing the impact on the latency and packet loss of electric power services. The test results show that the latency increased for the eMBB services on the public network, while it did not change significantly for electric power services during traffic congestion and bursts.

Table 4-1 Test results

Test Case	Maximum Latency		Packet Loss Rate		Maximum Jitter	
Service type	Electric power service	Public network service	Electric power service	Public network service	Electric power service	Public network service
Before congestion	1 ms	1 ms	0	0	19 μs	19 μs
Public network slice congestion	1 ms	28 ms	0	22.7%	17 μs	27 μs
Public network slice burst	1 ms	28 ms	0	0	19 μs	22 μs

4.4 FlexE Small-Granularity Bearer Technology

Currently, the minimum granularity defined by the OIF is 5 Gbit/s. This means that the channel utilization is low when the electric power communication network carries low-speed services. FlexE overcomes this by dividing 5 Gbit/s granularity slots into sub-slots. In this way, the 1 Gbit/s granularity can be achieved for more refined isolation. The implementation of the 1 Gbit/s granularity does not change the way slots are divided in the 5 Gbit/s granularity. Instead, the 5 Gbit/s slot is expanded from a time dimension, and five pieces of 1 Gbit/s data occupy one standard FlexE-based 5 Gbit/s slot in terms of TDM. As shown in Figure 4-7, each 5 Gbit/s slot is divided into five 1 Gbit/s sub-slots (represented by five colors). In multiple slot transmission periods, blocks of five colors are transmitted alternately, and the slots of the original 5 Gbit/s channel are evenly allocated. This is how the small-granularity bearer capability of FlexE is implemented.

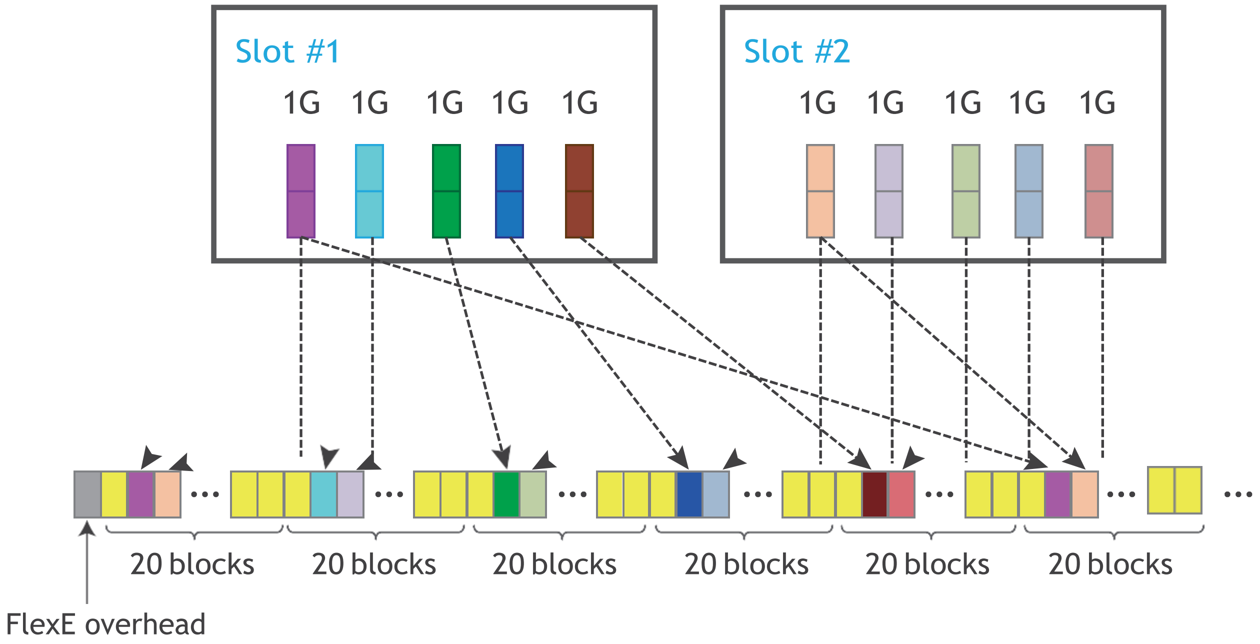


Figure 4-7 Implementation of 1 Gbit/s granularity bearer

Because the slot division structure of FlexE is not changed, the 1 Gbit/s granularity is compatible with the main architecture defined in the OIF standard. In this way, slices with smaller granularities can be divided based on service requirements. Huawei has already achieved technical support for FlexE slices with a minimum granularity of 2 Mbit/s on 10GE ports.

4.5 Comparison Between FlexE and HQoS

HQoS uses a multi-level queue scheduling mechanism to guarantee the bandwidth of services of a large number of users in the DiffServ model. In addition, it uses multi-level scheduling to distinguish between user-specific and service-specific traffic and subsequently provide differentiated bandwidth management. However, preemption based on statistical multiplexing in HQoS cannot ensure that the forwarding latency and jitter meet requirements during congestion or burst traffic.

FlexE, on the other hand, can implement physical isolation on one port or optical fiber link. It allows services to share hardware resources of the port or optical fiber link, while ensuring they are independent on the forwarding plane. It achieves this using FlexE slot multiplexing to divide a physical port of a high-bandwidth pipe into several sub-channel ports, which are then applied to different network slices. FlexE interfaces are based on slot multiplexing and have an independent MAC layer, and frame processing on one FlexE interface is not affected by other FlexE interfaces. In contrast, HQoS does not have an independent MAC layer, and the physical MAC layer is shared. Therefore, frames are processed one after another, leading to HOL blocking, which affects the latency and jitter of services. FlexE outperforms HQoS with more affective isolation and by ensuring that the latency and jitter indicators meet the requirements of relay protection services.

05 Relay Protection Service Bearing Using FlexE

5.1 Design for the FlexE-based Relay Protection Service Bearer Solution

5.1.1 Creating an Exclusive Network Slice for Relay Protection Service Bearer

On the electric power communication network, relay protection services are mission-critical services that pose the highest requirements on the network Service-Level Agreement (SLA). To address these requirements, Huawei proposed the next-generation intent-driven IP communication network solution for power transmission and transformation. This solution uses the FlexE technology to divide the power communication network into multiple physically isolated network slices. Each slice can be configured with exclusive network resources. One slice can be used to carry relay protection services to isolate them from other electric power services. This ensures that the other services do not interfere with the relay protection services. It also meets the communication requirements of the relay protection services for low latency, low jitter, and consistent two-way latency. The bandwidth of other slices can be flexibly configured based on the requirements of different electric power services to implement efficient bearing.

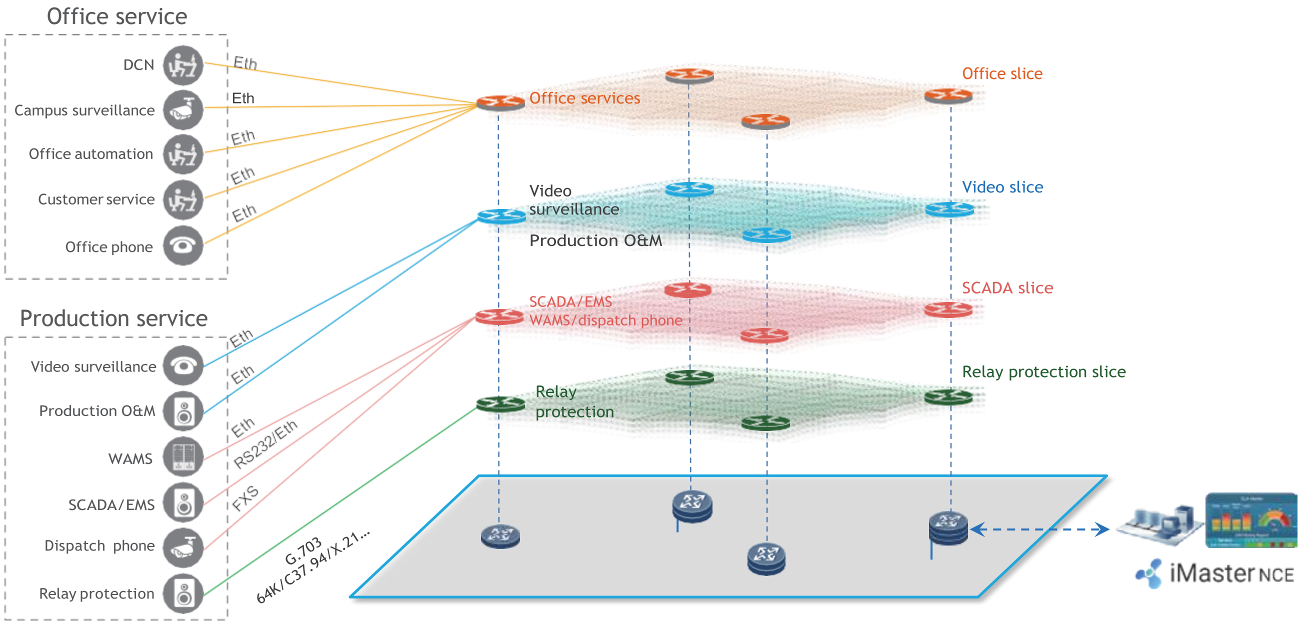


Figure 5-1 FlexE slices

Because FlexE isolates network resources between slices, resources on one slice cannot preempt those on another slice. This means that a dedicated network slice with exclusive resources can be used to bear relay protection services, ensuring that these services are not affected by other services, without the need to deploy QoS for the network slice. The dedicated slice can be used to bear multiple relay protection services, which share network resources on the slice. FlexE not only meets SLA requirements of relay protection services, but also fully utilizes network resources on the slice. The bandwidth resources required by each electric power service at the access, aggregation, and core layers can be estimated based on the network topology. Sufficient network resources for each FlexE slice of electric power services can then be reserved.

Table 5-1 Suggestions on FlexE slices of electric power services

Slice	Service on the Slice	Service Type	Recommended Access-Side Bandwidth for the Slice
Slice 1	Relay protection service	Mission-critical service	≤ 1 Gbit/s
Slice 2	SCADA/EMS/WAMS/dispatch phone	Mission-critical service	≤ 1 Gbit/s
Slice 3	Substation video surveillance/production O&M	Mission-critical service	≤ 1 Gbit/s
Slice 4	Office automation/customer service/video conference	Office service	≤ 10 Gbit/s

5.1.2 Using PWE3 for Relay Protection Service Bearer

Traditional protection relays require low-speed interfaces (such as C37.94, G.703 64K, and X.21) on the communication network. Huawei routers allow multiple types of relay protection service interfaces to be directly connected to protection relays. On the slice used to bear relay protection services, a local PE encapsulates the relay protection service flow into Ethernet packets and uses TDMoPSN to transmit the Ethernet packets to the remote PE through a PWE3 channel. After receiving the Ethernet packets, the remote PE decapsulates them to obtain the original relay protection service flow.

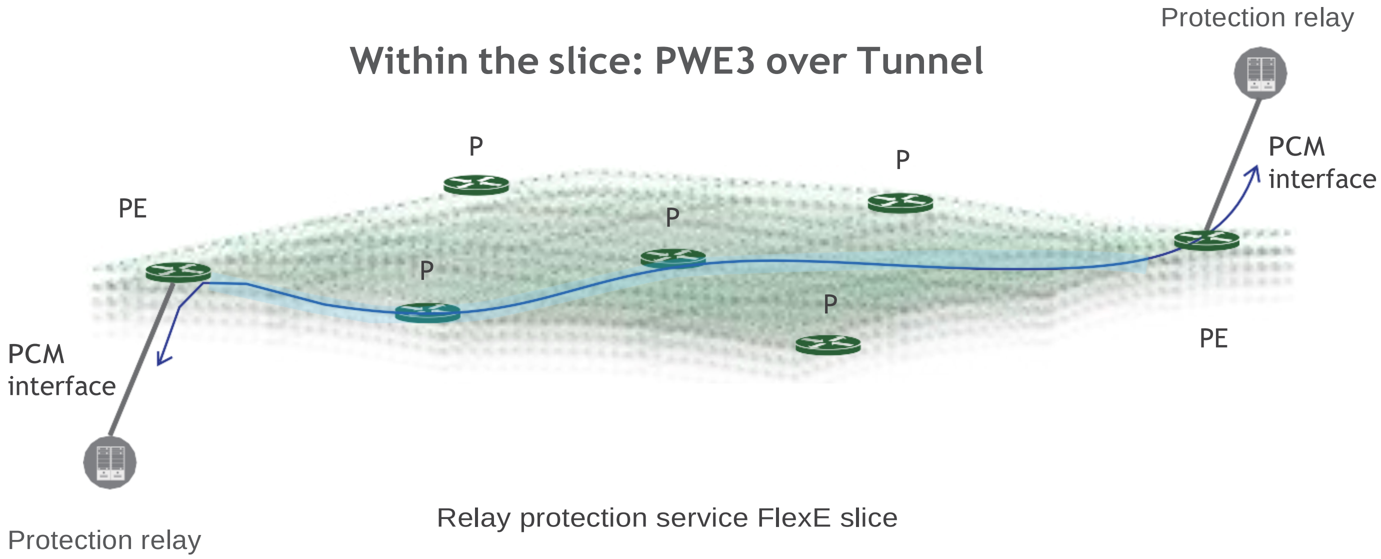

Within the slice: PWE3 over Tunnel
Protection relay
PCM
interface
P
P
P
P
P
PE
PE
PCM
interface
Protection relay
Relay protection service FlexE slice

Figure 5-2 FlexE network slice for relay protection service bearer

On the slice used to bear relay protection services, path planning must be performed using TE technologies to ensure co-routed round-trip paths. Such planning is required regardless of whether static TE, RSVP-TE, SR-MPLS TE, or SRv6 TE tunnels are used as PWE3 channels, and is necessary for ensuring consistent two-way latency. If sufficient network resources are reserved for FlexE slices and co-routed round-trip paths are planned, TDMoPSN can meet the SLA requirements of relay protection services without the need to deploy additional functions, such as HQoS and latency compensation.

5.2 How FlexE Ensures the Quality of Relay Protection Services

To ensure the reliability of relay protection services on electric power communication networks, a primary/secondary channel redundancy design is used. The primary channel uses the optical fiber composite overhead ground wire (OPGW) in a power transmission line that directly connects two substations. If only one OPGW is available between two substations or they are not directly connected through optical fibers, the secondary channel must detour to other substations. In the theoretical analysis and testing stages, the primary channel communication model is designed based on the direct-connection scenario, where optical fibers directly connect two pieces of communication equipment. An "extreme scenario" is used in the design of the secondary channel communication model. This extreme scenario uses a communication distance of 500 km and 15 hops.

5.2.1 Ensuring a Low Latency for Relay Protection Services

On the FlexE slice of relay protection services, the latency over the PWE3 channel that carries such services is mainly comprised of three parts: Ingress_latency, Transit_latency, and Egress_latency.

- Ingress_latency includes the PWE3 encapsulation latency and hardware forwarding latency on the ingress. The maximum encapsulation latency on the ingress is 125 μs because the encapsulation interval on the ingress is generally set to the value. The maximum hardware forwarding latency on the ingress is Device_latency.
- Transit_latency includes the optical transmission latency, hardware forwarding latency, and queuing latency. The queuing latency on transit nodes is 0 because sufficient bandwidth resources are reserved for FlexE slices. The optical transmission latency is 5 μs/km, which is a constant. Without congestion on FlexE slices, the maximum hardware forwarding latency on each transit node is Device_latency.
- Egress_latency includes the jitter buffer and hardware forwarding latency on the egress. To ensure that a fixed one-way latency of 1000 μs is achieved, it is recommended to set the half-bucket depth of the jitter buffer on the egress to 1000 μs. The maximum hardware forwarding latency on the egress is Device_latency.

In the extreme scenario when the FlexE slice of relay protection services is not congested, the maximum theoretical latency over a PWE3 channel is mainly comprised of the following three parts:

Max_Ingress_latency
= Maximum encapsulation latency + Maximum hardware forwarding latency on the ingress
= 125 μs + Device_latency
Max_Egress_latency
= Jitter buffer + Maximum hardware forwarding latency on the egress
= 1000 μs + Device_latency
Max_Transit_latency
= Maximum optical transmission latency + Maximum hardware forwarding latency of 14 transit nodes
= 5 μs/km × 500 km + 14 × Device_latency
= 2500 μs + 14 × Device_latency

The maximum theoretical latency (Max_T_latency) over the PWE3 channel is calculated as follows:

Max_T_latency
= Max_Ingress_latency + Max_Egress_latency + Max_Transit_latency
= 3625 μs + 16 × Device_latency

Sufficient resources need to be planned for FlexE slices to ensure that congestion does not occur on the FlexE slice that bears relay protection services. If the Device_latency of each node is less than 85.9 μs, the transmission latency of E2E relay protection services is less than 5 ms. This is true even in the extreme scenario, and therefore meets the strictest low-latency transmission requirements of relay protection services. In general, the hardware forwarding latencies of routers from mainstream vendors are much lower than 85.9 μs in congestion-free scenarios. Hard isolation of FlexE slices and proper planning of network resources are key to ensuring that slices remain free of congestion.

5.2.2 Ensuring a Low Jitter for Relay Protection Services

If sufficient bandwidth resources are reserved for the FlexE slice that bears relay protection services, no buffer queuing latency or jitter occurs on the involved communication equipment. Additionally, this FlexE slice remains unaffected by any congestion that occurs on other slices. Relay protection services exclusively use network resources on the slice allocated to them. The jitter over the PWE3 channel is analyzed as follows:

- Packet encapsulation on the ingress involves a fixed latency and no jitter.
- The transmission through transit nodes over optical fibers involves a fixed latency and no jitter.
- If relay protection services are locally added and dropped on transit nodes, hardware forwarding is required. This affects E2E relay protection services and causes jitter.
- The jitter buffer on the egress can compensate for jitter. A sufficient jitter buffer needs to be planned to ensure that the egress induces no jitter on the E2E relay protection services and that no buffer overflow or underflow occurs.

To summarize, PWE3 can ensure a jitter of less than 200 μs for E2E relay protection services on a FlexE slice when combined with a suitable jitter buffer. This meets the strictest one-way low-jitter transmission requirements of relay protection services.

5.2.3 Ensuring a Low Two-Way Latency Variation for Relay Protection Services

On the FlexE slice used to bear relay protection services, the two-way latency variation of these services transmitted over a PWE3 channel mainly depends on the following three factors:

- Whether the encapsulation latencies of the two end nodes are the same. As an example, assume that the encapsulation interval is 125 μs on the ingress, the encapsulation latency on one end node is the minimum encapsulation latency (0 μs), and the encapsulation latency on the other end node is the maximum encapsulation latency (125 μs). In this example, a two-way latency variation of 125 μs is generated during encapsulation.
- Impact on E2E services by service adding and dropping on transit nodes. In a typical relay protection scenario, four relay protection services are locally added and dropped on each transit node. The local service adding and dropping causes a two-way latency variation on E2E services. For example, locally adding and dropping four relay protection services on each transit node may cause latency in E2E relay protection services transmitted in one direction (forward transmission) but not in the other direction (backward transmission). In an extreme scenario where E2E relay protection services traverse 15 hops, the forward transmission is affected by the adding and dropping of 60 relay protection services (4 services x 15 hops), whereas the backward transmission is not affected. Suppose that the relay protection service flow transmitted over a PWE3 channel is encapsulated into 64-byte (512-bit) packets and the granularity of the FlexE slice is 1 Gbit/s. In this case, the additional forward transmission latency brought by local service adding and dropping on transit nodes is calculated as follows:

Forward_latency_additional

= Number of hops x Additional forward transmission latency on each hop

= Number of hops x (Size of relay protection service packets added and dropped on each hop/FlexE slice bandwidth)

=15 × (4 × 512 bit/1 Gbit/s)

= 30.7 μs

In this extreme scenario, backward transmission incurs no additional latency. Therefore, an additional two-way latency variation of 30.7 μs is generated because services are added and dropped on transit nodes.

- Whether round-trip paths are co-routed. The difference in length between bidirectional optical fibers that carry PWE3 services can be ignored. If TE and static bidirectional co-routed LSP technologies are used, round-trip paths pass through the same transit nodes. This means that the round-trip paths are consistent, resulting in no two-way latency variation.

The maximum two-way latency variation of E2E relay protection services is calculated as follows:

Max_Two-Way latency variation

= Maximum encapsulation latency variation between the two end nodes + Maximum two-way latency variation on transit nodes

= 125 μs + 30.7 μs

= 155.7 μs

< 200 μs

To summarize, TE and static bidirectional co-routed LSP technologies can ensure the maximum two-way latency variation of E2E relay protection services on the FlexE slice does not exceed 200 μs, even in the extreme scenario. This meets the two-way latency variation requirements of relay protection services.

5.3 Performance Tests of FlexE-based Relay Protection Service Bearer

Primary/secondary channel redundancy is recommended for relay protection services. To verify the performance of this redundancy design, tests are carried out in direct-connection and multi-hop scenarios.

- Direct-connection scenario: The primary channel directly connects two protection relays. The FlexE hard isolation bearer performance of the primary channel is tested and verified.

- Multi-hop scenario: The secondary channel passes through 15 hops. The FlexE hard isolation bearer performance and PWE3 transmission performance of the secondary channel are tested and verified.

5.3.1 Performance Test in the Direct-Connection Scenario

Figure 5-3 shows the networking for the performance test in the direct-connection scenario. Two 100GE interfaces of a router are directly connected to the 100GE interfaces of another router through optical fibers, and FlexE is deployed on these interfaces to provide two 5 Gbit/s slices. The tester connects to the routers through Ethernet interfaces and simulates two types of electric power service flows by sending fixed-length packets to the routers. According to the theoretical analysis in section 5.2, the transmission of relay protection services through optical fibers generates a fixed latency and no jitter or two-way latency variation. In this test environment, optical fibers with a total length of less than 1 km are used to connect the routers. This test mainly focuses on the hard isolation performance of FlexE. Therefore, no PCM interfaces or PWE3 channels are used to bear services.

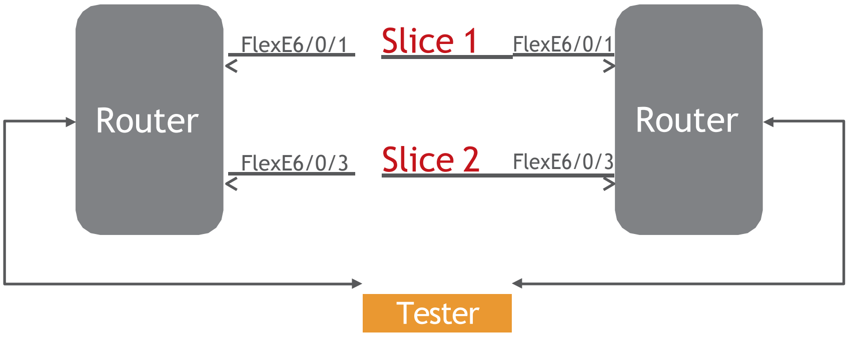


Figure 5-3 Networking for the performance test in the direct-connection scenario

Details about the test are as follows:

- Scenario without congestion on both slices: The tester injects bidirectional 100 Mbit/s traffic into slice 1 to simulate relay protection services and injects bidirectional 4.7 Gbit/s traffic into slice 2 to simulate other types of electric power services. The priorities of the services on slice 2 are not differentiated. Then the latencies, jitters, and two-way latency variation on the two slicesare tested.

- Scenario with congestion only on slice 2: The tester injects bidirectional 100 Mbit/s traffic to simulate relay protection services and injects bidirectional 900 Mbit/s traffic along with 4.7 Gbit/s traffic to trigger congestion on slice 2. The priorities of the services on slice 2 are not differentiated. The latencies, jitters, and two-way latency variation on the two slices are then tested.

Table 5-2 FlexE performance test results in the direct-connection scenario (without PWE3)

Slice	Slice 1			Slice 2		
Performance indicator	No congestion on both slices	Congestion only on slice 2	Indicator deterioration ratio	No congestion on both slices	Congestion only on slice 2	Indicator deterioration ratio
Minimum	35.72	36.15	1.20%	35.74	2329.45	6417.77%
Maximum	44.5	45.04	1.21%	44.72	2618.82	5756.04%
Average	37.25	37.36	0.30%	37.27	2532.54	6695.12%
Jitter (μs)	8.78	8.89	1.25%	8.68	289.37	3122.38%

According to the test results, the latency and jitter performance on the two slices meets requirements when both slices are not congested. When slice 2 is congested, the latency and jitter indicators of slice 2 deteriorate significantly. However, slice 1 is not affected by the congestion on slice 2, and the latency and jitter indicator deterioration ratios on slice 1 are less than 2%.

The results of the performance test in this scenario demonstrate that the performance indicators on a congestion-free FlexE slice over the primary channel are not affected by other congested slices. FlexE slices provide hard isolation channels for different types of electric power services, thereby realizing high-quality network communication services and ensuring high-quality bearer of relay protection services.

5.3.2 Performance Test in the Multi-Hop Scenario

In a multi-hop performance test, the isolation performance between FlexE slices is tested first. Figure 5-4 shows the networking used for the test. To simulate the extreme 15-hop scenario, 15 pairs of 100GE interfaces on the two routers are connected through optical fibers, and FlexE is enabled on the interfaces. A serpentine networking of two routers is formed by internally connecting FlexE interfaces on each router. Two FlexE slices are created, with bandwidth set to 5 Gbit/s for each slice. E2E protection services are transmitted in the simulated 15-hop networking. The tester connects to the two routers through common Ethernet interfaces and simulates two types of electric power service flows by sending fixed-length packets to the routers. According to the theoretical analysis in section 5.2, the transmission of relay protection services through optical fibers generates a fixed latency and no jitter or two-way latency variation. In this test environment, optical fibers with a total length of less than 2 km are used to connect the routers. This test mainly focuses on the performance of isolation between FlexE slices. Therefore, no PCM interfaces or PWE3 channels are used to bear services.

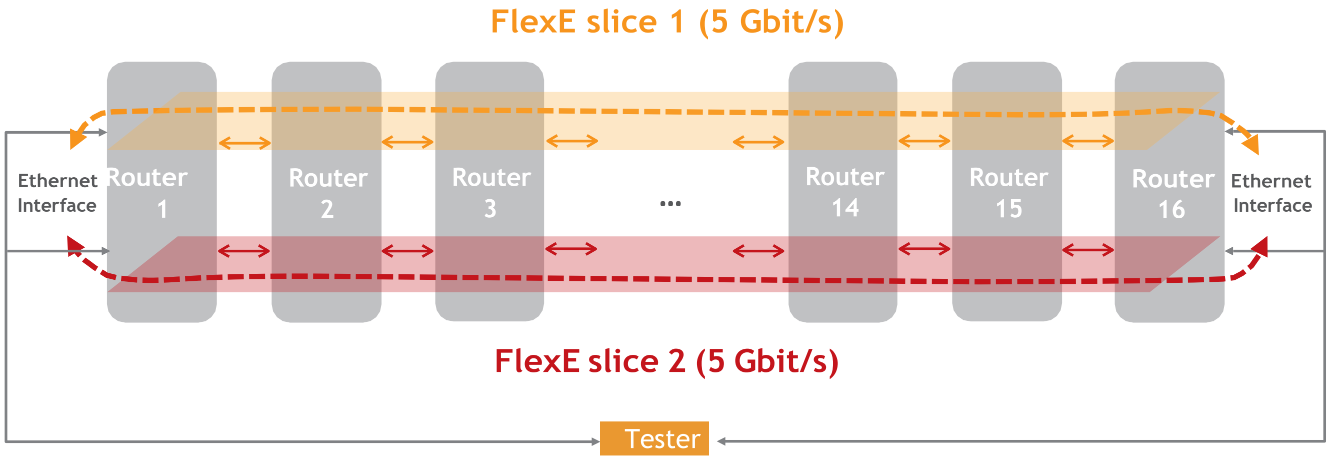


Figure 5-4 Networking for testing FlexE isolation performance in a multi-hop scenario (without PWE3)

Details about the test are as follows:

The tester injects bidirectional 2 Gbit/s traffic into slice 1 to simulate relay protection services. It also injects bidirectional 8 Gbit/s traffic into slice 2 to simulate other types of electric power services, exceeding slice 2's capacity and thereby causing congestion. Table 5-3 shows the performance test results on the two slices in the multi-hop scenario.

Table 5-3 FlexE performance test results in the multi-hop scenario (without PWE3)

Slice	Slice 1		Slice 2	
Performance indicator	Forward transmission performance indicator	Backward transmission performance indicator	Forward transmission performance indicator	Backward transmission performance indicator
Minimum	250.26	250.92	20186.19	273.67
Maximum	265.54	273.79	20230.51	20231.19
Average	255.87	256.14	20208.75	2026.31
Jitter (μs)	15.28	22.87	44.32	19957.52
Maximum two-way latency variation (μs)	23.52		19956.84	

According to the test results, the latency and jitter indicators on slice 2 deteriorate significantly. However, slice 1 is not affected by slice 2. These results demonstrate that FlexE technology achieves hard isolation in the multi-hop scenario as long as network resources are properly planned, even when HQoS is not configured. This proves that FlexE can provide differentiated and high-quality network communication services for relay protection services.

Figure 5-5 shows the networking used to test the performance of relay protection service bearer through PCM interfaces and a PWE3 channel in the multi-hop scenario. Optical fibers with the total length less than 1 km are used to connect 100GE interfaces of 16 routers. A FlexE slice is used to bear relay protection services, with its bandwidth set to 1 Gbit/s. The tester is connected to the routers at the two ends through PCM interfaces and injects a 2 Mbit/s relay protection service flow. Routers use the PWE3 technology to bear the relay protection services and encapsulate service flows into 64-byte (512-bit) packets. In addition, each transit node locally adds and drops four forward relay protection services, introducing an uncertain forward transmission latency and increasing the two-way latency variation generated on the transit nodes. This test simulates the scenario mentioned in section 5.2.3, in which locally adding and dropping services on transit nodes affect E2E relay protection services.

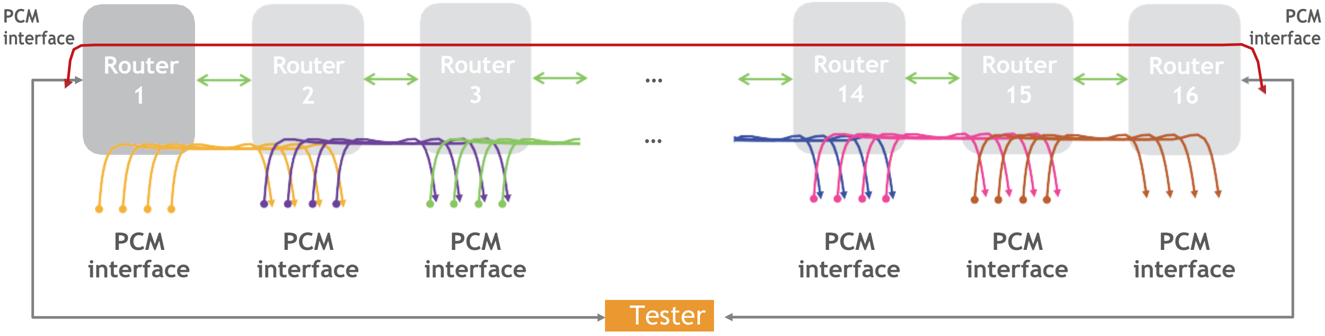


Figure 5-5 Networking for testing FlexE bearer performance in a multi-hop scenario (with PWE3)

The encapsulation interval on the ingress is set to 125 μs, and the half-bucket depth of the jitter buffer on the egress is set to 1000 μs. 60 tests are carried out. In each test, optical fibers of the PCM interfaces used to transmit E2E relay protection services are disconnected and then re-connected. This is performed to re-establish the bearer channel for relay protection services. The performance test results of E2E relay protection services are as follows:

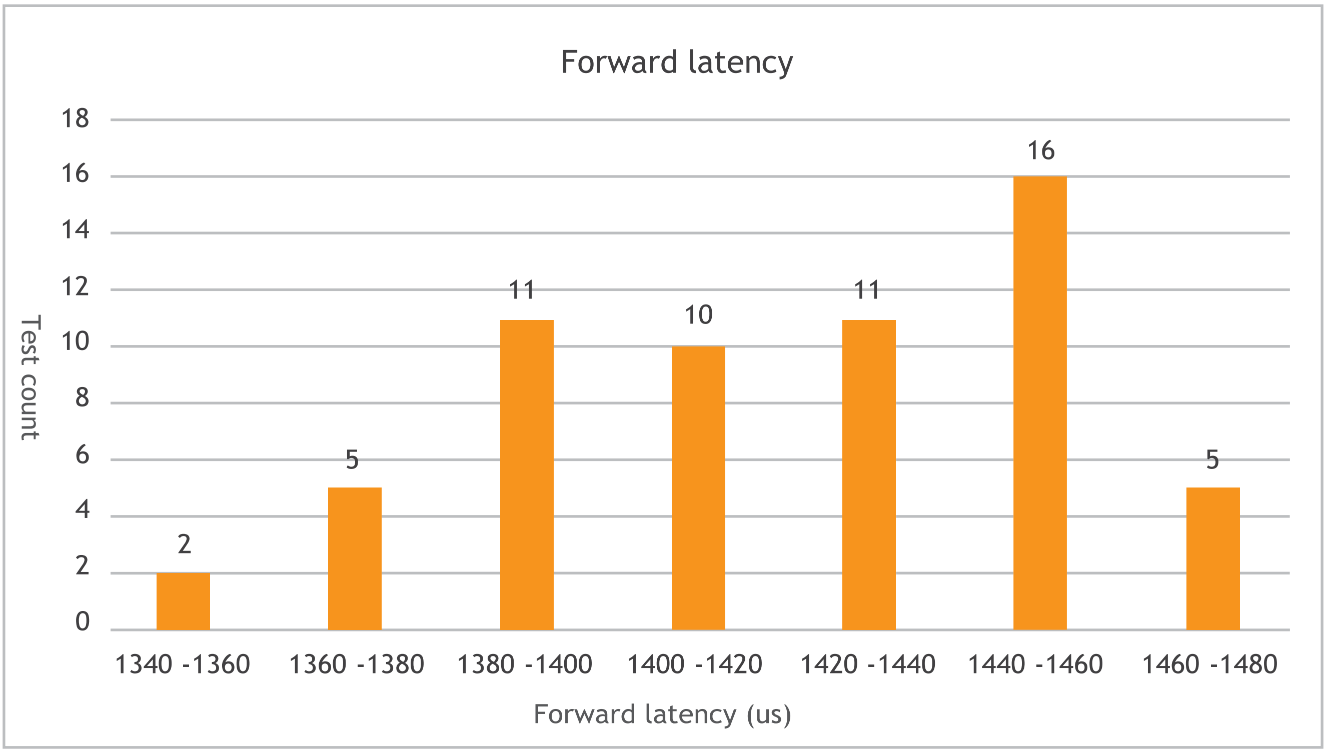


Figure 5-6 Forward latency statistics

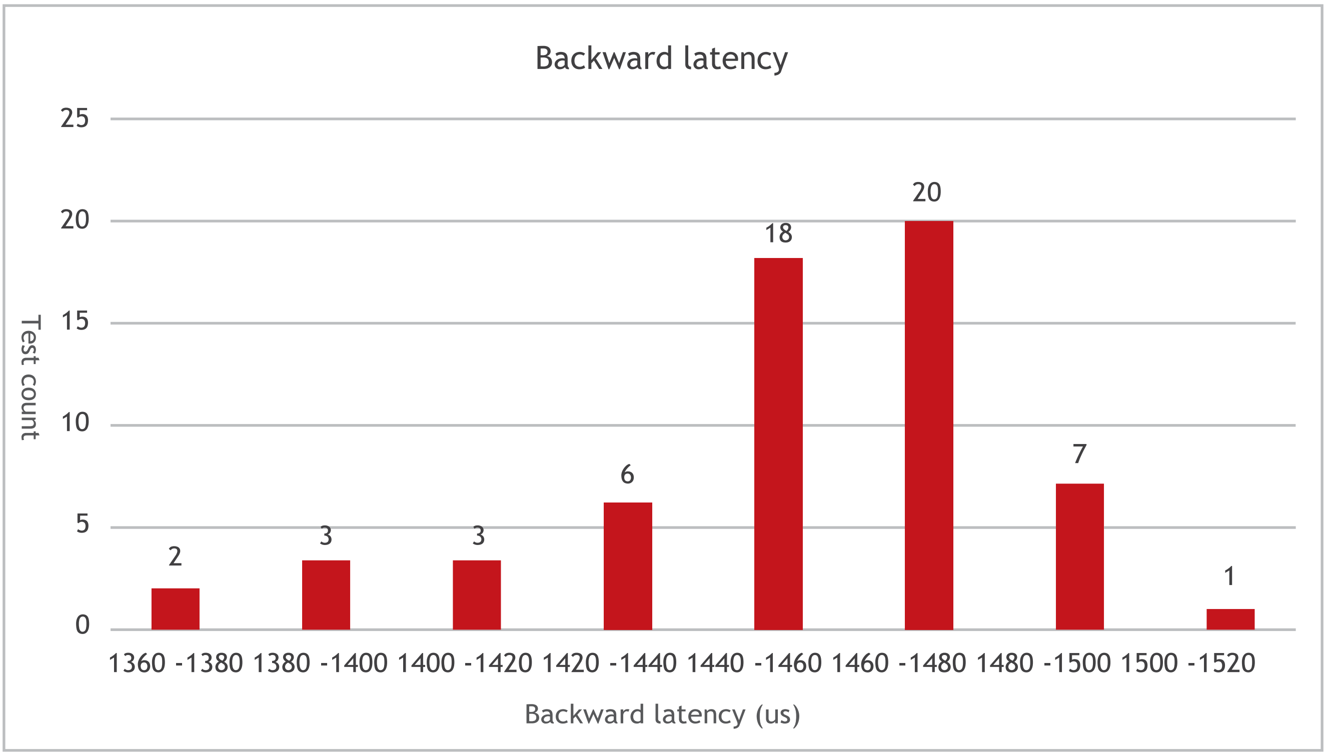


Figure 5-7 Backward latency statistics

Table 5-4 Performance test results of relay protection services in the multi-hop scenario (with PWE3)

Performance indicator	Forward Transmission Performance Indicator	Backward Transmission Performance Indicator
Minimum latency (μs)	1349	1373
Maximum latency (μs)	1477	1517
Maximum two-way latency variation (μs)	168	

According to the theoretical analysis in section 5.2, transmission of relay protection services over 500 km of optical fibers in the extreme scenario generates a fixed latency of 2500 μs and no jitter or two-way latency variation. Even the maximum latency (in either forward or backward transmission) plus the fixed latency of 2500 μs is less than 5000 μs. In each test, the one-way jitter of relay protection services is less than 5 μs. The maximum two-way latency variation is 168 μs, which is less than 200 μs. In summary, the three key performance indicators (latency, jitter, and two-way latency variation) meet the strict requirements of relay protection services, even in the extreme scenario where relay protection services are transmitted across 15 hops through a PWE3 channel on a FlexE slice and technologies such as HQoS and delay compensation are not deployed.

06 Summary

FlexE technology can resolve the conflicts brought by traditional Ethernet statistical multiplexing, ensure that services of Ethernet slices are independent of each other, and solve problems in various scenarios such as service isolation, stable latency, and low jitter scenarios. To meet the development requirements of smart grids, Huawei employs the FlexE technology. This technology is able to meet the strict network transmission requirements of relay protection services and carry relay protection services with high quality, as verified by Huawei. Huawei's FlexE-based Intent-Driven IP network can reliably carry mission-critical services such as relay protection and SCADA services, ensuring smooth service migration to IP networks and meeting the requirements of current and future electric power communication networks. In this way, efficient ICT assurance is provided for the evolution and development of smart grids.

07 References

[1] OIF Flex Ethernet Implementation Agreement: IA OIF-FLEXE-01.0

[2] OIF Flex Ethernet Implementation Agreement: IA OIF-FLEXE-02.0

[3] https://tools.ietf.org/html/draft-izh-ccamp-flexe-fwk-03

[4] https://datatracker.ietf.org/wg/detnet/about/

A Acronyms and Abbreviations

Acronym or Abbreviation	Full Name
BBF	Broadband Forum
BGP-LS	Border Gateway Protocol-Link State
CESoPSN	Structure-Aware TDM Circuit Emulation Service over Packet Switched Network
DWDM	Dense Wavelength Division Multiplexing
eMBB	Enhanced Mobile Broadband
FlexE	Flexible Ethernet
HQoS	Hierarchical Quality of Service
HOL	Head Of Line blocking
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IoT	Internet of things
MEF	Metropolitan Ethernet Forum
MPLS	Multi-Protocol Label Switching
NGMN	Next Generation Mobile Network
OAM	Operation, Administration and Maintenance
OTN	Optical Transport Network
OIF	Optical Internetworking Forum

Acronym or Abbreviation	Full Name
OPGW	Optical Fiber Composite Overhead Ground Wire
PCM	Pulse Code Modulation
PDH	Plesiochronous Digital Hierarchy
PWE3	Pseudo Wire Emulation Edge to Edge
PSN	Packet Switched Network
PCS	Physical Coding Sublayer
PHY	Physical Layer
PMA	Physical Medium Attachment
PMD	Physical Media Dependent
QoS	Quality of Service
QoE	Quality of Experience
RSVP-TE	Resource Reservation Protocol-Traffic Engineering
SDH	Synchronous Digital Hierarchy
SAToP	Structure-Agnostic TDM over Packet
SCADA	Supervisory Control and Data Acquisition
TDM	Time Division Multiplexing
TDMoPSN	Time Division Multiplexing over Packet Switched Network
UNI	User-to-Network Interface
NNI	Network to Network Interface
uRLLC	ultra-Reliable and Low-Latency Communication
WAMS	Wide Area Measurement System

HUAWEI TECHNOLOGIES CO., LTD.
Huawei Industrial Base
Bantian Longgang
Shenzhen 518129, P.R. China
Tel: +86-755-28780808
www.huawei.com

Trademark Notice

General Disclaimer

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.