EANTC Independent Test Report

Huawei iMaster NCE-IP

Autonomous Network Solution for SRv6

November 2023

Contents

Introduction

EANTC, an independent test lab based in Berlin (Germany), was commissioned by Huawei to verify the Autonomous Networks (AN) capabilities of the iMaster Network Cloud Engine for IP (NCE-IP). Our team was invited to verify in how far NCE could automatically provision, monitor, and optimize a Segment Routing over IPv6 (SRv6) end-to-end network solution with Huawei routers. The tests were carried out in August 2023 at Huawei premises in Beijing, China.

Autonomous Networks Concept and Implementation

Network automation plays a crucial role in progressing the telecommunications industry. The promised benefits are substantial; however, it is a critical time for pioneering communications service providers to take important steps now. The TM Forum has recently initiated an Autonomous Networks Manifesto which has been signed by 13 service providers so far, who promised to embark on the journey to accelerate the adoption of ANs.

In terms of cost savings and efficiency improvements to manage the exponentially increasing number of devices, AN technology promises to significantly reduce operational and capital expenditures. Autonomous networks operations are a way for carriers to prepare for service growth while keeping operational costs under control, and avoiding to grow the engineering work force.

The TM Forum reported that service providers could unlock over $700 billion of new revenues from industrial 5G and B2B2X (business to business to everything) opportunities through autonomous networks.

Autonomous networks are founded on several key principles:

1. **Automation Levels**: Autonomous networks aspire to achieve advanced levels of automation across various facets of network management. These facets encompass provisioning, monitoring, troubleshooting, optimization, and security.

2. **AI and Machine Learning Integration**: At the heart of autonomous networks lies the incorporation of artificial intelligence (AI) and machine learning (ML) technologies. These cutting-edge capabilities empower networks to make intelligent decisions, adapt to evolving circumstances, and enhance operational efficiency. They enable networks to learn from historical data, forecast potential issues, and engage in self-optimization.

1. **Intent-Driven Networking**: Autonomous networks frequently embrace the concept of intent-driven networking. In this framework, network operators articulate high-level business intents, and the network itself automatically translates these intents into precise network configurations and actions. This approach streamlines network provisioning and management, aligning network behavior with business objectives.

2. **Self-Awareness**: Autonomous networks are characterized by a heightened level of self-awareness. They possess the capability to continually monitor their own performance, recognize anomalies or irregularities, and proactively initiate corrective measures without necessitating human intervention. This self-awareness enhances network reliability and resilience.

3. **Efficiency and Reliability**: The principal objectives of autonomous networks include maximizing operational efficiency and bolstering network reliability. Automation reduces manual errors, accelerates response times, and enables networks to adapt swiftly to changing conditions, ultimately delivering superior service quality.

Autonomous Networks Categorization and Levels

An industry specification group (ISG) called "ENI" (Experiential Networked Intelligence) has been created under ETSI rules and has started drafting standards. Per the ETSI GR ENI 007 group report, it is mentioned that creating appropriate categories for ANs serves as a valuable guide for users when opting for a particular AI-assisted network setup.

TMForum's white paper provided the following as a definition of the AN levels:

Level	Description	Explanation
L0	Manual Operation and Management	The system delivers assisted monitoring capabilities, which means all dynamic tasks have to be executed manually
L1	Assisted Operation and Management	The system executes a certain repetitive sub-task based on pre-configured to increase execution efficiency
L2	Partial Autonomous Networks	The system enables closed-loop O&M for certain units based on AI model under certain external environments
L3	Conditional Autonomous Networks	Building on L2 capabilities, the system with awareness can sense real-time environmental changes, and in certain network domains, optimize and adjust itself to the external environment to enable intent-based closed-loop management
L4	High Autonomous Networks	Building on L3 capabilities, the system enables, in a more complicated cross-domain environment, analyse and make decision based on predictive or active closed-loop management of service and customer experience-driven networks
L5	Full Autonomous Networks	This level is the ultimate goal for telecom network evolution. The system possesses closed-loop automation capabilities across multiple services, multiple domains, and the entire lifecycle, achieving autonomous networks

Table 1: Definition of the AN Levels

One of the industry's issues is that the assessment of AN levels has not been well defined yet. It is way too early for any certification program, taking into account the complexity of AN level assessment for different technology areas – such as the IP transport networks, optical transmission networks, mobile radio access and core networks, broadband access, and so on.

Generally, there is a lot of uncertainty about current and desired AN levels in the industry. At the recent DTW Ignite conference in Copenhagen (September 2023), bold statements were made by some service providers, aiming to reach L4 level automation within two years across multiple service areas. This would be a very complex undertaking in a very limited time, given the fact that traditional OSS and BSS management systems still prevail in many operational environments.

The complexity of brownfield services is hard to automate – specifically for operators in established markets with diverse service offerings. From our point of view, it is quite unlikely that the promises can be implemented within the designated timelines, given the limited investment and development capabilities of Western communications services providers. In any case, it would require a fundamental change of how CSPs run their operations and, specifically, how much they trust third-party solutions to take critical provisioning and optimization decisions in an automated way.

At the same time, Autonomous Networks are about the only chance to prepare network operations for the future. Traditional operations of "VPN and IP pipes" have become increasingly commoditized. Reducing the provisioning times and providing value-added services with customer-focused options can only be achieved with automated operations.

More than service providers, many consultancies and service integrators have co-signed the TM Forum Manifesto mentioned above. Their value proposition will probably be to offer individual network migration support. While consultancy and individual integration will certainly be required, it seems to us at EANTC that integration alone would be quite costly and time-consuming. The industry would benefit from standardization, streamlining, interoperability of solutions, and realistic certification programs from our point of view. In the end, the procurement of AN components must become a part of regular procedures. AN components, with all their power to create superior, smooth, and cost-effective operations models – or to break it with disastrous results – requires strong quality assurance. A few major failures reported in the news could set back the industry for years.

Recently, the industry has tended towards paperwork-based certifications in what we like to coin the "Gartner model" at EANTC – but an industry operating with extremely complex technology solutions is at risk when procurement decisions are taken simply by reviewing paperwork and conducting functional proof of concept tests happily coordinated by vendors. The power and risk of ANs lies in non-functional aspects of network operations: Behavior in failover scenarios; adherence to technical SLAs; operations of large-scale service deployments; multi-vendor support in case operators do not want to depend on a single vendor across all network elements and management components.

To demonstrate that AN level assessment and quality assurance is possible, EANTC has put a stake in the ground together with Huawei, pioneering AN analysis criteria in one of the first independent evaluations for the IP transport network automation. Of course, the scope of this first analysis is limited. Much more diverse technology tests and scalability scenarios are left to the future, but with Huawei, we have found a brave vendor ready to submit their integrated AN and routing solution to an independent review.

We hope that the following detailed report provides a good read and will inspire the industry to develop detailed assessment methods for AN solutions. It is our pleasure at EANTC to contribute to this undertaking.

Test Topology

All tests were conducted in a lab scenario representing a realistic, innovative service provider network design based on Segment Routing over IPv6 (SRv6). Core, aggregation, and service edge routers were included in the test bed. The lab scenario was constructed to enable the execution of all test cases including redundancy failover. At the same time, the lab network required only a small number of routers to minimize the hardware resources needed for test execution.

Figure 1 below shows the details of the test bed. Two Huawei NetEngine 8000 routers served as provider ("P1" and "P2") routers, forming the core network in the center of the test bed. They were connected to two Huawei NE40E routers to the left side of the diagram, which served as Provider Edge ("PE1" and "PE2") routers, terminating services. These four routers together formed one Autonomous System (AS) running SRv6; see the section below for more details of the logical network design.

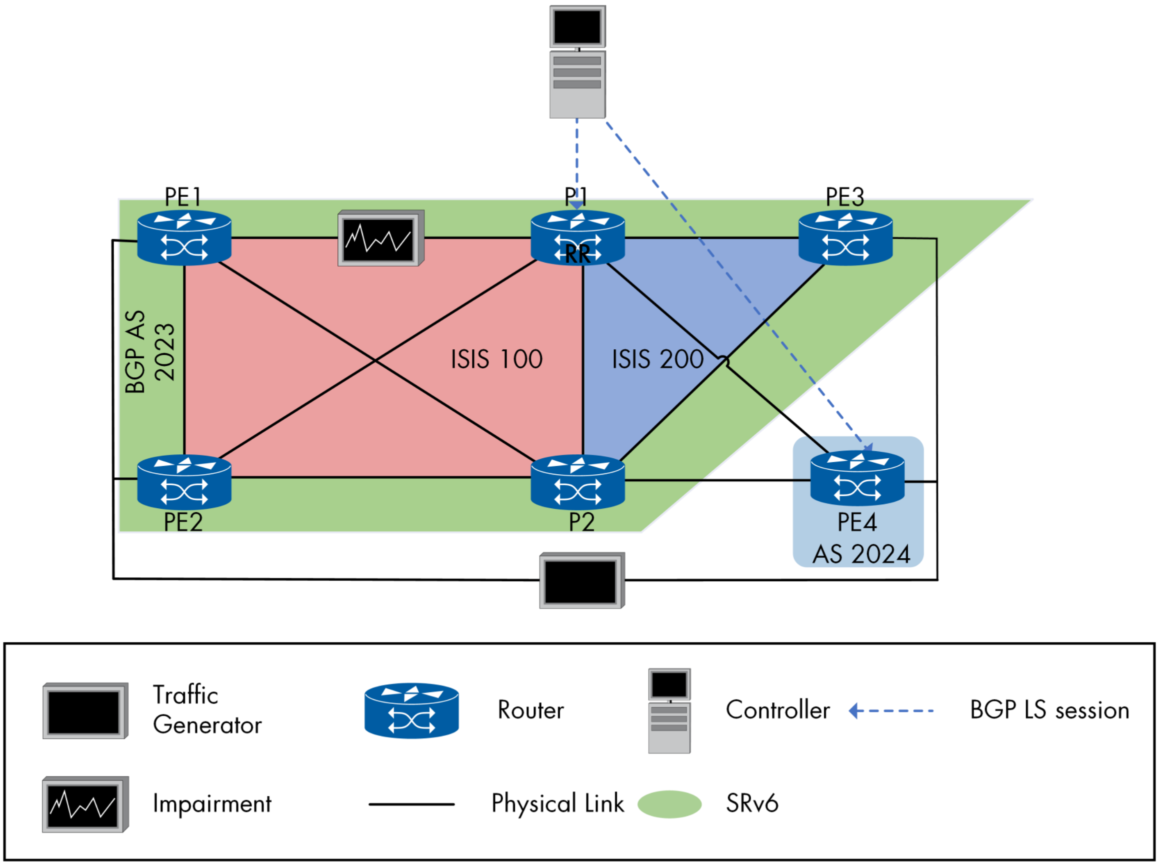


Figure 1: Test Topology

Towards the right side of the diagram, two Huawei ATN980C routers were connected and served as provider edge routers. One of them, "PE3", participated in the SRv6 domain as well and was part of another Autonomous System together with the core routers P1 and P2.

Finally, the edge router "PE4" was positioned outside the SRv6 domain, representing a legacy MPLS network with its own Autonomous System.

The main system under test was the Huawei iMaster Network Cloud Engine (NCE-IP). It controlled all routers in the test bed.

For testing purposes, a Spirent load generator was connected to each of the PE routers. It injected test traffic into the network, enabling the EANTC team to verify correct service creation, adequate latency performance, and failover out-of-service times.

An impairment generator was inserted in the link between PE1 and P1. With its help, we were able to manipulate the service quality of this link to force selective service failover activities based on quality, not just on complete loss of connectivity.

The main focus of the test bed was to facilitate functional provisioning and management tests of the iMaster NCE system. It was not optimized for performance and scalability tests, and we did not verify throughput performance or service scale aspects.

Hardware Details

The tables below list all hardware and software versions of equipment used in the test. All routers under test used production software available to customers. The iMaster NCE, however, was equipped with a pre-production beta software release not available to customers. Huawei explained that this software would be in the main branch of software development towards the next production version, scheduled to be released by Q1/2024. The reason to use pre-production software was to enable advanced test scenarios as described in this report, specifically those confirming level 4 autonomous networks.

Underlay and Overlay Networks

Based on the network architecture advice from EANTC, Huawei created two Autonomous Systems to form the core backbone for routing and exchanging data across different network segments. Additionally, the network consisted of two IS-IS routing instances. These IS-IS instances were dual-stack, supporting both IPv4 and IPv6, and were further enhanced with BGP-LS extensions for collecting link-state information.

Name	Software Version
iMaster NCE	V100R023C00B052 (unreleased)

Table 2: Controller Software

NE Name	NE Type	Software Version
PE1	NE40E-X3A(V8)	V800R022C00SPC600
PE2	NE40E-X3A(V8)	V800R022C00SPC600
PE3	ATN 980C	V800R022C00SPC600
PE4	ATN 980C	V800R022C00SPC600
P1	NetEngine 8000M8	V800R022C00SPC600
P2	NetEngine 8000X4	V800R022C00SPC600

Table 3: Network Element Hardware/Software

Name	Role	Software Version
Spirent TestCenter	Traffic generator	4.98.7626
Spirent Attero X	Impairment emulator	40.05.20

Table 4: Emulator Hardware/Software

Huawei's main architecture choice was to configure this service provider network with Segment Routing over IPv6 (SRv6). SRv6 is optimized to handle packet routing paths and implement traffic engineering service policies. Huawei created VPN services over SRv6 policies, such as L3VPNs and EVPN E-Lines.

All the underlay network configurations were manually executed. For the core, aggregation, and provider edge components in the test bed, these are complicated setup steps. Automation would be cumbersome and would not have a huge benefit because these are one-time configurations, as Huawei explained.

Although the test cases were primarily designed to confirm functionality (we did not focus performance or service scale testing at this stage yet), a total of 80 end -to-end services were configured via NCE to facilitate background data load and to create a realistic network services environment:

With the lab network physically connected, configured, and armed with background services, we were in a good position to start the testing.

Test Methodology

Before explaining the test results in detail, we'd like to quickly explain how we tested. EANTC's top-level goal in this project was to accurately determine the level of network autonomy—from L0 to L5—that the Huawei iMaster NCE system under test would provide in provisioning, troubleshooting, and optimization scenarios. EANTC chose a multi-step verification approach ensuring that our evaluation would be thorough and applicable to real-world scenarios, making the conclusions robust and valuable:

1. **Configuration Validation**: Each test case started and ended with checks of device configurations – before and after NCE introduced or modified services.

2. **Traffic Monitoring**: Throughout each test run, we generated test traffic on all foreground and background services, using the Spirent TestCenter. We monitored the traffic flow across all end-to-end services closely, validating that services were activated, or paths modified correctly. We measured failover times (by counting lost frames over time) and checked any potential effect on background service traffic as well.

3. **Protocol Identification**: In-band packet captures were used to analyze communication protocols used between the central controller and the Network Elements (NEs). Given the multitude of configuration and telemetry protocol options, we aimed to ensure proper and complete understanding of the exact protocols used by NCE to steer and monitor network elements. The goal was specifically to identify unwanted legacy protocols that might disrupt the innovative autonomous network scenario or impose a security risk (such as SNMPv2).

4. **Operator Observations**: Throughout the testing phases, we closely monitored the actual steps required by the system operator to complete each task, giving us another dimension for evaluating the network autonomy implemented by NCE.

Type of Service	EP 1	EP 2	P node	Number
L3VPN over SRv6 Policy	PE1	PE3	P1	10
L3VPN over SRv6 Policy	PE2	PE3	P2	10
L3EVPN over SRv6 Policy	PE1	PE3	P1	10
L3EVPN over SRv6 Policy	PE2	PE3	P2	10
EVPN E-Line over SRv6 Policy	PE1	PE3	P1	10
EVPN E-Line over SRv6 Policy	PE2	PE3	P2	10
L3VPN over SR TE	PE1	PE3	P1	10
L3VPN over SR TE	PE2	PE3	P2	10

Table 5: Background services configured for the test

Test Scope

In this evaluation, the system was assessed across three main areas of intelligent network operation and management:

- Advanced Network Provisioning
- Intelligent Fault Detection
- Path Optimization for IP Networks

ETSI's ENI ("Experiential Networked Intelligence") industry specification group (ISG) covers autonomous network principles and technologies. The draft standard ENI GR 035 is in its early stages; once finalized and approved, it will offer a complete framework for network operations management, featuring a closed-loop system for each individual phase and outlining the necessary management tasks at different operational levels.

Our test cases were aligned with the ETSI GR draft and exercised all stages of network autonomy.

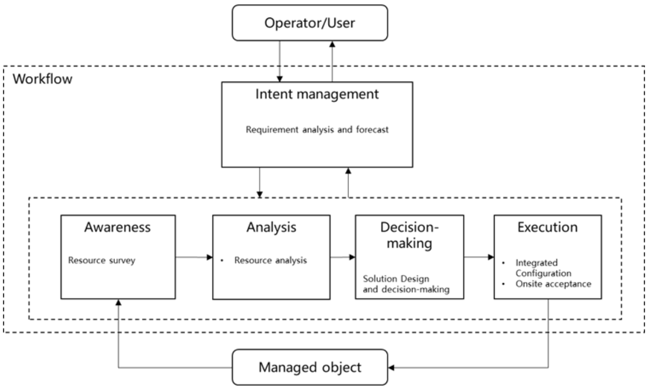


Figure 2: ETSI ENI GR 035 Reference Architecture

Test Results

The following subsections describe all test results. The network automation story of this report develops from straightforward service provisioning tasks, via monitoring and troubleshooting processes, towards automated network optimization scenarios.

1. Provisioning of VPN Services

In a Segment Routing provider network with automated service provisioning, the controller needs to offer advanced SRv6 functionalities such as SRv6 Policies and VPN overlay services. As part of a converged framework, the IP network is set up to easily manage many different services through simple input methods. The controller takes the responsibility of automatically translating network parameters for these services. Not only does it auto-deploy them, but it also verifies the service creation post-deployment. This results in a service provisioning process that is both rapid and intelligent, effectively minimizing manual intervention and speeding up the entire service rollout cycle.

First, for this and each additional test case, we checked that all network nodes and the NCE system were up and running properly before we started: Were network nodes and NCE connected properly using different communication protocols (NETCONF, SNMP, TELNET)? Were the necessary PCEP connections, BGP-LS sessions, and BGP IPv6 policy peering running? As a reminder, BGP-LS was needed to help with network topology monitoring/updates, while the BGP IPv6 policy peering was used for route exchange with a focus on influencing the data plane.

There are multiple steps required for successful automated service provisioning. First, the controller needs to develop a correct and suitable digital twin of the network situation. Second, the controller needs to allow the operator to specify the provisioning intent and needs to translate it into actions using policies and templates. We checked both parts.

✅ **NCE gathered all connectivity information and showed the correct and complete physical network topology** (see Figure 3).

During test execution, the iMaster NCE collected information on link status like bandwidth utilization (via Telemetry or SNMP), IGP metric, packet loss rate, and delay (via BGP-LS) and developed a digital twin of the network.

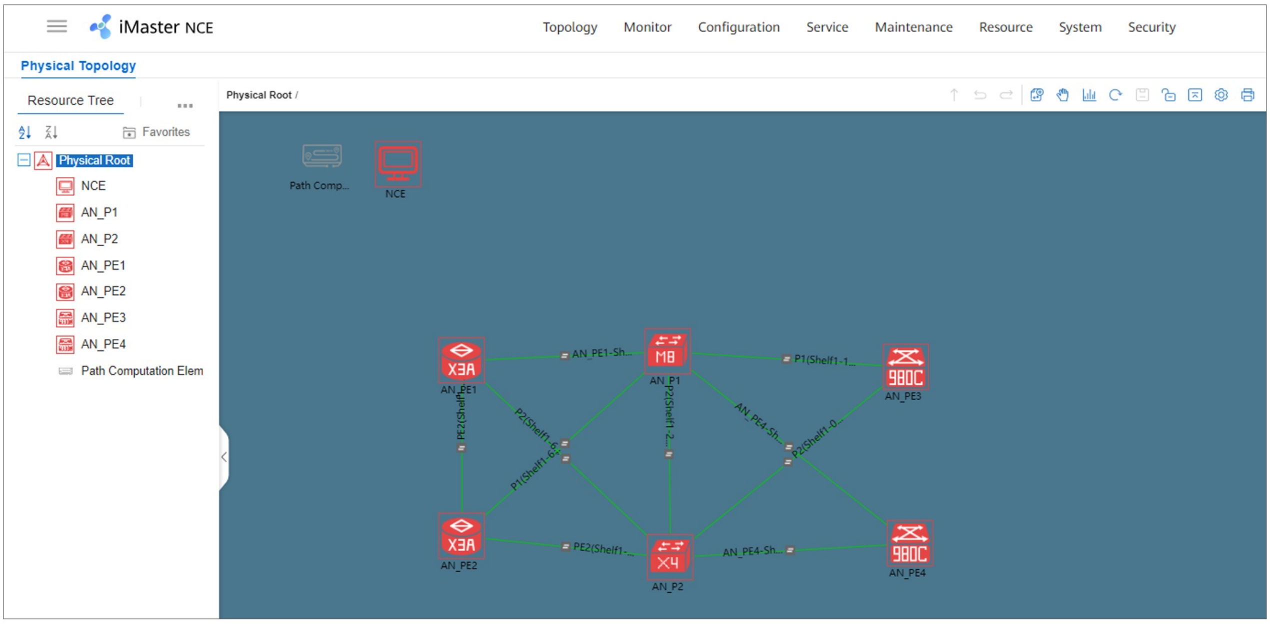


Figure 3: NCE View of Physical Network Topology

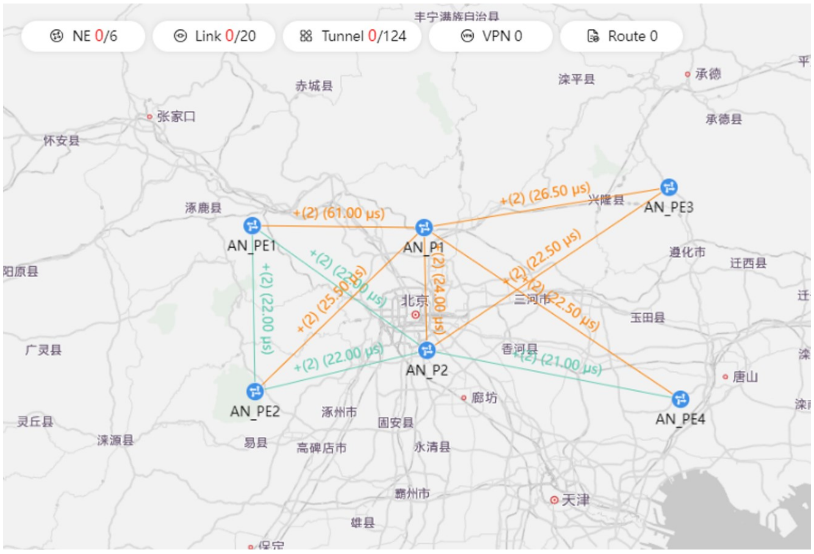


Figure 4: Digital Twin Delay View

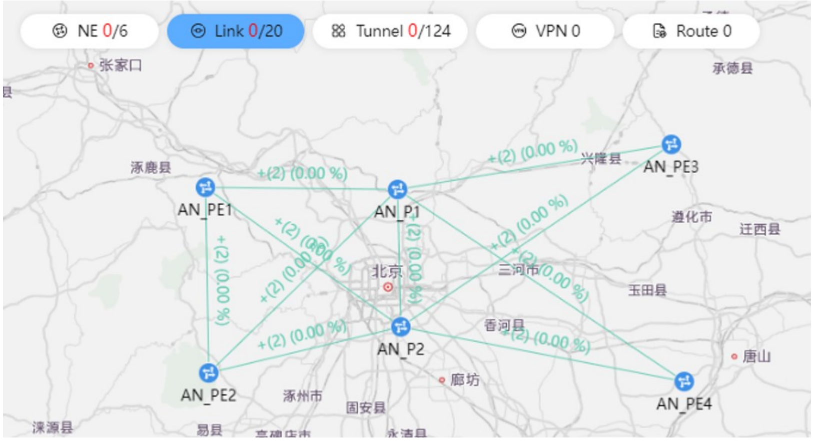


Figure 5: Digital Twin Bandwidth Utilization View

Provisioning: Intent Management Tasks

The objective is to validate the level at which provisioning intentions are translated. This involves generating service planning information, which covers PE planning, RD/RT planning, and network configuration templates. This data is then automatically converted to network technologies, such as L3VPN, along with corresponding protection requirements like VPN FRR, tunnel SRv6 policy, and SLA parameters.

✓ NCE demonstrated its ability to flexibly define service models for SRv6-based VPN services online, using service templates linked with tunnel templates.

We started by establishing tunnel templates for routers P1 and P2, setting their delay constraints at 50 ms and 100 ms, respectively. We configured the protection types to maintain a 1:1 ratio and designated which paths would serve as the primary and backup candidates.

For configuring L3EVPN templates, we chose an SRv6 policy with VPN FRR functionality enabled. Prior to this, route distinguisher (RD) and route type (RT) pools were established through resource pool management for later incorporation into the service template.

We then employed these templates to establish four L3EVPN services among PE1, PE2, and PE3 devices. To test the system's ability to update the digital twin continually, we manually forced a port-down scenario on a device; NCE successfully detected the change in interface resource status in near-real-time (the exact time between event and detection was not measured).

Additionally, we manually configured the sub-interface VLAN information and the IP address on the access ports where NCE provided prompts for available VLANs. These configurations were repeated for the remote end of the L3EVPN service (PE3).

Next, NCE calculated the tunnel path based on the delay constraints. When we increased the delay on the link between PE1 and P1, the system adjusted to maintain the service's SLA by computing new paths accordingly.

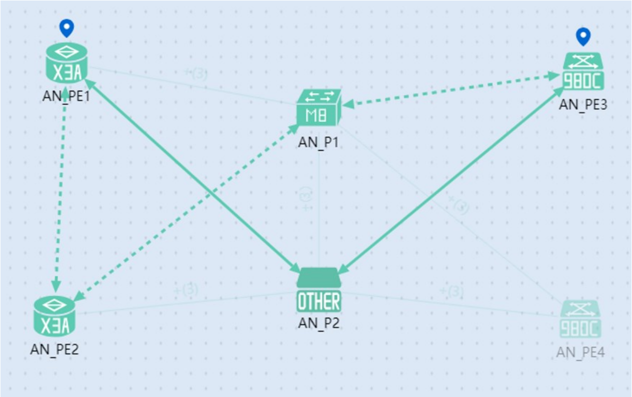
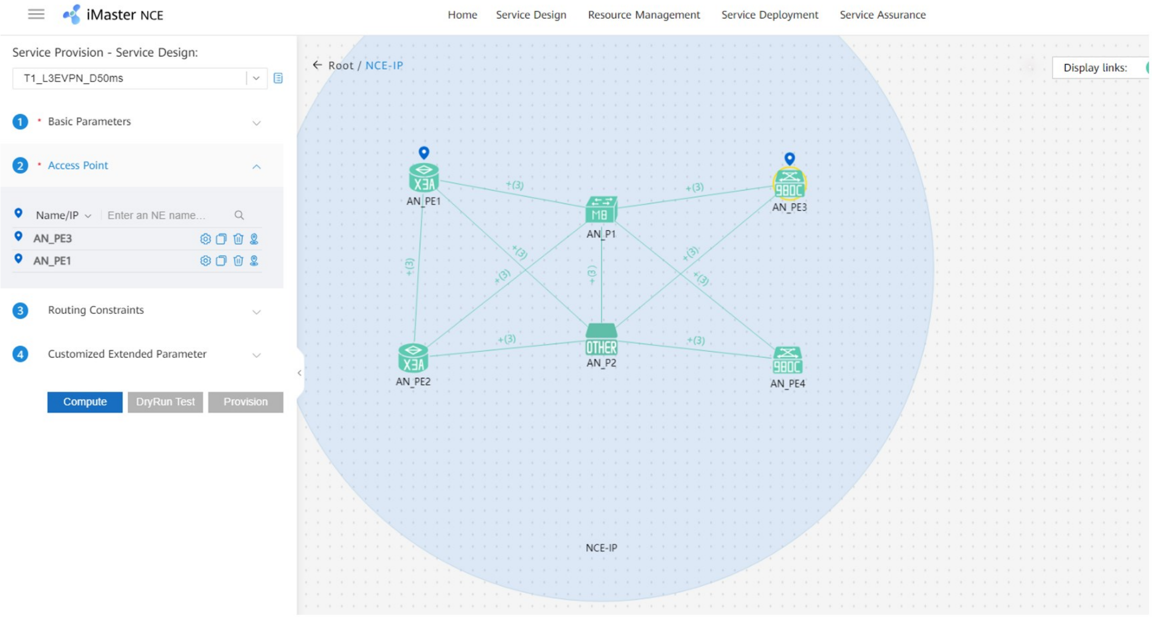


Figure 7: NCE Computed Primary and Backup Paths for S1(intent: less than 50 ms Path Latency)



Service Provision - Service Design: T1_L3EVPN_D50ms

Name/IP: Enter an NE name...
AN_PE3
AN_PE1

Figure 6: Network Status when Service Design was complete between PE1-PE3

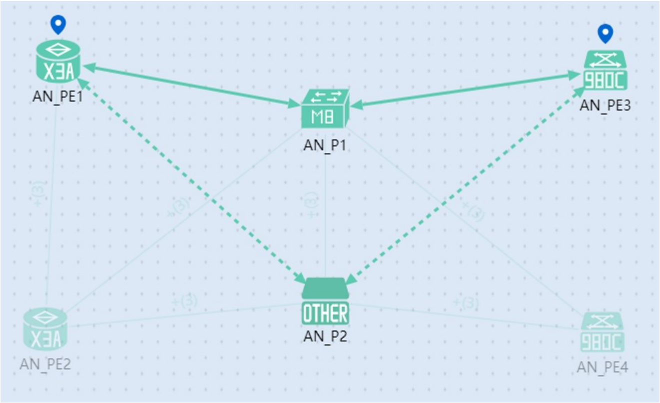


Figure 8: NCE Computed Primary and Backup Paths (less than 100 ms Path Latency)

At the same time, NCE automatically generated the service configuration based on the template and the IP resource pool information.

✓ Verdict: L4

We verified that the system can define service models dynamically. It automatically translates user requirements (intent) into network settings. This includes various configurations like VPN, interface, protection, and tunnel policies.

Provisioning: Awareness Tasks

The goal of this test case was to verify the NCE's autonomous network level concerning the network situation awareness, specifically regarding resources surveying.

For this function, NCE needs to monitor key network SLA metrics such as latency, bandwidth, and traffic continuously, while also dynamically identifying any changes in network conditions. Simultaneously, it needs to actively acquire information of available network device resources, including available ports and link bandwidth, and keep track of any resource alterations.

✓ **NCE continually monitored the network topology including the status of network resources and services. It updated the internal digital twin after a link failure within 31 seconds (average).**

We executed this test case using the same topology and services deployed previously. To verify continuous resource monitoring, we simulated a link failure between PE1 and P2 (see Figure 9). We then measured how long NCE took to change the link status. This test case was executed three times and resulted in an average status update delay of 31 seconds.

The second step was emulating delay and packet loss on a different link. The changes of delay and packet loss were reflected on the digital twin within an average time of 40-50 seconds.

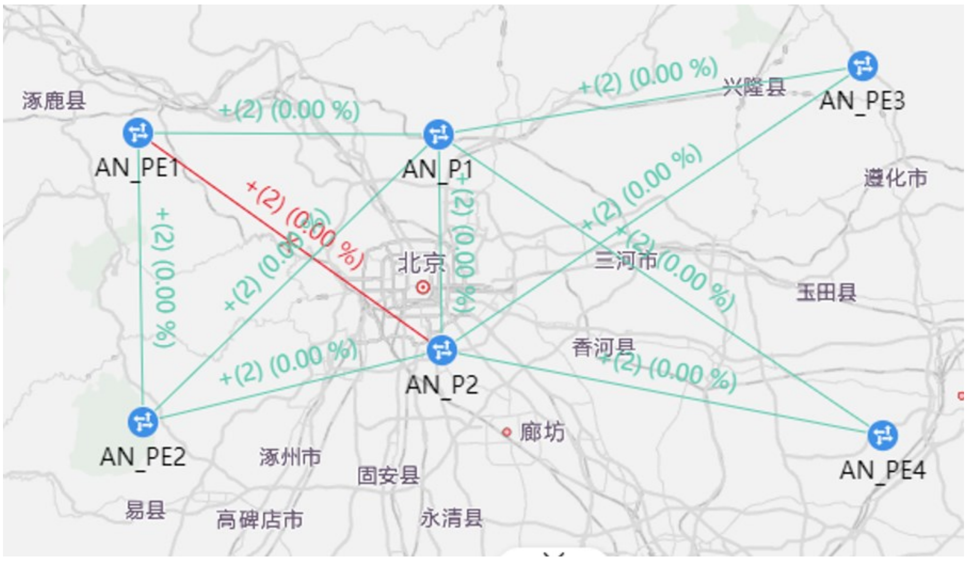


Figure 9: Link Failure Reflected by NCE's Digital Twin

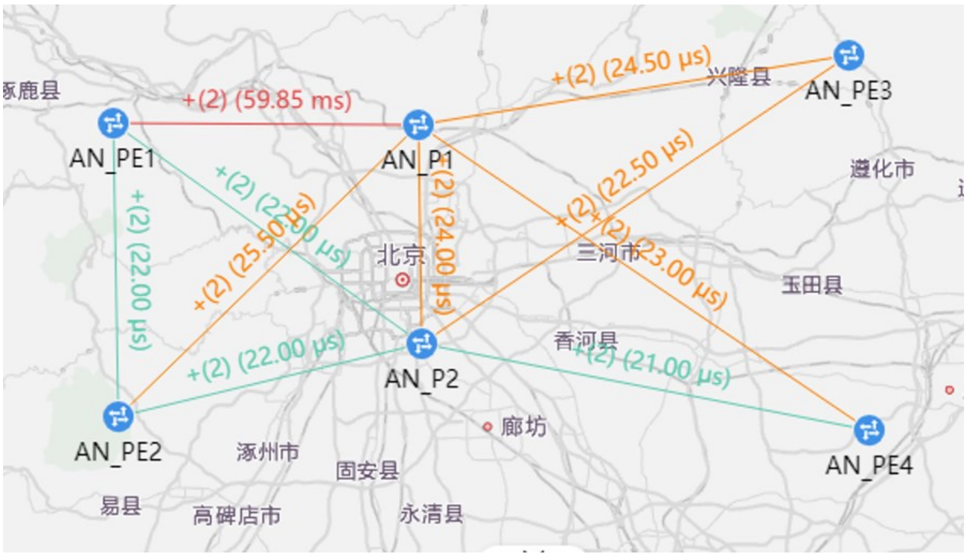
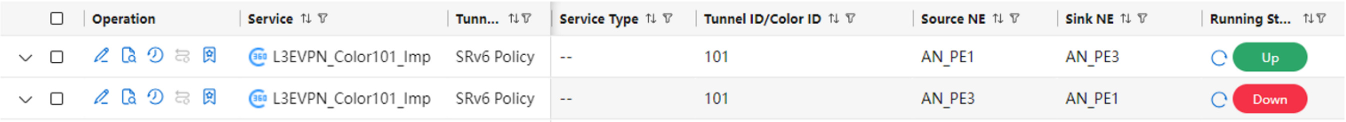


Figure 10: Emulated Delay (50 ms) between PE1-P1 Reflected on the Digital Twin



	□	Operation	Service ⇅ ▽	Tunn... ⇅ ▽	Service Type ⇅ ▽	Tunnel ID/Color ID ⇅ ▽	Source NE ⇅ ▽	Sink NE ⇅ ▽	Running St... ⇅ ▽
⌄	□		L3EVPN_Color101_Imp	SRv6 Policy	--	101	AN_PE1	AN_PE3	Up
⌄	□		L3EVPN_Color101_Imp	SRv6 Policy	--	101	AN_PE3	AN_PE1	Down

Figure 11: SRv6 Policy changed to Down

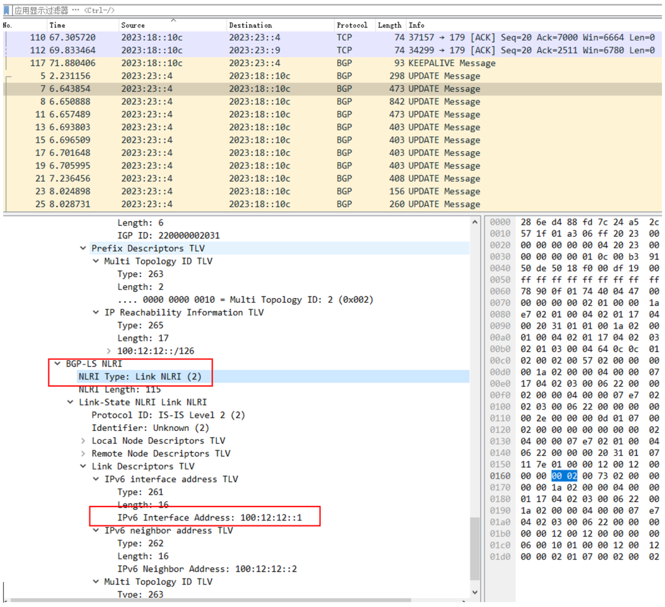
Finally, we emulated a "service down" event by removing the IPv6 address prefix from the loopback interface.

Previously, when the service was created, NCE had configured Seamless BFD (SBFD) to monitor service status between loopback interfaces at the service endpoints. By removing the address from this SBFD endpoint, the SBFD session broke down on P1 – as intended with our test. As a result, the SRv6 policy changed its status to be unavailable.

✅ **NCE correctly noticed the SRv6 policy change event within 22 seconds after the IPv6 address prefix had been removed** (see Figure 11).

For any measurements here, please keep in mind that the focus of the test was on functional verification. The NCE was running with a very low load, and the change affected only a few services. In a realistic environment, NCE might have to process many more notifications, which could affect the notification delay.

In each test run, we confirmed that updates were sent via BGP-LS packets by capturing and analyzing the data packets. To understand how NCE detected changes in link status, we monitored the packets on the NCE port and inspected the BGP update messages for changes (see Figure 12).



```
应用显示过滤器 … <Ctrl-/>
No.   Time        Source           Destination     Protocol  Length  Info
  110 67.305720   2023:18::10c     2023:23::4      TCP           74  37157 → 179 [ACK] Seq=20 Ack=7000 Win=6664 Len=0
  112 69.833464   2023:18::10c     2023:23::9      TCP           74  34299 → 179 [ACK] Seq=20 Ack=2511 Win=6780 Len=0
  117 71.880406   2023:18::10c     2023:23::4      BGP           93  KEEPALIVE Message
    5 2.231156    2023:23::4       2023:18::10c    BGP          298  UPDATE Message
    7 6.643854    2023:23::4       2023:18::10c    BGP          473  UPDATE Message
    8 6.650888    2023:23::4       2023:18::10c    BGP          842  UPDATE Message
   11 6.657489    2023:23::4       2023:18::10c    BGP          473  UPDATE Message
   13 6.693803    2023:23::4       2023:18::10c    BGP          403  UPDATE Message
   15 6.696509    2023:23::4       2023:18::10c    BGP          403  UPDATE Message
   17 6.701648    2023:23::4       2023:18::10c    BGP          403  UPDATE Message
   19 6.705995    2023:23::4       2023:18::10c    BGP          403  UPDATE Message
   21 7.236456    2023:23::4       2023:18::10c    BGP          408  UPDATE Message
   23 8.024898    2023:23::4       2023:18::10c    BGP          156  UPDATE Message
   25 8.028731    2023:23::4       2023:18::10c    BGP          260  UPDATE Message
```

```
            Length: 6
            IGP ID: 220000002031
        ⌄ Prefix Descriptors TLV
          ⌄ Multi Topology ID TLV
              Type: 263
              Length: 2
              .... 0000 0000 0010 = Multi Topology ID: 2 (0x002)
          ⌄ IP Reachability Information TLV
              Type: 265
              Length: 17
            › 100:12:12::/126
  ⌄ BGP-LS NLRI
      NLRI Type: Link NLRI (2)
      NLRI Length: 115
    ⌄ Link-State NLRI Link NLRI
        Protocol ID: IS-IS Level 2 (2)
        Identifier: Unknown (2)
      › Local Node Descriptors TLV
      › Remote Node Descriptors TLV
      ⌄ Link Descriptors TLV
        ⌄ IPv6 interface address TLV
            Type: 261
            Length: 16
            IPv6 Interface Address: 100:12:12::1
        ⌄ IPv6 neighbor address TLV
            Type: 262
            Length: 16
            IPv6 Neighbor Address: 100:12:12::2
        ⌄ Multi Topology ID TLV
            Type: 263
```

```
0000  28 6e d4 88 fd 7c 24 a5  2c
0010  57 1f 01 a3 06 ff 20 23  00
0020  00 00 00 00 00 04 20 23  00
0030  00 00 00 00 01 0c 00 b3  91
0040  50 de 50 18 f0 00 df 19  00
0050  ff ff ff ff ff ff ff ff  ff
0060  78 90 0f 01 74 40 04 47  00
0070  00 00 00 00 02 01 00 00  1a
0080  e7 02 01 00 04 02 01 17  04
0090  00 20 31 01 01 00 1a 02  00
00a0  01 00 04 02 01 17 04 02  03
00b0  02 01 03 00 04 64 0c 0c  01
00c0  02 00 02 00 57 02 00 00  00
00d0  00 1a 02 00 00 04 00 00  07
00e0  17 04 02 03 00 06 22 00  00
00f0  02 00 00 04 00 00 07 e7  02
0100  02 03 00 06 22 00 00 00  00
0110  00 2e 00 00 00 0d 01 07  00
0120  02 00 00 00 00 00 00 00  02
0130  04 00 00 07 e7 02 01 00  04
0140  06 22 00 00 00 20 31 01  07
0150  11 7e 01 00 00 12 00 12  00
0160  00 00 00 02 00 73 02 00  00
0170  00 00 1a 02 00 00 04 00  00
0180  01 17 04 02 03 00 06 22  00
0190  1a 02 00 00 04 00 00 07  e7
01a0  04 02 03 00 06 22 00 00  00
01b0  00 00 12 00 12 00 00 00  00
01c0  06 00 10 01 00 00 12 00  12
01d0  00 00 02 01 07 00 02 00  02
```

Figure 12: BGP Update Message for Link Failure

Verdict: L4

✅ **We confirmed that the system uses a digital twin for near real-time network resource monitoring. It can quickly identify network and service statuses (in seconds) as well as quality metrics. The system also automatically creates a network topology that includes resource status, available ports, link bandwidth, and service resource utilization.**

Provisioning: Analysis And Decision-Making Tasks

The next step towards automation of service provisioning are the analysis and decision-making tasks. These include the auto-allocation of resources, in this case specifically the Virtual Routing Function route descriptors and route targets [VRF RD/RT], the choice of network interfaces and VLANs. Additionally, the auto-generation of service configurations and assurance solutions contributes to the automation level of analysis and decision-making tasks as well.

To test these aspects, we increased the emulated link delay change between PE1 and P1 (see Figure 10 above) from 50 ms to 60 ms. Subsequently, we checked the template T1 path computation in NCE.

NCE correctly analyzed that the delay constraints for paths using template T1 were violated. NCE correctly took the decision to change the path so that the service adhered to the delay constraints again. The RT and RD for S1and S2 services were automatically allocated. In parallel, we checked that the path computation for template T2 didn't change because delay constraints (100 ms) of this template were not violated.

Verdict: L4

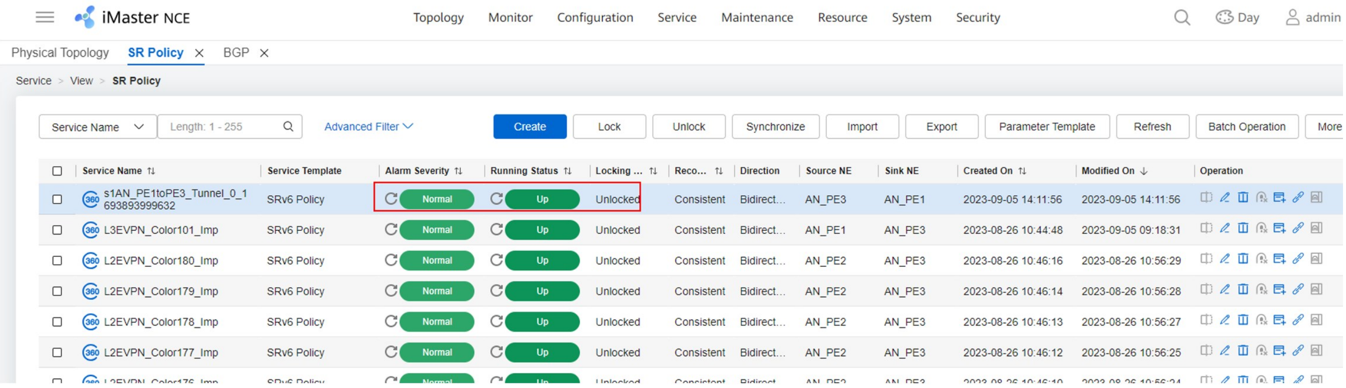
✓ **We confirmed that NCE automatically assigned network resources like RDs and RTs according to user requirements. It also calculated the best network paths and generated device configurations automatically. All these functionalities were fully simulated and tested in NCE's digital twin prior to actual rollout to network elements.**

Provisioning: Execution Tasks

As our final test step of provisioning activities, we validated the Autonomous Network's ability of implementing and verifying the provisioning actions. During this step, NCE was expected to deploy the previously created and verified configurations automatically, as per the service design. The system was expected to validate services, check the service status, and confirm if service requirements would be met.

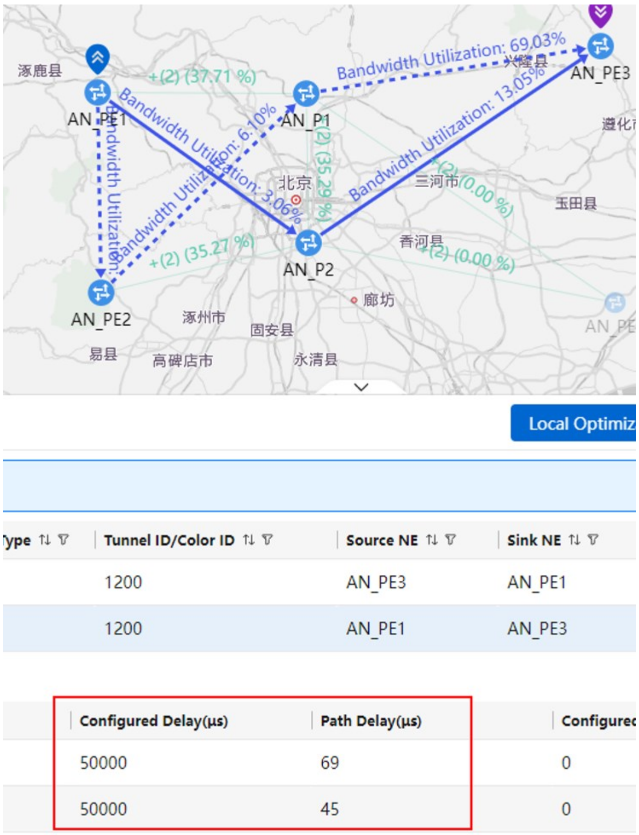
To kick off this test step, we initiated Service S1 and verified its status on the NCE, ensuring that it met the appropriate delay constraints and color ID. We then reviewed the SRv6 Policy path within NCE and confirmed that the path delay information was automatically acquired (see Figure 13). The configurations on the network nodes also reflected the newly deployed service correctly. We also verified the L3EVPN configurations on the PE1 devices.

Next, we tested the SRv6 policy path that was automatically created on the routers. We validated the service by generating traffic from its endpoints using a traffic generator; traffic was forwarded without loss. Additionally, we verified that BGP-LS updates were used to deploy the SRv6 Policy and also examined the NETCONF deployment logs on the AN system and confirmed that the details of the Huawei-specific YANG model were accurate (see Figure 15). It's worth noticing that vendors often choose to use their proprietary YANGs to quickly adapt to new features evolution while the OpenConfig can take longer time to incorporate these innovations.



□	Service Name ⇅	Service Template	Alarm Severity ⇅	Running Status ⇅	Locking ... ⇅	Reco... ⇅	Direction	Source NE	Sink NE	Created On ⇅	Modified On ↓	Operation
□	s1AN_PE1toPE3_Tunnel_0_1 693893999632	SRv6 Policy	Normal	Up	Unlocked	Consistent	Bidirect...	AN_PE3	AN_PE1	2023-09-05 14:11:56	2023-09-05 14:11:56	
□	L3EVPN_Color101_Imp	SRv6 Policy	Normal	Up	Unlocked	Consistent	Bidirect...	AN_PE1	AN_PE3	2023-08-26 10:44:48	2023-09-05 09:18:31	
□	L2EVPN_Color180_Imp	SRv6 Policy	Normal	Up	Unlocked	Consistent	Bidirect...	AN_PE2	AN_PE3	2023-08-26 10:46:16	2023-08-26 10:56:29	
□	L2EVPN_Color179_Imp	SRv6 Policy	Normal	Up	Unlocked	Consistent	Bidirect...	AN_PE2	AN_PE3	2023-08-26 10:46:14	2023-08-26 10:56:28	
□	L2EVPN_Color178_Imp	SRv6 Policy	Normal	Up	Unlocked	Consistent	Bidirect...	AN_PE2	AN_PE3	2023-08-26 10:46:13	2023-08-26 10:56:27	
□	L2EVPN_Color177_Imp	SRv6 Policy	Normal	Up	Unlocked	Consistent	Bidirect...	AN_PE2	AN_PE3	2023-08-26 10:46:12	2023-08-26 10:56:25	
□	L2EVPN_Color176_Imp	SRv6 Policy	Normal	Up	Unlocked	Consistent	Bidirect...	AN_PE2	AN_PE3	2023-08-26 10:46:10	2023-08-26 10:56:24	

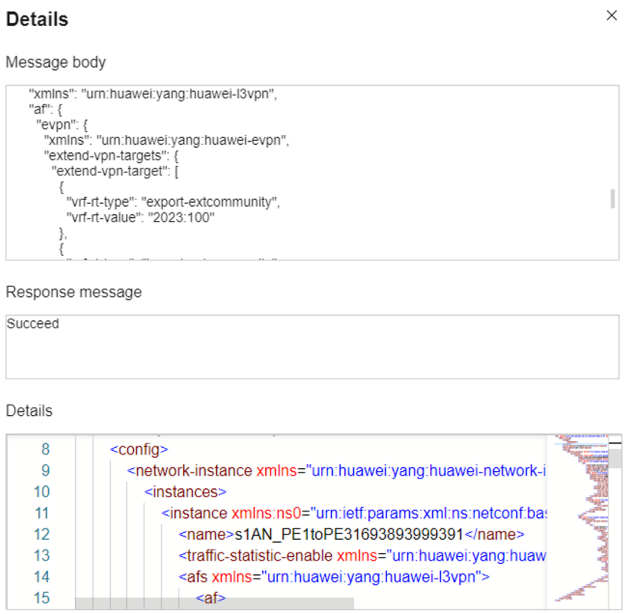
Figure 13: NCE Deployed SRv6 Policy, showing that the Policy Status is up



ype ⇅ ▽	Tunnel ID/Color ID ⇅ ▽	Source NE ⇅ ▽	Sink NE ⇅ ▽
	1200	AN_PE3	AN_PE1
	1200	AN_PE1	AN_PE3

Configured Delay(µs)	Path Delay(µs)	Configurec
50000	69	0
50000	45	0

Figure 14: Configured and Measured Path Delay



Details

Message body

```
"xmlns": "urn:huawei:yang:huawei-l3vpn",
"af": {
  "evpn": {
   "xmlns": "urn:huawei:yang:huawei-evpn",
   "extend-vpn-targets": {
    "extend-vpn-target": [
     {
      "vrf-rt-type": "export-extcommunity",
      "vrf-rt-value": "2023:100"
     },
     {
```

Response message

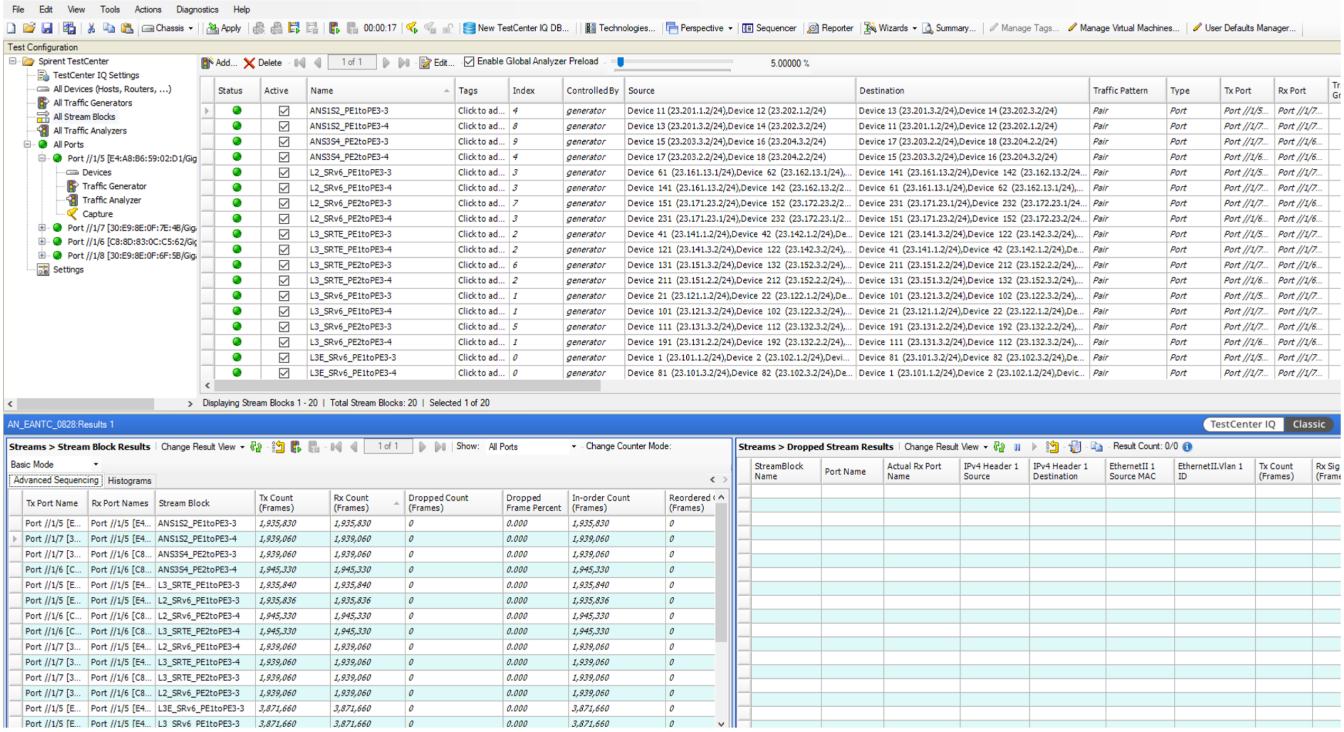
Succeed

Details

```
<config>
  <network-instance xmlns="urn:huawei:yang:huawei-network-i
    <instances>
      <instance xmlns:ns0="urn:ietf:params:xml:ns:netconf:bas
        <name>s1AN_PE1toPE31693893999391</name>
        <traffic-statistic-enable xmlns="urn:huawei:yang:huaw
        <afs xmlns="urn:huawei:yang:huawei-l3vpn">
          <af>
```

Figure 15: YANG Model used by NCE for Provisioning

We then explored the system's behavior when encountering configuration failures. Before setting up Service S3 between PE2 and PE3 devices—preassigned with the RD value 2023:102—we intentionally created a conflicting service with the same RD value through the CLI. When attempting to initiate the service, the AN system correctly flagged an error and indicated a failure in service provisioning.



Test Configuration

- Spirent TestCenter
  - TestCenter IQ Settings
  - All Devices (Hosts, Routers, ...)
  - All Traffic Generators
  - All Stream Blocks
  - All Traffic Analyzers
  - All Ports
    - Port //1/5 [E4:A8:B6:59:02:D1/Gig
      - Devices
      - Traffic Generator
      - Traffic Analyzer
      - Capture
    - Port //1/7 [30:E9:8E:0F:7E:4B/Gig
    - Port //1/6 [C8:8D:83:0C:C5:62/Gig
    - Port //1/8 [30:E9:8E:0F:6F:5B/Gig
  - Settings

☑ Enable Global Analyzer Preload 5.00000 %

Status	Active	Name	Tags	Index	ControlledBy	Source	Destination	Traffic Pattern	Type	Tx Port	Rx Port
●	☑	ANS1S2_PE1toPE3-3	Click to ad...	4	generator	Device 11 (23.201.1.2/24),Device 12 (23.202.1.2/24)	Device 13 (23.201.3.2/24),Device 14 (23.202.3.2/24)	Pair	Port	Port //1/5...	Port //1/7...
●	☑	ANS1S2_PE1toPE3-4	Click to ad...	8	generator	Device 13 (23.201.3.2/24),Device 14 (23.202.3.2/24)	Device 11 (23.201.1.2/24),Device 12 (23.202.1.2/24)	Pair	Port	Port //1/7...	Port //1/7...
●	☑	ANS3S4_PE2toPE3-3	Click to ad...	9	generator	Device 15 (23.203.3.2/24),Device 16 (23.204.3.2/24)	Device 17 (23.203.2.2/24),Device 18 (23.204.2.2/24)	Pair	Port	Port //1/7...	Port //1/6...
●	☑	ANS3S4_PE2toPE3-4	Click to ad...	4	generator	Device 17 (23.203.2.2/24),Device 18 (23.204.2.2/24)	Device 15 (23.203.3.2/24),Device 16 (23.204.3.2/24)	Pair	Port	Port //1/6...	Port //1/6...
●	☑	L2_SRv6_PE1toPE3-3	Click to ad...	3	generator	Device 61 (23.161.13.1/24),Device 62 (23.162.13.1/24),...	Device 141 (23.161.13.2/24),Device 142 (23.162.13.2/24...	Pair	Port	Port //1/5...	Port //1/7...
●	☑	L2_SRv6_PE1toPE3-4	Click to ad...	3	generator	Device 141 (23.161.13.2/24),Device 142 (23.162.13.2/2...	Device 61 (23.161.13.1/24),Device 62 (23.162.13.1/24),...	Pair	Port	Port //1/7...	Port //1/7...
●	☑	L2_SRv6_PE2toPE3-3	Click to ad...	7	generator	Device 151 (23.171.23.2/24),Device 152 (23.172.23.2/2...	Device 231 (23.171.23.1/24),Device 232 (23.172.23.1/24...	Pair	Port	Port //1/7...	Port //1/6...
●	☑	L2_SRv6_PE2toPE3-4	Click to ad...	3	generator	Device 231 (23.171.23.1/24),Device 232 (23.172.23.1/2...	Device 151 (23.171.23.2/24),Device 152 (23.172.23.2/24...	Pair	Port	Port //1/6...	Port //1/6...
●	☑	L3_SRTE_PE1toPE3-3	Click to ad...	2	generator	Device 41 (23.141.1.2/24),Device 42 (23.142.1.2/24),De...	Device 121 (23.141.3.2/24),Device 122 (23.142.3.2/24),...	Pair	Port	Port //1/5...	Port //1/7...
●	☑	L3_SRTE_PE1toPE3-4	Click to ad...	2	generator	Device 121 (23.141.3.2/24),Device 122 (23.142.3.2/24),...	Device 41 (23.141.1.2/24),Device 42 (23.142.1.2/24),De...	Pair	Port	Port //1/7...	Port //1/7...
●	☑	L3_SRTE_PE2toPE3-3	Click to ad...	6	generator	Device 131 (23.151.3.2/24),Device 132 (23.152.3.2/24),...	Device 211 (23.151.2.2/24),Device 212 (23.152.2.2/24),...	Pair	Port	Port //1/7...	Port //1/6...
●	☑	L3_SRTE_PE2toPE3-4	Click to ad...	2	generator	Device 211 (23.151.2.2/24),Device 212 (23.152.2.2/24),...	Device 131 (23.151.3.2/24),Device 132 (23.152.3.2/24),...	Pair	Port	Port //1/6...	Port //1/6...
●	☑	L3_SRv6_PE1toPE3-3	Click to ad...	1	generator	Device 21 (23.121.1.2/24),Device 22 (23.122.1.2/24),De...	Device 101 (23.121.3.2/24),Device 102 (23.122.3.2/24),...	Pair	Port	Port //1/5...	Port //1/7...
●	☑	L3_SRv6_PE1toPE3-4	Click to ad...	1	generator	Device 101 (23.121.3.2/24),Device 102 (23.122.3.2/24),...	Device 21 (23.121.1.2/24),Device 22 (23.122.1.2/24),De...	Pair	Port	Port //1/7...	Port //1/7...
●	☑	L3_SRv6_PE2toPE3-3	Click to ad...	5	generator	Device 111 (23.131.3.2/24),Device 112 (23.132.3.2/24),...	Device 191 (23.131.2.2/24),Device 192 (23.132.2.2/24),...	Pair	Port	Port //1/7...	Port //1/6...
●	☑	L3_SRv6_PE2toPE3-4	Click to ad...	1	generator	Device 191 (23.131.2.2/24),Device 192 (23.132.2.2/24),...	Device 111 (23.131.3.2/24),Device 112 (23.132.3.2/24),...	Pair	Port	Port //1/6...	Port //1/6...
●	☑	L3E_SRv6_PE1toPE3-3	Click to ad...	0	generator	Device 1 (23.101.1.2/24),Device 2 (23.102.1.2/24),Devi...	Device 81 (23.101.3.2/24),Device 82 (23.102.3.2/24),De...	Pair	Port	Port //1/5...	Port //1/7...
●	☑	L3E_SRv6_PE1toPE3-4	Click to ad...	0	generator	Device 81 (23.101.3.2/24),Device 82 (23.102.3.2/24),De...	Device 1 (23.101.1.2/24),Device 2 (23.102.1.2/24),Devic...	Pair	Port	Port //1/7...	Port //1/7...

Displaying Stream Blocks 1 - 20 | Total Stream Blocks: 20 | Selected 1 of 20

AN_EANTC_0828:Results 1

Streams > Stream Block Results | Change Result View | 1 of 1 | Show: All Ports | Change Counter Mode:

Basic Mode

Advanced Sequencing | Histograms

Tx Port Name	Rx Port Names	Stream Block	Tx Count (Frames)	Rx Count (Frames)	Dropped Count (Frames)	Dropped Frame Percent	In-order Count (Frames)	Reordered (Frames)
Port //1/5 [E...	Port //1/5 [E4...	ANS1S2_PE1toPE3-3	1,935,830	1,935,830	0	0.000	1,935,830	0
Port //1/7 [3...	Port //1/5 [E4...	ANS1S2_PE1toPE3-4	1,939,060	1,939,060	0	0.000	1,939,060	0
Port //1/7 [3...	Port //1/6 [C8...	ANS3S4_PE2toPE3-3	1,939,060	1,939,060	0	0.000	1,939,060	0
Port //1/6 [C...	Port //1/6 [C8...	ANS3S4_PE2toPE3-4	1,945,330	1,945,330	0	0.000	1,945,330	0
Port //1/5 [E...	Port //1/5 [E4...	L3_SRTE_PE1toPE3-3	1,935,840	1,935,840	0	0.000	1,935,840	0
Port //1/5 [E...	Port //1/5 [E4...	L2_SRv6_PE1toPE3-3	1,935,836	1,935,836	0	0.000	1,935,836	0
Port //1/6 [C...	Port //1/6 [C8...	L2_SRv6_PE2toPE3-4	1,945,330	1,945,330	0	0.000	1,945,330	0
Port //1/6 [C...	Port //1/6 [C8...	L3_SRTE_PE2toPE3-4	1,945,330	1,945,330	0	0.000	1,945,330	0
Port //1/7 [3...	Port //1/5 [E4...	L2_SRv6_PE1toPE3-4	1,939,060	1,939,060	0	0.000	1,939,060	0
Port //1/7 [3...	Port //1/5 [E4...	L3_SRTE_PE1toPE3-4	1,939,060	1,939,060	0	0.000	1,939,060	0
Port //1/7 [3...	Port //1/6 [C8...	L3_SRTE_PE2toPE3-3	1,939,060	1,939,060	0	0.000	1,939,060	0
Port //1/7 [3...	Port //1/6 [C8...	L2_SRv6_PE2toPE3-3	1,939,060	1,939,060	0	0.000	1,939,060	0
Port //1/5 [E...	Port //1/5 [E4...	L3E_SRv6_PE1toPE3-3	3,871,660	3,871,660	0	0.000	3,871,660	0
Port //1/5 [E...	Port //1/5 [E4...	L3_SRv6_PE1toPE3-3	3,871,660	3,871,660	0	0.000	3,871,660	0

Streams > Dropped Stream Results | Change Result View | Result Count: 0/0

StreamBlock Name	Port Name	Actual Rx Port Name	IPv4 Header 1 Source	IPv4 Header 1 Destination	EthernetII 1 Source MAC	EthernetII.Vlan 1 ID	Tx Count (Frames)	Rx Sig (Frame

Figure 16: Generated Traffic over the New Services

Subsequently, no S3 service information was found on the PE2 and PE3 devices, indicating that the configuration had been automatically rolled back.

After removing the conflicting RD VPN configuration from the router, we reattempted provisioning Service S3, which was successful this time. Upon deploying the fourth service, we checked the status of all newly implemented services and confirmed their correct operation by generating traffic over them, again observing no packet loss.

In an additional experiment, we set up a Layer 3 Ethernet VPN (L3EVPN) service using Segment Routing over IPv6 (SRv6) policies across multiple Autonomous Systems (AS). To achieve egress peer engineering, we employed the BGP Egress Peer Engineering (EPE) extension, which enables the allocation of BGP peer (SIDs) to routes between different ASs. This information was then propagated to the network controller through the BGP-LS protocol.

Utilizing Huawei's NCE, we configured the SRv6 policy between PE1 in AS 2023 and PE4 in AS 2024, following the same procedure as previously outlined. The test was successful; we confirmed the applied configurations on the routers and observed no packet loss during traffic generation.

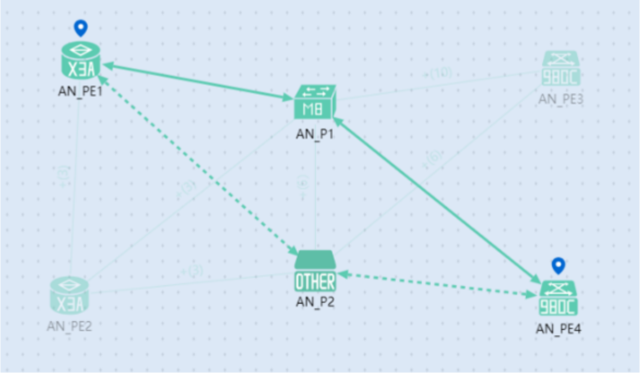


Figure 17: Primary and Backup Path for S6

Verdict: L4

✓ **NCE correctly automated the service configuration delivery; it automatically checked and validated the service status to ensure the actual deployment would meet the specified requirements. In case the delivery failed, all configurations were correctly rolled back.**

2. Monitoring and Troubleshooting in the Maintenance Process

Automated service fault management enables rapid identification of service issues, enhanced root cause analysis, and self-repair mechanisms. It should cover fault detection, alerts for potential network issues, smart automated diagnosis, and auto-adjustment of service paths.

For the tests in the monitoring and troubleshooting section, we reused the previously deployed four VPN services in the SRv6 lab topology. All of them traversed through L1 (PE1-P1 link) and some of them used L6 (PE2-P2 link) for a backup link.

We evaluated the five steps for autonomous network deployments in this section, in the same way as we had done it for provisioning activities: Intent management, awareness, analysis, decision-making, and execution tasks.

Monitoring: Intent Management Tasks

The autonomous network's desired capability for scenario-specific monitoring involves comprehending the intended objectives for service monitoring, assurance, and fault analysis. These intentions are then executed through the system's internal processing logic.

Huawei explained that NCE features a monitoring tool that utilizes Huawei’s proprietary “IFIT” telemetry protocol (IFIT stands for “In-situ Flow Information Telemetry”). This protocol uses actual service packets to gauge key performance metrics of an IP network, including packet loss rate and latency. Additionally, the tool offers visualization features for operations and maintenance, allowing for centralized network management and graphical representation of performance data.

To use the feature, we configured NCE to monitor the four L3EVPN services previously provisioned, including the respective EVPN endpoints. The IFIT flow detection was performed through Static VPN and Peer IP/Peer Locator sequences.

The measurement mode was set to capture latency, bandwidth, and packet loss metrics. Upon completing these steps, NCE successfully created a monitoring instance for the selected L3VPN services, enabling near-real-time performance tracking and evaluation.

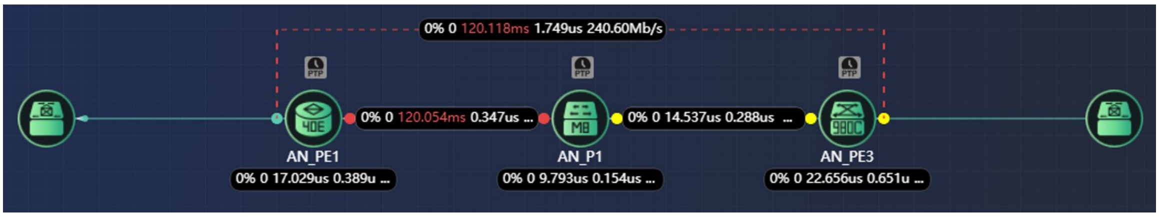


Figure 18: S2 Live Monitoring Topology

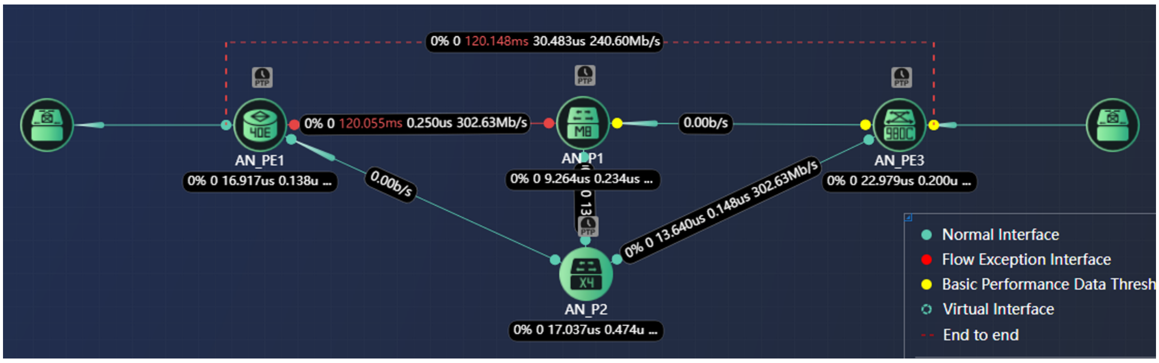


Figure 19: S2 Topology Reflects Use of the Backup Path

✓ The iMaster NCE presented a visual and near-live monitoring representation of network devices and link status. We verified that the system comes with pre-configured fault analysis correlation rules. These rules can be manually selected to align with the specific requirements for analyzing service faults.

Verdict: L3

Monitoring: Awareness Tasks

Huawei explained that NCE automatically sets up comprehensive monitoring for services, covering end-to-end SLA metrics, traffic, and the status of network components. Additionally, the system employs AI techniques to automatically recognize network issues, consolidating various alarms into streamlined alerts for more efficient fault identification.

To validate the claim, the Huawei team manually deactivated the link between P1 and PE3 using the router's command-line interface. The router triggered SNMP alarms within ten seconds, and NCE updated the service status and topology just as quickly.

Figures 18 and 19 illustrate a change in the primary path from (PE1-P1-PE3) to the backup path (PE1-P2-P1-PE3) to avoid the failed link between P1 and PE3.

The Service S1 initially had a primary path of PE1-P2-PE3 (adhering to the delay constraints of 50ms) and was not supposed to be affected by the deployed failure.

However, an unexpected packet loss on the S1 traffic was observed, with the IFIT topology revealing the activation of a backup path. The Huawei team clarified that this occurred because the S-BFD packets utilized the shortest IGP path in the reverse direction (PE3 to PE1), not through the SRv6 tunnel, causing the control packets to get lost on the way to the headend. This led NCE to presume the path was down, subsequently tearing down the SRv6 tunnel. The issue was resolved by the Huawei team subsequently, by reconfiguring BFD in the reverse direction through the SRv6 tunnel.

Huawei explained that NCE uses an AI tool called "Intelligent Incident Management" to support monitoring. The Intelligent Incident Management tool has two main aspects:

- Alarm Clustering: Utilizes frequent itemset mining algorithms. After training, the model calculates confidence levels based on time and topology features to cluster related alarms.
- Root Cause Identification: Operates in two modes:
  - → Expert Experience Injection: Uses pre-collected expert experience as feature input to identify root causes.
  - → Neural Network Training: Undergoes offline training using association matrices and fault propagation diagrams to create a causality matrix, aiding in root cause identification.

It took the AI tool twelve (12) minutes to pinpoint the root cause of the fault and to provide visual representation of the location of the fault.

In a subsequent test involving the shutdown of two interfaces (on L1 and L6 links), we received distinct, aggregated alarms for each incident, complete with an updated topology pinpointing the locations.

✅ Verdict: L4

The system identified service status changes and network metrics within minutes during the test. It also used AI and flow-based detection to automatically pinpoint network issues and aggregate alarms for root fault identification; this step took 12 minutes in the test.

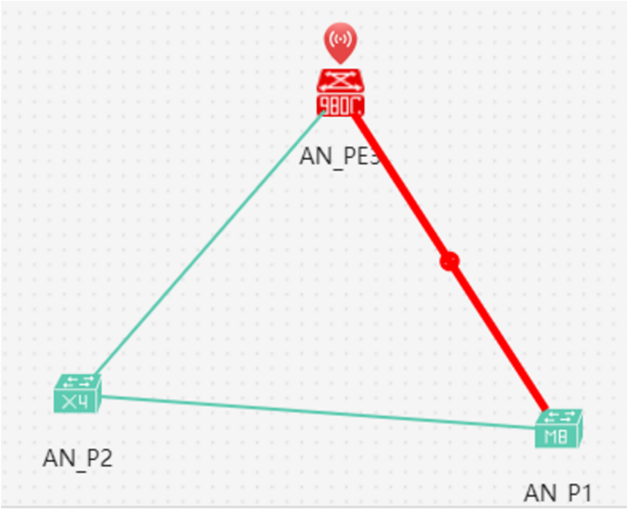


Figure 20: Failure Location

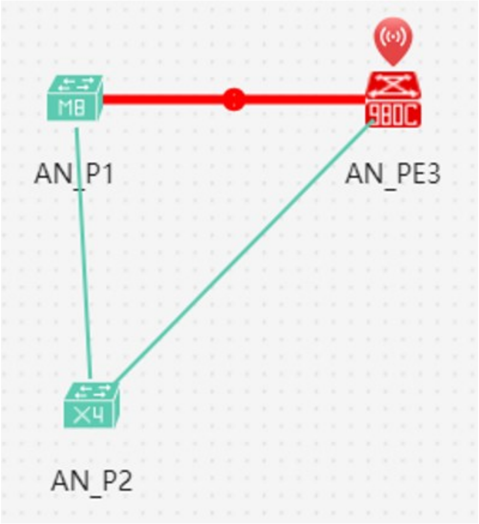
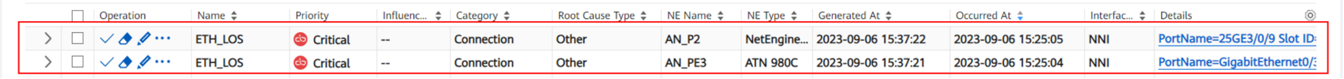


Figure 23: Location of the Second Failure



	☐	Operation	Name	Priority	Influenc...	Category	Root Cause Type	NE Name	NE Type	Generated At	Occurred At	Interfac...	Details
>	☐	✓	ETH_LOS	Critical	--	Connection	Other	AN_P2	NetEngine...	2023-09-06 15:37:22	2023-09-06 15:25:05	NNI	PortName=25GE3/0/9 Slot ID:
>	☐	✓	ETH_LOS	Critical	--	Connection	Other	AN_PE3	ATN 980C	2023-09-06 15:37:21	2023-09-06 15:25:04	NNI	PortName=GigabitEthernet0/:

Figure 21: Root fault of the generated alarms

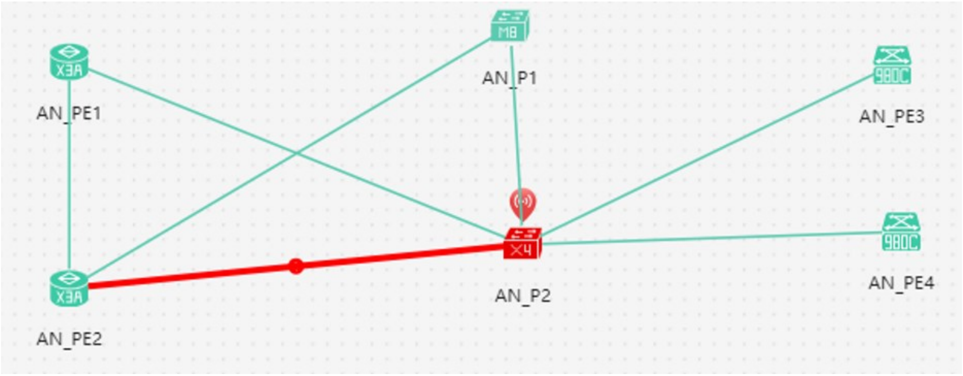


Figure 22: Location of one Failure

Monitoring: Analysis Tasks

This automation task includes demarcation and location of failures. NCE is expected to detect and analyze service flows for hop-by-hop diagnosis. This way, NCE shall swiftly isolate service issues, correlate them with network-level problems, and pinpoint the smallest unit needing replacement.

EANTC verified these tasks as part of the previous (awareness task) test. NCE correctly identified and located the faults (using the previously described AI tool). However, NCE did not perform any automated tests for diagnose purposes. For this reason, NCE's monitoring capabilities do not qualify for Autonomous Networks Level 4 from EANTC's perspective. NCE is not capable of hop-by-hop fault localization yet; instead, it relies on end-to-end alarm data which does not enable fully automated analysis.

✓ Verdict: L3

Monitoring: Decision-making Tasks

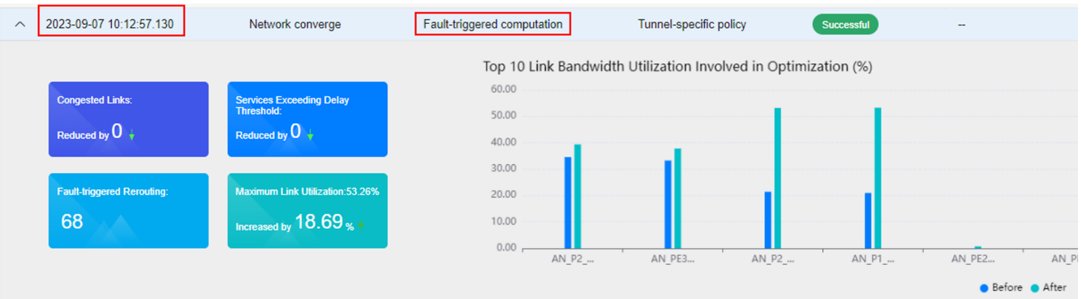
After detecting a service fault, NCE is expected to evaluate the network status and automatically compute alternative paths online, based on path computation policies and service SLA requirements.

NCE performs all decision-making operations automated and without user notification, as Huawei explained. To evaluate whether decision-making would take place, EANTC and Huawei checked the Optimization history in the NCE application as part of this test.

We manually shut down a physical interface and found that NCE correctly calculated the alternative paths, while still abiding with the tunnels delay constraints (50 ms or 100 ms) for primary and backup paths. The triggers for path calculations and the optimization result are shown in figures 24 and 25 below.

✓ Verdict: L4

After identifying a service issue, NCE correctly calculated backup routes in line with policy and service quality standards. The chosen solution was pre-verified by NCE in a digital twin before implementation.



2023-09-07 10:12:57.130 | Network converge | Fault-triggered computation | Tunnel-specific policy | Successful | --

Congested Links: Reduced by 0

Services Exceeding Delay Threshold: Reduced by 0

Fault-triggered Rerouting: 68

Maximum Link Utilization:53.26% Increased by 18.69 %

Figure 24: Decision Making Triggers

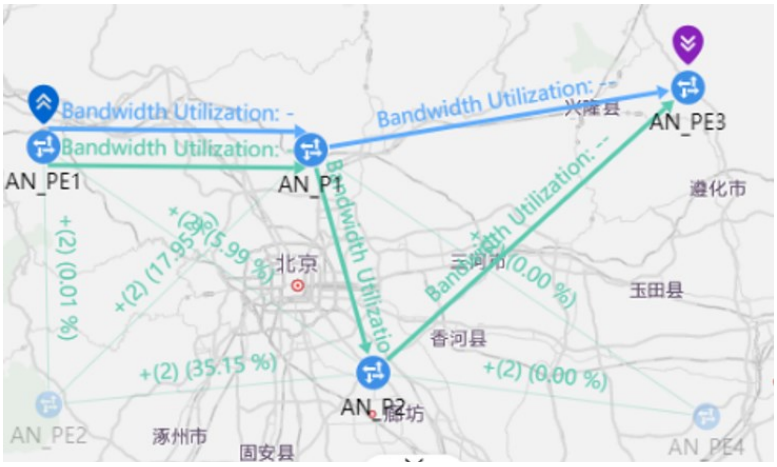


Figure 25: Before and After Path Optimization

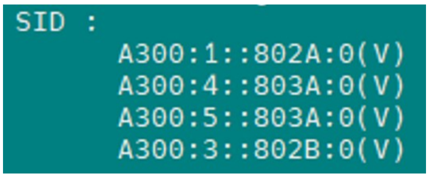
Monitoring: Execution Tasks

As the final part of automated monitoring and troubleshooting, NCE is expected to automatically complete the service verification and check whether the damaged services are recovered, including whether the service connectivity and SLA meet the requirements (again).

In our test, NCE automatically reviewed the policy state and SLA metrics for the path subsequently to the optimization steps described above. NCE showed the configured constraints (delay, bandwidth, and packet loss) including the then-current telemetry values of the established path (see Figure 26).

Then, for each path, the system was able to provide the actual SRv6 SID information for each hop along the segments (for S2, it consisted of four SIDs). These SIDs were also displayed on the end device PE1 as the utilized SIDs, directing traffic through the primary path (see figures 26 and 27).

✅ **NCE correctly acted on the triggered faults and pushed new SRv6 policy paths to the devices through BGP.**

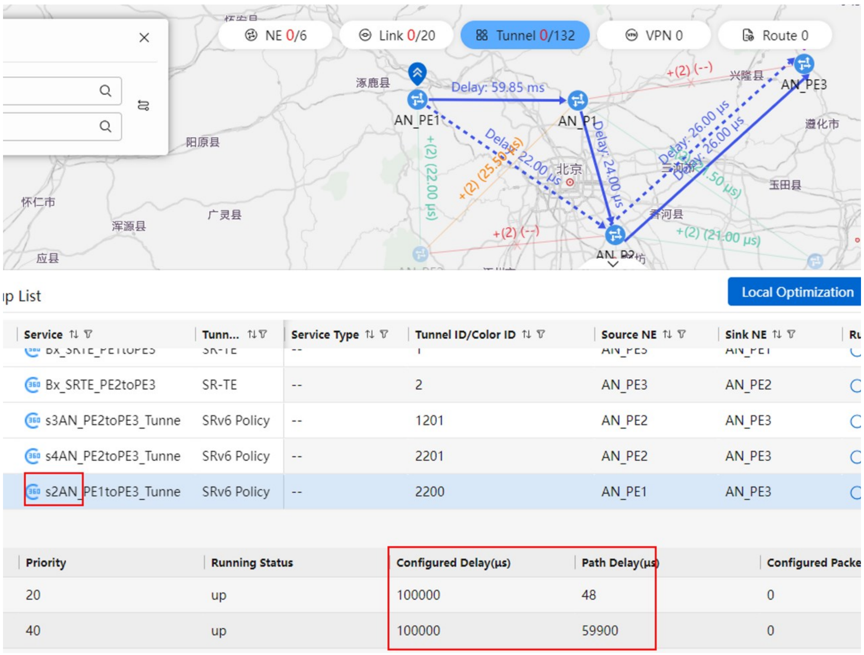


```
SID :
       A300:1::802A:0(V)
       A300:4::803A:0(V)
       A300:5::803A:0(V)
       A300:3::802B:0(V)
```

Figure 28: S2 SRv6 Candidate Path SIDs on PE1

To validate the technique NCE employed to push configurations for SRv6 policy path information, the Huawei team captured packets between NCE and the directly attached router (the route reflector). Analyzing the captured packet exchange, we confirmed that the modifications were carried out through BGP update messages as desired.

EANTC inspected the sub-TLVs (Type Length Values) within the tunnel encapsulation attribute of the network packets (see Figure 29), which is crucial for specifying the encapsulation and transportation mechanisms of packets across a tunnel. We noticed that the segment list within these sub-TLVs corresponds accurately with the SRv6 Segment Identifier (SID) values that the Network Control Engine (NCE) displayed and configured on the devices.

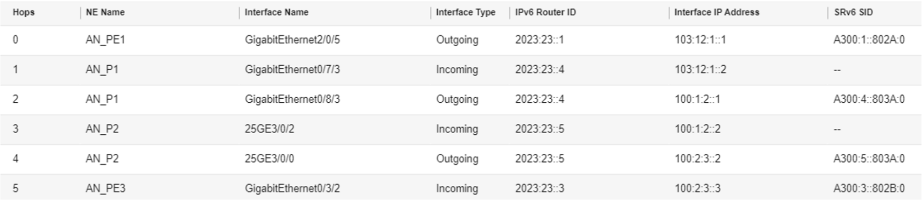


ıp List

Service	Tunn...	Service Type	Tunnel ID/Color ID	Source NE	Sink NE	Ru
Bx_SRTE_PE1toPE3	SR-TE	--	1	AN_PE3	AN_PE1	
Bx_SRTE_PE2toPE3	SR-TE	--	2	AN_PE3	AN_PE2	
s3AN_PE2toPE3_Tunne	SRv6 Policy	--	1201	AN_PE2	AN_PE3	
s4AN_PE2toPE3_Tunne	SRv6 Policy	--	2201	AN_PE2	AN_PE3	
s2AN_PE1toPE3_Tunne	SRv6 Policy	--	2200	AN_PE1	AN_PE3	

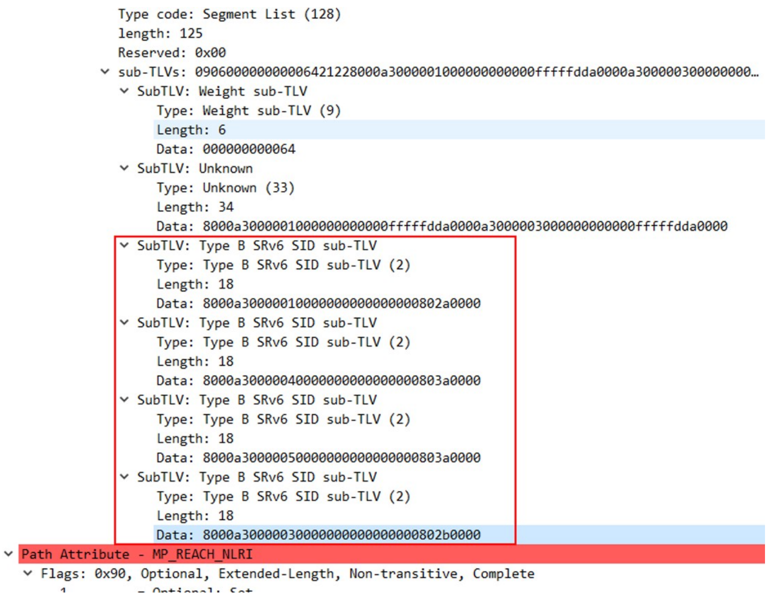
Priority	Running Status	Configured Delay(µs)	Path Delay(µs)	Configured Packe
20	up	100000	48	0
40	up	100000	59900	0

Figure 26: SLA Metrics for the new Deployed Path for S2



Hops	NE Name	Interface Name	Interface Type	IPv6 Router ID	Interface IP Address	SRv6 SID
0	AN_PE1	GigabitEthernet2/0/5	Outgoing	2023:23::1	103:12:1::1	A300:1::802A:0
1	AN_P1	GigabitEthernet0/7/3	Incoming	2023:23::4	103:12:1::2	--
2	AN_P1	GigabitEthernet0/8/3	Outgoing	2023:23::4	100:1:2::1	A300:4::803A:0
3	AN_P2	25GE3/0/2	Incoming	2023:23::5	100:1:2::2	--
4	AN_P2	25GE3/0/0	Outgoing	2023:23::5	100:2:3::2	A300:5::803A:0
5	AN_PE3	GigabitEthernet0/3/2	Incoming	2023:23::3	100:2:3::3	A300:3::802B:0

Figure 27: S2 SRv6 SIDs for the Primary Path on NCE



```
        Type code: Segment List (128)
        length: 125
        Reserved: 0x00
      ⌄ sub-TLVs: 090600000000006421228000a30000010000000000000ffffdda0000a300000300000000…
        ⌄ SubTLV: Weight sub-TLV
            Type: Weight sub-TLV (9)
            Length: 6
            Data: 000000000064
        ⌄ SubTLV: Unknown
            Type: Unknown (33)
            Length: 34
            Data: 8000a30000010000000000000ffffdda0000a30000030000000000000ffffdda0000
        ⌄ SubTLV: Type B SRv6 SID sub-TLV
            Type: Type B SRv6 SID sub-TLV (2)
            Length: 18
            Data: 8000a30000010000000000000000802a0000
        ⌄ SubTLV: Type B SRv6 SID sub-TLV
            Type: Type B SRv6 SID sub-TLV (2)
            Length: 18
            Data: 8000a30000040000000000000000803a0000
        ⌄ SubTLV: Type B SRv6 SID sub-TLV
            Type: Type B SRv6 SID sub-TLV (2)
            Length: 18
            Data: 8000a30000050000000000000000803a0000
        ⌄ SubTLV: Type B SRv6 SID sub-TLV
            Type: Type B SRv6 SID sub-TLV (2)
            Length: 18
            Data: 8000a30000030000000000000000802b0000
⌄ Path Attribute - MP_REACH_NLRI
  ⌄ Flags: 0x90, Optional, Extended-Length, Non-transitive, Complete
```

Figure 29: S2 Segment SIDs Updated through BGP-LS Packet

✅ Verdict: L4

NCE automatically adjusted service paths and validated the successful deployment of services, ensuring both connectivity and SLA compliance.

3. Network Optimization— Intelligent IP Network Path Optimization

The final step in operating autonomous networks is to optimize services without human interaction. The network's ability to respond to a failure is as crucial as being proactive and vigilant towards the potential deterioration of the service quality. We tested the capabilities of Huawei's NCE solution in this area.

The necessary optimization functions involve gathering information from the traffic flows and measuring various performance metrics such as latency, throughput, and packet loss. Through the analysis of these metrics, strategic changes are made to eliminate bottlenecks and optimize network resources, thereby improving the network's overall performance and efficiency.

Optimization: Intent Management Tasks

We validated whether NCE would be able to define service goals and thresholds, select predictive algorithms, and set rules for path calculations and traffic adjustments.

All tests in this section used the same architecture and services as in the previous areas. Initially, we distributed these services' traffic across two links. We started the test by changing the packet loss tolerance to 5 %, and service delay constraints to 100 ms.

The Huawei team enabled "Automatic optimization targeting improvements" for delay, traffic, and packet loss metrics. These optimizations were set to be performed at five-minute intervals.

NCE provides an "Auto Approval" feature for optimizations. When turned on, optimizations are executed immediately without a manual approval step – which is an active choice with advantages and disadvantages that each network operator needs to take individually. We chose to evaluate "Auto Approval" in both settings—activated and deactivated. These configurations allowed the controller to effectively understand and implement the intended network path optimizations.

✓ Verdict: L3

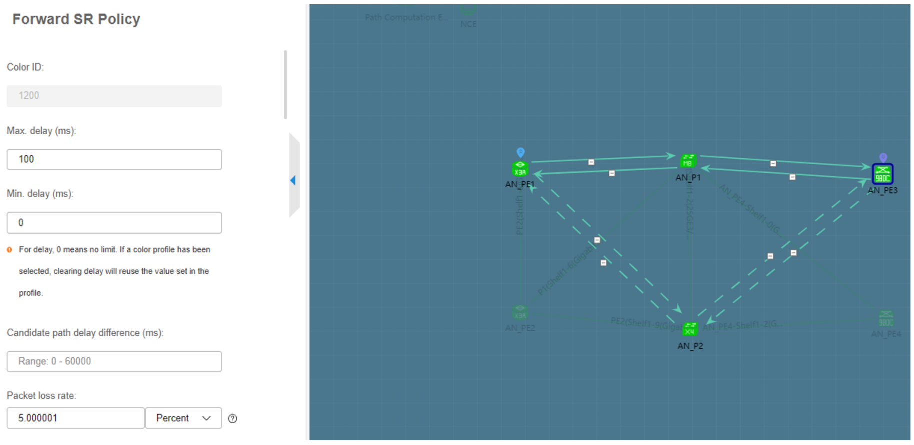
NCE provides built-in optimization correlation rules. These rules need to be manually selected to match optimization requirements (latency, bandwidth, and packet loss rate).

Optimization: Awareness Tasks

The purpose of this test was to validate the system's capability to automatically gather and update key network metrics, including bandwidth, delay, packet loss rate, and the status of tunnels.

Huawei informed us that NCE systematically collects these metrics from tunnels and links on all network devices through Telemetry for SRv6 policy traffic, SNMP for link traffic and BGP-LS. During the testing process, we introduced specific changes to the network environment: A packet loss rate of 8 % on link L3 (PE1-P1) using an impairment device, a static delay of 100 ms on L6 (PE2-P2 link) through link configuration and increased bandwidth utilization over the threshold of 70 % using a packet generator.

NCE mirrored these simulated conditions into its digital twin. The identification and reflection of delay and packet loss changes in the digital twin were accomplished within less than ten seconds.



Forward SR Policy

Color ID: 1200

Max. delay (ms): 100

Min. delay (ms): 0

For delay, 0 means no limit. If a color profile has been selected, clearing delay will reuse the value set in the profile.

Candidate path delay difference (ms): Range: 0 - 60000

Packet loss rate: 5.000001 Percent

Figure 30: Modify SR Policy Delay, Packet Loss Rate Thresholds

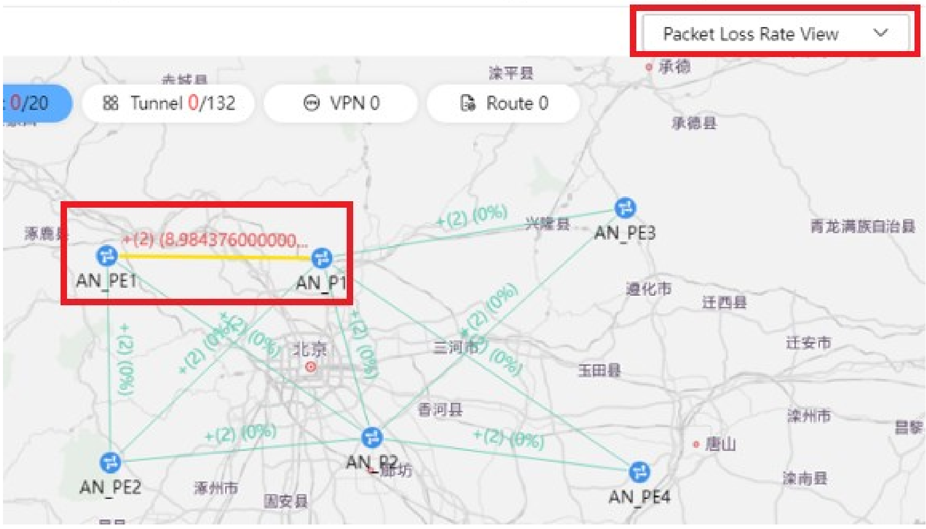


Figure 31: Digital Twin Reflecting the Applied Packet Loss

Meanwhile, updating the traffic conditions within the tunnels based on these changes was effectively carried out in less than ten minutes.

✓ Verdict: L4

The system automatically detected delay, packet loss rate, and link status change in seconds; and detected the link and tunnel traffic changes within ten minutes.

Optimization: Analysis Tasks

To identify the optimization possibilities, NCE needs to quickly assess network traffic based on alerts or exceeded thresholds for delay, bandwidth, and packet loss. Then it identifies the TE tunnels needing optimization based on service traffic requirements. The system offered two approaches, both of which we assessed:

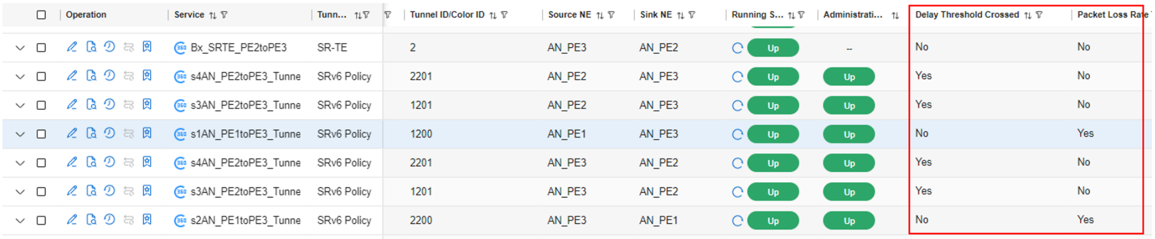
- The first is an automatic method that identifies and acts on any exceeded thresholds for delay, packet loss, or bandwidth usage, with a record of these actions available in the optimization history.
- The second method requires operator approval before implementing any changes, allowing the operator to review and accept the suggested alternatives. In practical applications, operators often appreciate having these decision-making options.

Automatic Approach

The controller offered an overview of the SRv6 Policies analysis results.

Following the completion of the auto-optimization interval, the controller implemented the required adjustments to align with the pre-configured tunnel parameters and thresholds. The procedure was executed automatically in the designated "Auto Optimization Mode." We investigated NCE's history records to review the system analysis results thoroughly.

Figure 33 shows the pre- and post-optimization paths for Service 3. The backup path, which previously followed a particular route, was altered to bypass the link with the heightened delay value, ensuring adherence to the Service Level Agreement (SLA) of S3.



□	Operation	Service	Tunn...	Tunnel ID/Color ID	Source NE	Sink NE	Running S...	Administrati...	Delay Threshold Crossed	Packet Loss Rate
□		Bx_SRTE_PE2toPE3	SR-TE	2	AN_PE3	AN_PE2	Up	--	No	No
□		s4AN_PE2toPE3_Tunne	SRv6 Policy	2201	AN_PE2	AN_PE3	Up	Up	Yes	No
□		s3AN_PE2toPE3_Tunne	SRv6 Policy	1201	AN_PE2	AN_PE3	Up	Up	Yes	No
□		s1AN_PE1toPE3_Tunne	SRv6 Policy	1200	AN_PE1	AN_PE3	Up	Up	No	Yes
□		s4AN_PE2toPE3_Tunne	SRv6 Policy	2201	AN_PE3	AN_PE2	Up	Up	Yes	No
□		s3AN_PE2toPE3_Tunne	SRv6 Policy	1201	AN_PE3	AN_PE2	Up	Up	Yes	No
□		s2AN_PE1toPE3_Tunne	SRv6 Policy	2200	AN_PE3	AN_PE1	Up	Up	No	Yes

Figure 32: Status of Services

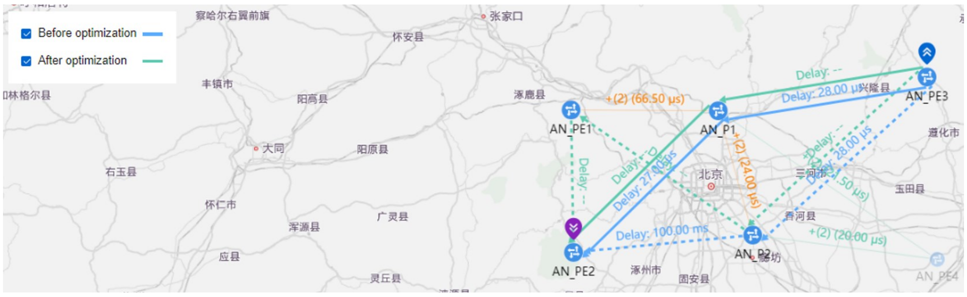
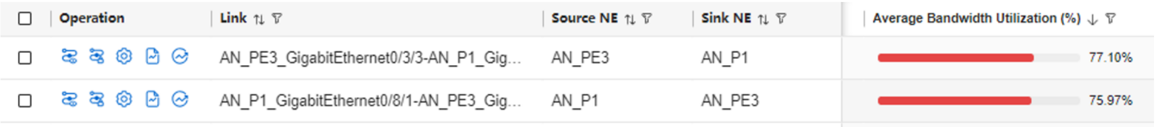
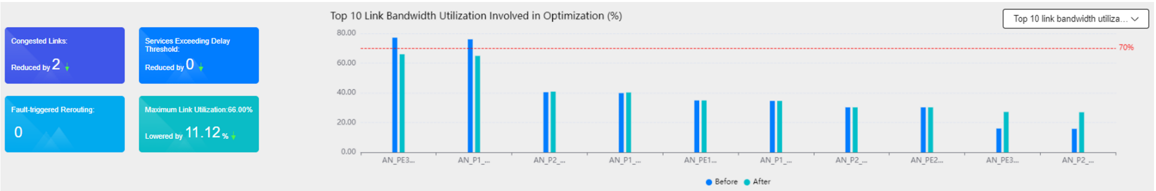


Figure 33: Optimization has been Applied



□	Operation	Link	Source NE	Sink NE	Average Bandwidth Utilization (%)
□		AN_PE3_GigabitEthernet0/3/3-AN_P1_Gig...	AN_PE3	AN_P1	77.10%
□		AN_P1_GigabitEthernet0/8/1-AN_PE3_Gig...	AN_P1	AN_PE3	75.97%

Figure 34: Utilization Acceded the Defined Threshold



Congested Links: Reduced by 2

Services Exceeding Delay Threshold: Reduced by 0

Fault-triggered Rerouting: 0

Maximum Link Utilization:66.00% Lowered by 11.12%

Figure 35: Optimization History shows Lowering the Bandwidth Utilization

To validate NCE’s analysis capabilities, we increased the traffic of Services 3 and 4 traversing the same link (P1-PE3), to cause them to exceed the bandwidth utilization threshold (Figure 34).

NCE correctly executed optimization steps, displaying the details of all tunnels involved in this procedure and presenting the results through visual graphs (Figure 34).

Pre-Approval Approach

We checked the S4 service optimization detail information in NCE, which showed the expected optimization suggestions (Figure 35).

✓ Verdict: L4

NCE quickly evaluated information that exceeded preset thresholds, including delay, packet loss rate, and bandwidth. Within minutes, it automatically pinpointed the TE tunnels in need of optimization and generated solutions that complied to both the service SLA and established optimization guidelines.

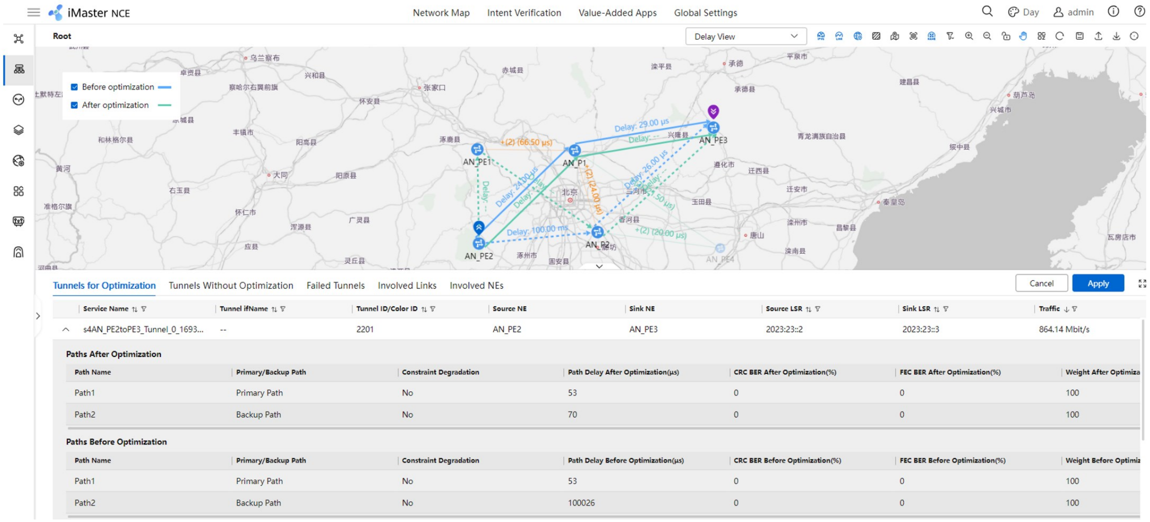
Optimization: Decision-making Tasks

The next step towards fully automated network optimization is the path calculation using constraints – such as affinity attributes and cost values –, resulting in a decision for optimized traffic engineering tunnels complying to all delay, bandwidth, and packet loss criteria, all without manual intervention.

We validated NCE’s behavior in decision-making for network optimization in two modes (similar to the previous step): An automatic and a pre-approval approach.

Automatic Approach

NCE was expected to perform all decision-making steps automatically. We inspected NCE’s optimization history log to obtain the process information. Figure 36 shows that optimization decisions were undertaken as expected.



Service Name	Tunnel ifName	Tunnel ID/Color ID	Source NE	Sink NE	Source LSR	Sink LSR	Traffic
s4AN_PE2toPE3_Tunnel_0_1693...	--	2201	AN_PE2	AN_PE3	2023:23::2	2023:23::3	864.14 Mbit/s

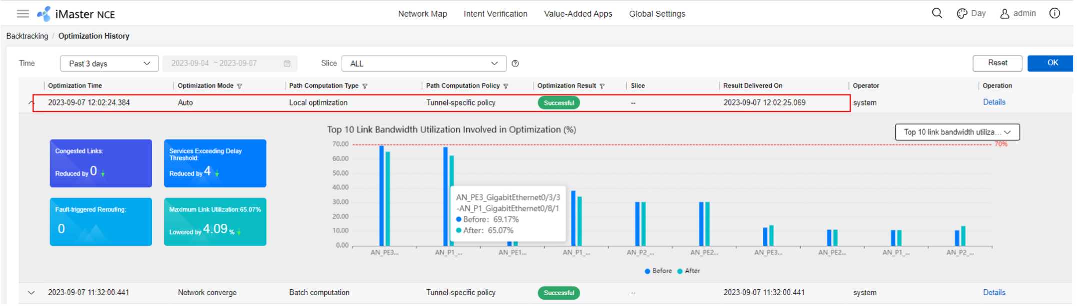
Paths After Optimization

Path Name	Primary/Backup Path	Constraint Degradation	Path Delay After Optimization(μs)	CRC BER After Optimization(%)	FEC BER After Optimization(%)	Weight After Optimiza
Path1	Primary Path	No	53	0	0	100
Path2	Backup Path	No	70	0	0	100

Paths Before Optimization

Path Name	Primary/Backup Path	Constraint Degradation	Path Delay Before Optimization(μs)	CRC BER Before Optimization(%)	FEC BER Before Optimization(%)	Weight Before Optimiz
Path1	Primary Path	No	53	0	0	100
Path2	Backup Path	No	100026	0	0	100

Figure 36: The system offers Suggestions for Optimization (Primary/Backup Paths)


iMaster NCE
Network Map
Intent Verification
Value-Added Apps
Global Settings
Day
admin
Backtracking / Optimization History
Reset
OK
Top 10 link bandwidth utiliza...
Congested Links: Reduced by 0
Services Exceeding Delay Threshold: Reduced by 4
Fault-triggered Rerouting: 0
Maximum Link Utilization:65.07% Lowered by 4.09 %
Top 10 Link Bandwidth Utilization Involved in Optimization (%)
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
70%
AN_PE3_GigabitEthernet0/3/3 -AN_P1_GigabitEthernet0/8/1
Before: 69.17%
After: 65.07%
AN_PE3...
AN_P1_...
AN_PE1...
AN_P1_...
AN_P2_...
AN_PE2...
AN_PE3...
AN_PE2...
AN_P1_...
AN_P2_...
Before
After

Time: Past 3 days | 2023-09-04 ~ 2023-09-07 | Slice: ALL

Optimization Time	Optimization Mode	Path Computation Type	Path Computation Policy	Optimization Result	Slice	Result Delivered On	Operator	Operation
2023-09-07 12:02:24.384	Auto	Local optimization	Tunnel-specific policy	Successful	--	2023-09-07 12:02:25.069	system	Details
2023-09-07 11:32:00.441	Network converge	Batch computation	Tunnel-specific policy	Successful	--	2023-09-07 11:32:00.441	system	Details

Figure 37: Delay and Packet Loss Optimization Information

Auto Approve Disabled

NCE offered to take decisions for those tunnels requiring optimization (see Figure 37). We verified that the suggestions were accurate.

✓ Verdict: L4

Using near real-time information, NCE autonomously decided about tunnel optimization strategy. Prior to implementation, this solution was validated by NCE in a digital twin environment.

Optimization: Execution Tasks

The final goal of all the autonomous optimization tasks is to implement the solution. We expected NCE to enable one-click optimization for latency, bandwidth, and packet loss, with auto-rollback for issues. NCE was further expected to auto-verify the tunnel service performance (latency and traffic) post optimization delays and to confirm compliance with all service level criteria.

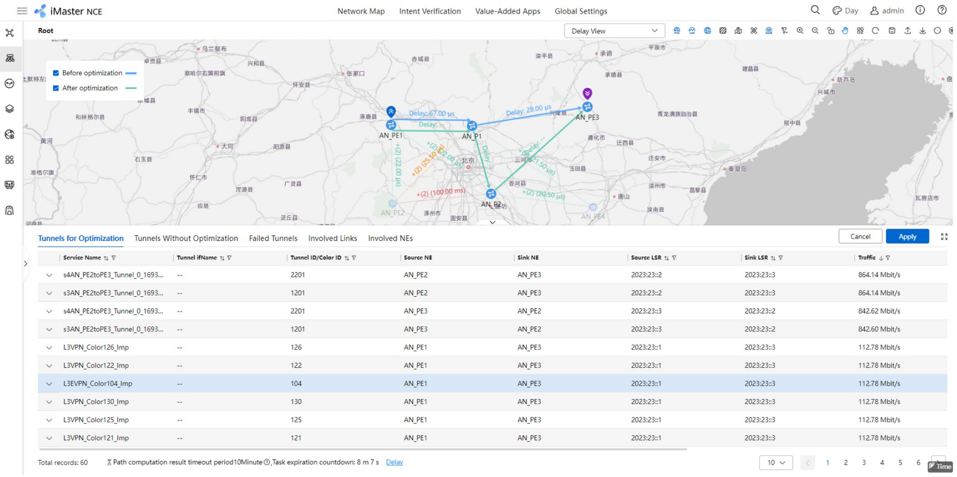
It was a straightforward action to allow NCE executing the optimizations that had been suggested in the previous steps. (Obviously, we continued with the same methods described further above to trigger optimization.)

We verified that NCE instructed the routers to optimize tunnels without human interaction. We also verified that NCE automatically checked the path metrics after the execution step: The user interface of NCE showed that the optimized tunnels did not exceed any thresholds and adhered to the pre-configured required SLA values for delay and packet loss (see Figure 38).

The traffic statistics generated by NCE did not show any packet loss for the optimized services. Additionally, our packet captures between the controller and the network showed the SRv6 Policy path optimization commands were carried through BGP update messages.

✓ Verdict: L4

The system automatically completed path optimization in seconds. Traffic was not interrupted during the optimization, and no packet loss occurred. After the optimization, the system automatically verified and confirmed the results, including the TE tunnel status and SLA compliance.

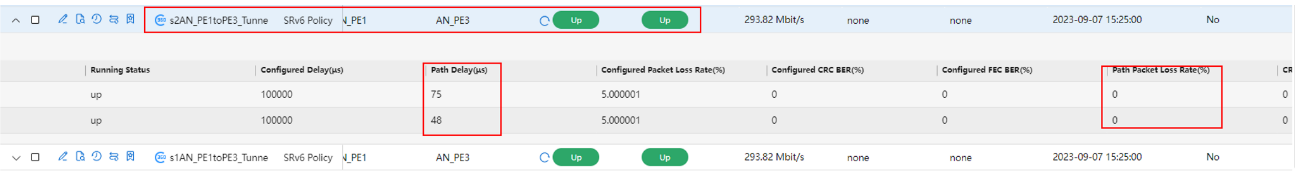


	Service Name	Tunnel ifName	Tunnel ID/Color ID	Source NE	Sink NE	Source LSR	Sink LSR	Traffic
∨	s4AN_PE2toPE3_Tunnel_0_1693...	--	2201	AN_PE2	AN_PE3	2023:23::2	2023:23::3	864.14 Mbit/s
∨	s3AN_PE2toPE3_Tunnel_0_1693...	--	1201	AN_PE2	AN_PE3	2023:23::2	2023:23::3	864.14 Mbit/s
∨	s4AN_PE2toPE3_Tunnel_0_1693...	--	2201	AN_PE3	AN_PE2	2023:23::3	2023:23::2	842.62 Mbit/s
∨	s3AN_PE2toPE3_Tunnel_0_1693...	--	1201	AN_PE3	AN_PE2	2023:23::3	2023:23::2	842.60 Mbit/s
∨	L3VPN_Color126_Imp	--	126	AN_PE1	AN_PE3	2023:23::1	2023:23::3	112.78 Mbit/s
∨	L3VPN_Color122_Imp	--	122	AN_PE1	AN_PE3	2023:23::1	2023:23::3	112.78 Mbit/s
∨	L3EVPN_Color104_Imp	--	104	AN_PE1	AN_PE3	2023:23::1	2023:23::3	112.78 Mbit/s
∨	L3VPN_Color130_Imp	--	130	AN_PE1	AN_PE3	2023:23::1	2023:23::3	112.78 Mbit/s
∨	L3VPN_Color125_Imp	--	125	AN_PE1	AN_PE3	2023:23::1	2023:23::3	112.78 Mbit/s
∨	L3VPN_Color121_Imp	--	121	AN_PE1	AN_PE3	2023:23::1	2023:23::3	112.78 Mbit/s

Total records: 60 ⌛ Path computation result timeout period10Minute ⓘ, Task expiration countdown: 8 m 7 s Delay

10 ∨ < 1 2 3 4 5 6 >

Figure 38: Tunnels suggested for Optimization



∧ □	s2AN_PE1toPE3_Tunne	SRv6 Policy	N_PE1	AN_PE3	Up	Up	293.82 Mbit/s	none	none	2023-09-07 15:25:00	No

Running Status	Configured Delay(μs)	Path Delay(μs)	Configured Packet Loss Rate(%)	Configured CRC BER(%)	Configured FEC BER(%)	Path Packet Loss Rate(%)	CR
up	100000	75	5.000001	0	0	0	0
up	100000	48	5.000001	0	0	0	0

∨ □	s1AN_PE1toPE3_Tunne	SRv6 Policy	N_PE1	AN_PE3	Up	Up	293.82 Mbit/s	none	none	2023-09-07 15:25:00	No

Figure 39: Service 2 Path Metrics after Optimization

Results Summary

Across all test areas and cases, the Huawei solution with iMaster NCE-IP was able to reach a very competitive AN level, and to prove almost all of the claims made by Huawei.

Please see the table and Figure below for an overview of all test results:

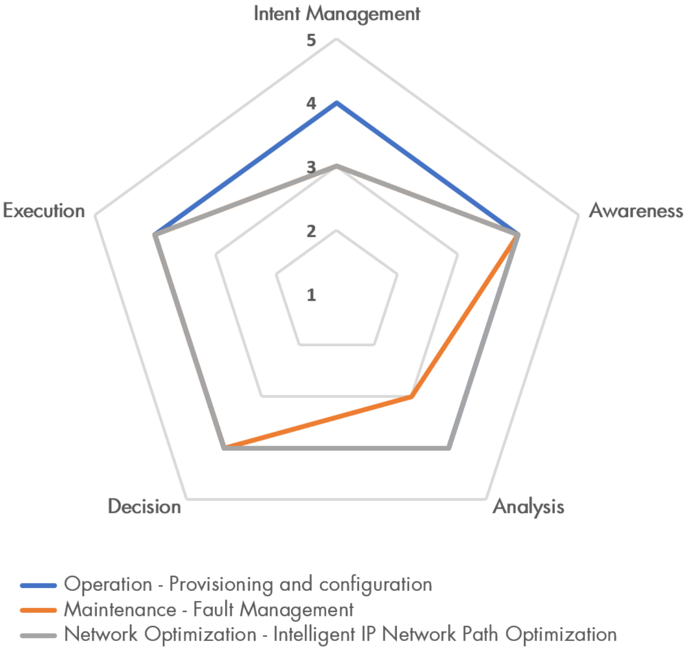


Figure 40: Test Results

Conclusion

Our independent functional tests of Huawei's NCE-IP and SRv6-based router solution using NetEngine 8000, NE-40 and ATN-901 routers confirmed Huawei's superior level of automated provisioning, monitoring, troubleshooting, and network optimization reached. Throughout the tests, the beta software version of NCE—which, as Huawei stated, will be made available for general customer access in Q1/2024—proved to be a very powerful tool, handling a range of SLA maintenance, troubleshooting, and optimization scenarios smoothly. We were not commissioned to include any field-scale performance or service complexity tests—which would, frankly speaking, have been premature at this stage of technology standardization.

Our initial, independent verification proved that there is a viable path to reach L4 automation within a single-vendor ecosystem and for selected innovative protocol deployments already at this stage of the industry.

	Intent Management	Awareness	Analysis	Decision Making	Execution
Service Provisioning	L4	L4	L4	L4	L4
Monitoring and Troubleshooting	L3	L4	L3	L4	L4
Network Optimization	L3	L4	L4	L4	L4

Table 6: Test Results

While every reasonable effort has been made to ensure accuracy and completeness of this publication, the authors assume no responsibility for the use of any information contained herein. All brand names and logos mentioned here are registered trademarks of their respective companies.

EANTC AG
Salzufer 14, 10587 Berlin, Germany
info@eantc.de, www.eantc.de
[v1.0 20231103]