Nokia Network Services Platform

Release 19

The Nokia Network Services Platform (NSP) enables network automation for large-scale IP/MPLS, Ethernet, optical, IP/optical and microwave networks. By accelerating service fulfillment and simplifying network management, assurance and SDN control, the Nokia NSP provides maximum agility, efficiency and network reliability.

The NSP works across multiple network domains and layers, physical/virtual infrastructure and with equipment from multiple vendors. It provides network operators with faster network services delivery, maximum performance and reliability, and software-defined networking (SDN) control to optimize network utilization, latency and traffic engineering.

With 5G, the cloud and the Internet of Things (IoT), customer expectations have increased, driving the need for network services to be delivered on demand with finer-grain programmability that enables consumption of what is needed, precisely when and where it is needed. This requires provisioning services in a way that makes optimal use of their network assets, along with continual intent-based management and insight-driven automation to ensure that business-level and network-level requirements are met for services. The NSP provides the visibility and control needed to deliver on network requirements end to end.

Features

- Unified automation, optimization and assurance for IP/MPLS, Ethernet, optical, IP/optical and microwave networks
- Secure and reliable service provisioning automation with network-aware path placement to meet SLAs
- Optimal path instantiation from an external Path Computation Element (PCE)
- Policy-based, real-time network optimization and flow control driven by key performance indicators (KPIs) and streaming telemetry
- Support for multiple tenants, physical and virtual domains, IP and optical layers, Layer 0–Layer 3 (L0-L3) service technologies, and multivendor equipment.

Benefits

- Increase margin on existing services and enable new revenue through innovating service options/ SLAs
- Gain faster, simpler network service innovation and delivery with optimal usage of the network
- Get the most return on investment (ROI) through increased performance at the lowest cost using SDN control to optimize path instantiation in real time
- Maximize the use of network assets even during high usage/fault conditions without jeopardizing SLAs
- Extend automation, control and assurance across a broad scope with flexibility to leverage existing investments.

With the NSP, network operators and engineers can:

- Securely and reliably create on-demand network services with maximum operational efficiency, provisioning them in seconds/minutes instead of days/weeks
- Add real-time awareness to optimize on-demand service provisioning that makes the best use of available network assets
- Improve time-to-market for NSP-delivered services with tightly integrated workflows that include operations, administration and maintenance (OAM) validation and monitoring through assurance and supervision applications
- Improve ROI by offering higher performing and lower latency services through optimizing networks and capacity use in real time
- Extend network automation capabilities through open application programming interfaces (APIs) and model-driven programmability that deliver the best fit and focus to enable broader software architectures.

How the Nokia NSP works

The NSP addresses dynamic connectivity needs through on-demand creation, maintenance and removal of IP/MPLS, Ethernet and optical network services and resources. It uses a powerful policy engine and intent-based, standards-based service models to quickly and efficiently create network services. An intelligent, network-aware service connection manager optimizes the mapping of service connections to network tunnels and resources in real time.

With simple REST/RESTCONF APIs, IT and operations support systems (OSSs) and service orchestrators can integrate with the NSP. This set of NSP northbound APIs enables access to abstracted models that hide service provisioning complexity and enable assurance.

The NSP DevPortal enables free access to API documentation with examples, tools and remote labs tailored to various use cases.

Third-party application interoperability is certified for leading industry IT/OSS vendors by the NSP Connected Partner Program, which ensures validation of integrations through the NSP northbound API.

With model-driven mediation and multiple southbound device management protocols, the NSP can deploy services, paths and other network resources over IP, optical or Carrier Ethernet network equipment and across equipment from multiple vendors.

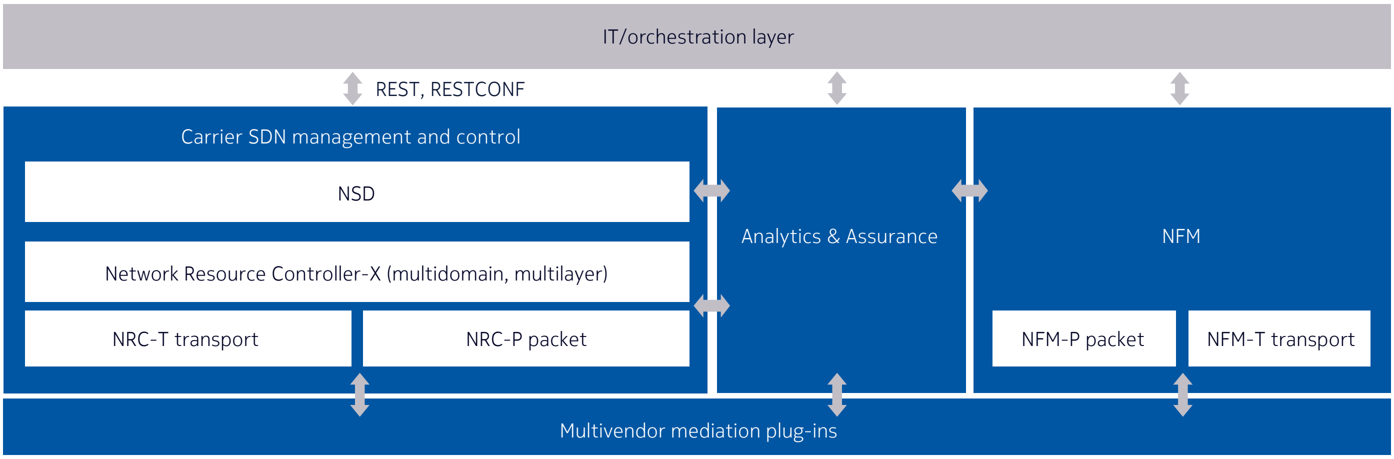
Product components

The NSP consists of seamlessly integrated modules (see Figure 1):

- Network Services Director (NSD) for model-driven service automation and network management
- Network Resource Controller (NRC) modules for IP and optical path and flow control and multilayer coordination
- Network Functions Manager (NFM) modules for IP/MPLS and optical network management and assurance.

Application-specific assurance functions are part of all modules. Modules also share a common set of REST/RESTCONF APIs.

Figure 1. Nokia NSP product architecture


IT/orchestration layer
REST, RESTCONF
Carrier SDN management and control
NSD
Network Resource Controller-X (multidomain, multilayer)
NRC-T transport
NRC-P packet
Analytics & Assurance
NFM
NFM-P packet
NFM-T transport
Multivendor mediation plug-ins

Network Services Director

The Network Services Director (NSD) provides model-driven service automation and network management for multivendor networks. It automates IP/MPLS and Carrier Ethernet service management (fulfillment and assurance) by mapping abstract service definitions to detailed service templates using operator-defined policies. It also provides provisioning for complex multi-technology services across multidomain networks.

NSD maintains abstracted service models through its model-driven mediation framework that uses Yet Another Next Generation (YANG) models and a command line interface to support multivendor provisioning and other model-driven applications.

A key benefit of NSD provisioning is that it is network-aware and manages a centralized database of service connection resources (tracking tunnel bandwidth). This means that as it provisions services, the NSD performs an inline optimal path selection through an intelligent path search within its database. This search finds available paths that will best meet required bandwidth, span, latency, cost, path diversity and other constraints. Based on operator-defined policies, the NSD can, for example, select links with a low link utilization to minimize potential congestion.

The NSD allows operators to customize the binding of service connections to tunnels/paths by letting operators define service-specific policies.

If there is no service connection path that meets the specified requirements (i.e., if one does not currently exist or if none has the required characteristics), then through policy the NSD can leverage the NRC module to establish a new path with the required SLA.

Together with the NSP's open, programmable APIs, the NSD can be used to discover and manage L2/L3 services across multivendor networks and to automate tasks (by its Service Fulfillment and Workflow Manager) to achieve simple, cost-effective and error-free service fulfillment and operations.

In addition, tightly integrated NSP applications for service assurance, including topologies and other visualization capabilities, enable superior visibility to simplify problem resolution and keep pace with automation.

Service Fulfillment

The NSD's Service Fulfilment application offers a programmable, template-driven approach to L2/L3 service discovery, provisioning and automation across multivendor networks. Service templates can be programmed to take user input and apply customized configurations to the network using device-specific mediation scripts.

By defining service templates for a service offering, engineering and planning teams can control and manage a catalog of standard services and configurations that can be deployed to the network. With vendor agnostic-user inputs, device- and vendor-specific complexities can be significantly reduced.

Provisioning a new service is simplified through predefined service templates that enable service deployment with minimal user input. Tunnels are automatically created or selected based on associated tunnel profiles. Mediation scripts for the template ensure the desired configurations are applied to each device based on user input. This significantly reduces the knowledge needed to create, manage and troubleshoot services in multivendor environments, resulting in fewer errors during service operations.

The NSD Workflow Manager extends the service automation capabilities of the Service Fulfillment application by allowing workflow automation scripts to be assigned to service templates. This can be useful for performing automated pre-deployment and post-deployment actions during service provisioning.

Workflow Manager

As part of its model-driven network management, the NSD module provides a Workflow Manager (WFM) for programmable network and service automation. The WFM enables orchestration across all NSP-managed network elements and NSP platform infrastructure and applications as well as with external systems. Its programmable automation enables fine-grain control for a wide scope of operational responsibilities, including network migrations, configuration management, performance testing, security management and software management.

Workflows can be initiated manually, scheduled, or triggered by network events or as side-effects of other NSP operations. Existing workflows can be easily adjusted to adapt to customer-specific procedures and to support new network element releases, including for third-party vendor equipment.

Network Resource Controller

Network Resource Controller (NRC) modules perform multidomain IP/MPLS and optical path control, flow control and multilayer coordination functions. For example, path computations are centrally calculated across IP/MPLS, optical or IP/optical networks.

NRC modules serve path instantiation requests from northbound applications, including the NSD, OSSs and orchestration systems as well as PCE clients (PCCs) such as routers. Because the NRC modules are centralized, they have the full multidomain and multilayer network view required to calculate the optimal path for any combination of business objectives (e.g., lowest cost) and technical constraints (e.g., exact bandwidth or latency required).

The NRC modules also incorporate SDN standards such as those for a stateful PCE architecture. They employ various path optimization algorithms to ensure the best path placement for services and load-balancing for path distribution across the network. This includes the Nokia Bell Labs Self-Tuned Adaptive Routing (STAR) algorithm, which is proven to be able to place 24 percent more paths on the network than with present modes of operation using Constrained Shortest Path First (CSPF).

Sophisticated service/network KPIs and analytics serve as triggers for policies that adapt the network by rerouting paths or adding more bandwidth to service connections as necessary.

By reducing complexity, enabling more effective use of network assets and lowering overall congestion, the NRC allows network operators to reduce overall CAPEX and OPEX and increase revenue from existing assets.

There are three NRC modules:

- Network Resource Controller – Packet (NRC-P)
- Network Resource Controller – Transport (NRC-T)
- Network Resource Controller – X (NRC-X)

Network Resource Controller – Packet

The NRC-P enables OPEX and CAPEX savings by automating traffic placement and path optimization, thereby maximizing network usage on existing assets. The NRC-P also enables greater service innovation by making it faster and easier to scale new services by limiting traditional network complexity hurdles. It intelligently automates capacity growth for elastic services when and where profitable. It provides finer-grain programmability for tailor-made service offerings. And it enables premium service revenue with traffic-engineered SLAs to entice customer upgrades to value-added options.

The NRC-P has significant importance for meeting the requirements and bandwidth demands of 5G, cloud and IoT. The NRC-P enables the network to achieve the highest reliability and quality by dynamically adapting it to changing traffic patterns.

The NRC-P consists of five feature packages:

- Path Control
- Optimization
- Peer Engineering
- OpenFlow Control
- Simulation.

The Path Control package manages the creation of Label Switched Paths (LSPs) across IP network elements and supports both Resource Reservation Protocol (RSVP) and Segment Routing technologies. It maintains a unified topology built from several Interior Gateway Protocol-Traffic Engineering (IGP-TE) and current-path databases that are synchronized with the network elements.

The NRC-P is open and standards-based. It communicates with network elements such as IP routers using the Path Computation Element Communication Protocol (PCEP) and leverages multiple standards-based techniques for topology discovery.

The Optimization package addresses several use cases, including:

- Congestion resolution with flow redirection to alternate paths
- VIP-source, subnet-based steering and VIP link management
- Per-Autonomous System (AS)-based traffic optimization
- Internet peering engineering (for both ingress and egress)
- Insight-driven automation use cases (e.g. quality of service improvement) with Nokia Deepfield

The Peer Engineering package provides the functionality that was formerly associated with NSP Release 17 NRC-F, leveraging protocols such as OpenFlow and Border Gateway Protocol (BGP) to perform intelligent traffic steering and automation, per flow or per route, using policy-based redirection as needed. It intelligently steers traffic to the various alternate paths in the network that are determined to alleviate congestion and/or deliver the traffic in a more optimal or load-balanced way.

The OpenFlow Control package enables identified flows to be redirected when there is congestion.

The Simulation package delivers an offline simulation tool to allow engineers to become familiar with the system's behavior before moving to full automation.

Network Resource Controller – Transport

The NRC-T manages the creation of a transport path connection for L1 optical transport networks and L0 wavelength division multiplexing (WDM) networks. The NRC-T maintains an optical topology and current path database that is synchronized with the network elements and takes physical-layer knowledge such as impairments into consideration to ensure that optimal paths are computed.

Further details on the NRC-T are documented in optical-specific materials. Contact your Nokia optical sales representative for more information.

Network Resource Controller – X

The NRC-X provides cross-domain coordination between multiple layers and domains. IP/optical multilayer traffic engineering ensures that services are delivered on the best path at optimal quality. The base NRC-X functions include topology discovery and correlation as well as multilayer analysis, for example, to identify shared risk.

The NRC-X leverages the NRC-P and NRC-T modules, and it can also act as a hierarchical controller interfacing with third-party SDN controllers. It is a key part of Nokia's IP/optical SDN.

Network Functions Manager

Network Functions Manager (NFM) modules perform comprehensive network management for network infrastructure deployment, provisioning, maintenance, statistics collection, proactive OAM testing, troubleshooting and OSS mediation. The NFM modules provide base fault, configuration, accounting, performance and security (FCAPS) management with many advanced extensions for network deployment automation, service templates and assurance. There are two NFM modules:

- Network Functions Manager – P (NFM-P)
- Network Functions Manager – T (NFM-T)

Network Functions Manager – P

The NFM-P enables IP network and service management across all domains of IP/MPLS, Carrier Ethernet and microwave networks, including access, aggregation, metro and core. The NFM-P also delivers unified operations whether network services are running in a virtualized environment or on specialized hardware platforms. This includes mobile management from backhaul to packet core (including the latest Nokia cloud-based Evolved Packet Core [EPC] solution) as well as IP/microwave transmission.

The NFM-P provides an advanced scripting framework to enable customized programmatic control for automation of network deployment, audits and bulk maintenance changes.

The NFM-P provides inventory, performance and utilization intelligence through its Analytics for Network & Services application. It provides multivendor route analytics through its Control Plane Assurance Manager (CPAM) application.

The NFM-P also delivers an integrated carrier-grade Virtual Network Functions (VNF) manager (VNFM) for Nokia IP Routing and EPC VNFs, which fits into ETSI NFV management and orchestration (MANO) environments leveraging OpenStack.

Network Functions Manager – T

The NFM-T centralizes and consolidates multiple functions for the management of optical networks from access to metro to core. The NFM-T allows network operations staff to efficiently plan, deploy and manage the optical network over its complete life cycle. It also provides element, network and service management, which support multiple optical technologies, services and network sizes.

The NFM-T provides common optical management for end-to-end operations. This includes service provisioning over multi-technology optical transport networks: SDH/SONET, Carrier Ethernet, WDM, reconfigurable optical add-drop multiplexer (ROADM), optical transport networking (OTN) and packet. Fault management web apps reduce the time and cost of network and service assurance operations. A common northbound API enables OSS integration.

Further details on the NFM-T are documented in optical-specific materials. Contact your Nokia optical sales representative for more information.

Model-driven Mediation and management

NSD, NRC-P and NRC-X modules all leverage the NSP's Model-Driven Mediation (MDM), which provides a more agile, DevOps-ready multivendor framework for supporting new equipment releases and service models at just-in-time speed.

With MDM, device upgrades are decoupled from traditional NSP upgrades. Forward-compatibility for supporting new devices and service models is inherently provided in existing NSP module releases—without requiring platform or module upgrades.

This new paradigm shift to model-driven management is fundamentally different from the present mode of operations and delivers a dramatic improvement over the current process. For example, in the past, operators may have had to wait many months for some new equipment releases to be supported because equipment feature support and the necessary device and service object models needed to be changed in the management system code-base by vendor software designers. In many cases there were also further delays that resulted from waiting for the new release to be made available in the next upcoming vendor release cycle.

In addition, the deployment timeline for vendor software needs to be planned, implemented and tested for platform-wide or module upgrades, which adds many more months to go live—especially when OSS integrations also need to be re-validated.

Now, with Nokia NSP model-driven management, we can significantly reduce these many-months-long deployment delays to a minimum—as little as hours or days in many cases, depending on the project scope.

With MDM, new device features can efficiently be exposed to northbound systems by adopting new southbound and northbound models and by creating new adaptation scripts to translate between the two. There is no longer a need to change internal models.

The maximum level of automation is enabled by leveraging YANG modeling, which has become predominant in modern IP networks. With the YANG model being hot-deployed, management support can be ready in NSP applications as soon as the YANG model is made available and deployed using MDM. This is possible because the object models and NSP support are automatically derived from the YANG model.

Support is provided out-of-the-box for many standards, including IETF L2 and L3 service models. In addition, a web GUI for provisioning and RESTCONF northbound APIs are auto-generated from YANG models.

Network slicing and multi-tenancy for Network-as-a-Service (NaaS)

The NSP enables the creation of virtual network slices (also known as network partitioning), which enables a functional mechanism that can be used to support 5G network slicing. For 5G networks, the NSP functions through an integration with an end-to-end Network Slice Orchestrator to find the optimal location of gateways and Cloud-RAN, adding value by abstracting the complexity of the underlying network and assisting with automating slice connectivity creation, monitoring and optimization.

However, network slices are more than just a network abstraction because they minimally must enable the independent existence of multiple tenants on every single physical infrastructure used along the connectivity path. The network slice is essentially a distinct set of connections between multiple infrastructure points (either physical or virtual). This network slice must also be able to ensure a deterministic SLA across the connectivity.

Driven by these requirements, it is important for network slices to be implemented independent of the underlying network technology. In addition, to best fit existing brownfield networks, multiple technologies must be supported by a single network slice.

For example, a transport slice managed by the NSP can be implemented with any supported technology: IP, optical, passive optical network or microwave. The transport slice can use any tunnel type: IP, MPLS, Segment Routing or outdoor unit/optical channel. And the transport slice can use any L0/L1/L2/L3 service type.

In this way, the network slice simplifies operations by abstracting the complexity of the implementation from tenants. Each tenant on the operator's network can create and manage its own virtual network slice—distinct, secure and independent of other tenants' slices and of the operator's own production network.

The tenant has complete end-to-end visibility of its services and the ability to monitor SLAs, turn up new services, change bandwidth between sites, reroute services between sites, and rapidly adapt to changing service requirements or network conditions. The operator retains a global view of the network and the ability to manage and monitor all elements.

Assurance and Analytics

Comprehensive network and service assurance from NSP Assurance and Analytics functions are integrated in NSD and NFM-P modules. These integrated capabilities are required to ensure effective realization of many automation use cases. To make automation work well in live network deployments, for example when using assurance and analytics to trigger automated actions, brings a critical need for superior visibility in daily operations.

NSP Assurance and Analytics functions are needed to ensure that operations keep pace by driving and automating smarter services placement on network resources so that requested SLAs can be honored.

Traditionally, once a service was instantiated, operators continuously surveyed alarms/ KPIs and took manual actions or, at best, user-driven, partially automated actions to continue safeguarding SLAs. As network service delivery becomes more dynamic and network demand and traffic patterns become less static and predictable, operators need a higher level of network and service supervision visibility and automated control. These requirements are needed to keep up with the higher rate of changes to the network and services.

NSP Assurance and Analytics functions are tightly integrated with NSP service automation and network resource control functions. All functions use common data (inventory, topology and services) and common data models. These closed-loop assurance capabilities leverage KPIs and analytics to drive automated policy-based optimization, thereby improving overall service health and network efficiency from initial delivery to daily operations.

An example is using the NSD for service provisioning to enable IP/MPLS network-aware path placement automation with service validation. In addition, service/network supervision visibility is given so operators can efficiently monitor network events and provide the correlation needed to perform intelligent root-cause and services-impact analysis.

Because dynamic assurance is only as good as the data that feeds it, the NSP Assurance and Analytics functions include policy triggers that encompass analysis/correlations from both IP and optical layers and from both physical and virtual domains.

NSP Assurance and Analytics also feeds the NSP NRC-P module with the KPIs needed to deliver intelligent steering and load-balancing of traffic. KPIs enable analytics-driven policies that automate actions to ensure critical SLAs are met and optimal use is made of IP/optical assets. To avoid network congestion that causes latency and performance degradation, traffic flows can be redirected, new multilayer paths established or existing paths resized dynamically, as dictated by policy. Dynamic tuning of network resources, such as redirecting traffic flows and services onto alternate paths, will also free up assets to generate additional revenue.

The NRC-P also works in conjunction with the NSP Assurance and Analytics functions, which collect link utilization and flow statistics and can be set up to monitor for congestion.

NSP Assurance and Analytics includes specialized applications for fault management, service and network supervision and assurance, network and service analytics, and route analytics.

The NSP provides a GeoMap layout manager to enhance customization of its topology visualization using map layouts across NSP. For example, administrators can create a default common map to be used for the Network Supervision and IP-Optical cross-coordinator maps.

By choosing to use the GeoMap for a given NSP application's topology map, the user can position network devices on a GeoMap world map and monitor them within their geographical context. The displayed world map is either imported by accessing the map provider's site over the internet (online mode) or is provided from locally installed map resources (offline mode). For devices supporting GPS location configuration, the GeoMap also syncs with the device and keeps track of any changes to the device position.

Technical specifications

NSP

- Base platform: x86 Quad Core, 64 Gb RAM (Please refer to the NSP Planning Guide for specific platform requirements)
- Hypervisors: Linux Kernel-based Virtual Machine (KVM)
- Operating system (OS): Red Hat® Enterprise Linux®
- Database: PostgreSQL

- Topology graph database: Neo4j
- Messaging: Apache® Kafka®
- Logging: Elastic
- Registry: Apache® Zookeeper™
- Single sign-On (SSO): Apereo Central Authentication Service (CAS)
- User management and access control based on Role-Based Access Control (RBAC) model
- Multi-tenancy: Service and resource tenant-based views and span of control
  - Supports creation of virtual network slices, also known as network partitioning
  - Allows independent existence of multiple tenants on a single physical infrastructure
- Multivendor MDM framework supporting:
  - Vendor-agnostic device modeling through developed adapters that are hot deployable
  - Out-of-the-box YANG models, including OpenConfig, IETF standards, Nokia Service Router Operating System (SR OS) support
  - Web GUIs for provisioning and RESTCONF northbound APIs auto-generated from YANG models
  - Flexibility of development using Python, JavaScript, Apache Velocity Template Language (VTL), Java
  - NSP DevPortal l integration toolset and virtual network lab for developing and testing new adapters
- Northbound integrations (OSS and service orchestration): REST APIs
- High availability per module

NSD

- Model-driven service automation and network management (fulfillment and assurance), including for:
  - VPN services: Layer 2 (Virtual Private LAN Service [VPLS], Ethernet VPN [EVPN]) and Layer 3 (IP-VPN, EVPN)
  - Ethernet Line (E-Line)
  - E-Line stitched services
  - Circuit emulation (C-Pipe)
  - Bandwidth on demand
  - Complex multi-technology services, e.g., Ethernet services into L3 VPN with VLAN handoffs to form a single VPN service (all supporting common QoS tunnel policy)
- Service provisioning path placement objectives to optimize selection for:
  - Hop (span)
  - Latency (microseconds)
  - Cost
  - Link utilization
  - Nokia Bell Labs STAR weighting
- Service Call Admission Control (CAC) at access interface granularity
- Path diversity constraints, enforcing service paths selected that are disjoint (bidirectionally and/or for protection at node or link granularity), e.g., for LSPs, Shared Risk Link Group (SRLG) paths
- Policies/templates: Configured through GUI
- Workflow Manager technologies for programmable automation:
  - Mistral Domain Specific Language (DSL)
  - YAML
  - YAQL
  - Jinja2
  - JavaScript
  - REST API

NRC-P (Packet)

- IP/MPLS PCE based on IETF standards
- PCEP standards compliance
- PCE leveraging Nokia SR OS:
  - Segment Routing Traffic Engineering (SR-TE) and Resource Reservation Protocol Traffic Engineering (RSVP-TE) LSPs

- Multi-area CSPF path computation for Intermediate System-to-Intermediate System (IS-IS)
  - Traffic Engineering (IS-IS-TE) and Open Shortest Path First – Traffic Engineering (OSPF-TE)
- Nokia Bell Labs STAR algorithm-based optimization
- Global concurrent optimization (GCO)
- Bandwidth management for both PCC- and PCE-initiated LSPs (RSVP-TE and SR-TE)
- Telemetry-driven path control and optimization
- Supports disjoint paths
- Supports anycast (in case of Segment Routing)
- Supports OpenFlow, BGP Flow Specification (FlowSpec) and IP Flow Information Export (IPFIX)

NRC-T (Transport)

- Optical PCE leverages Nokia 1830 Photonic Service Switch (PSS) Generalized Multiprotocol Label Switching (GMPLS) Wavelength Routing Engine (WRE) technology
- L0 and L1 tunnel/path computation

NRC-X (Cross-domain)

- Cross-domain IP/optical network topology and planning visibility (including customizable GeoMaps)
- IP/optical correlation of traffic engineering parameters such as SRLG or latency
- Topology analysis for reliability and risk mitigation
- Co-ordination for maintenance events
- Auto-discovery of links between routers and optical switches, e.g., by Link Layer Discovery Protocol (LLDP) snooping

NFM-P (Packet)

- IP/MPLS network management for:
  - IP access, aggregation, metro, core (including VNFs)
  - Carrier Ethernet
  - Mobile backhaul
  - Mobile packet core (including the Nokia cloud-based EPC solution)
  - IP/microwave

NFM-T (Transport)

- Optical network management for:
  - SDH/SONET
  - Carrier Ethernet
  - WDM
  - ROADM
  - OTN
  - Packet optical

Assurance and Analytics

- Support IP, optical and integrated IP/optical networks and services
  - Works with NSP SDN modules to extend SDN policy-based actions to automate closed-loop assurance
- Telemetry monitoring for pre-congestion scenarios to trigger closed-loop automated actions; supported monitoring protocols include SNMP, IPFIX and gRPC
- Customizable GeoMap topology layout manager
- Service and network supervision and assurance, including:
  - Health and KPI summary dashboards
  - Threshold configuration
  - Network and service topologies (including customizable GeoMaps)
  - Automated OAM test suite creation and testing
  - Link utilization topology visualization and interface summary views
- Advanced fault management:
  - Alarm correlation
  - Root-cause tree and impact analysis fault views
  - Event timelines
- Analytics reporting

Standards

Path Computation Element

(based on Nokia SR OS supporting IETF standards and drafts)

- PCE
  - RFC 4655: Path Computation Element (PCE)
  - RFC 5440: Path Computation Element (PCE) Communication Protocol (PCEP)
  - RFC 7420: PCEP Management Information Base (MIB) model
  - draft-ietf-pce-stateful-pce-14: PCEP Extensions for Stateful PCE
  - draft-ietf-pce-segment-routing-08: PCEP Extensions for Segment Routing
  - draft-alvarez-pce-path-profiles-04: PCE Path Profiles
- BGP-LS
  - RFC 7752: North-Bound Distribution of LinkState and Traffic Engineering (TE) Information Using BGP
  - draft-ietf-idr-bgp-ls-segment-routing-ext-04: BGP Link-State extensions for Segment Routing
- IS-IS/OSPF extensions
  - RFC 7684: OSPFv2 Prefix/Link Attribute Advertisement
  - draft-ietf-ospf-segment-routingextensions-04: OSPF Extensions for Segment Routing
  - draft-ietf-isis-segment-routing-extensions- 04: IS-IS Extensions for Segment Routing

Flows

- OpenFlow Switch Specification version 1.3.1
- BGP FlowSpec
- IPFIX
  - RFC 5101: Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information
  - RFC 5102: Information Model for IP Flow Information Export

NETCONF

- RFC 6241: Network Configuration Protocol
- RFC 6242: NETCONF over SSH

APIs

- Representational State Transfer (REST)

Data models

- RFC 6020: YANG data modeling language for NETCONF
- RFC 6021 & RFC 6991: Common YANG Data Types
- RFC 7223: A YANG data model for interface management
- RFC 7224: IANA Interface Type YANG Module
- RFC 7951: JSON Encoding of Data Modeled with YANG
- draft-ietf-i2rs-yang-network-topo-20: A Data Model for Network Topologies
- draft-ietf-liu-netmod-yang-schedule-04: A YANG Data Model for Configuration Scheduling
- draft-ietf-teas-yang-te-10: A YANG Data Model for Traffic Engineering Tunnels and Interfaces
- draft-ietf-teas-yang-te-topo-13: YANG Data Model for TE Topologies

Related materials

- Network Services Platform web page – includes NSP application notes and technical papers
- Video channel for Network Services Platform – includes NSP demo videos and product tours

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

Nokia operates a policy of ongoing development and has made all reasonable efforts to ensure that the content of this document is adequate and free of material errors and omissions. Nokia assumes no responsibility for any inaccuracies in this document and reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1908037466EN (September) CID187011