The Network Services Platform (NSP) provides WAN automation and management for IP/MPLS, Ethernet and optical networks, including service automation, network optimization and dynamic assurance.

NSP provides operators with more efficiency across multiple network layers, physical/virtual infrastructure, as well as equipment from multiple vendors.

Cloud and IoT customers expect operators to deliver network services on demand so they can consume only what they need, when and where they need it. For operators, that means provisioning services, and doing so in a way that makes optimal use of their network assets.

Nokia’s purpose-built Carrier SDN software addresses these challenges by blending experience in service management and assurance, and in building and managing large-scale IP/MPLS and optical networks.

Nokia Deepfield and NSP power intelligent network services with real-time visibility, analytics and automation for insight-driven automated networking. That approach delivers superior control and optimization for both network resources and application traffic flows, maximizing user experience and enhancing network security automation to protect against potentially devastating distributed denial of service (DDoS) attacks.

With NSP, network operators and engineers can:

- Create on-demand IP/optical services with maximum operational efficiency and provision 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 assurance capabilities such as integrated OAM tests and network and service supervision
- Improve return on investment (ROI) by offering higher performing and lower latency services through optimizing networks and capacity use in real time
- Extend WAN automation capabilities through open APIs and model-driven programmability that enable the best fit and focus to enable broader software architectures
How the Nokia NSP works

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 NSP. This set of NSP northbound APIs enables access to abstracted models that hide service provisioning complexity and enable assurance for the Carrier SDN era. The NSP Connected Partner Program certifies third-party application interoperability through the NSP northbound API for leading industry IT/OSS vendors.

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified automation, optimization and assurance for IP/MPLS, Ethernet,</td>
<td>Increase margin on existing services and enable new revenue through innovating</td>
</tr>
<tr>
<td>optical and IP/optical networks</td>
<td>service options/SLAs</td>
</tr>
<tr>
<td>Abstracted service provisioning automation with network-aware path</td>
<td>Gain faster, simpler network service innovation and delivery with optimal usage of</td>
</tr>
<tr>
<td>placement to meet SLAs</td>
<td>the network</td>
</tr>
<tr>
<td>Optimal path instantiation from centralized Path Computation Element</td>
<td>Get the most ROI through increased performance at the lowest cost using SDN control</td>
</tr>
<tr>
<td>(PCE)</td>
<td>to optimize path instantiation in real time</td>
</tr>
<tr>
<td>Policy-based, real-time network optimization and flow control driven</td>
<td>Maximize the use of network assets even during high usage/fault conditions without</td>
</tr>
<tr>
<td>by key performance indicators (KPIs) and streaming telemetry</td>
<td>jeopardizing SLAs</td>
</tr>
<tr>
<td>Support for multiple tenants, physical and virtual domains, IP and</td>
<td>Extend automation, control and assurance across broad scope with flexibility to</td>
</tr>
<tr>
<td>optical layers, L0–L3 service technologies and multivendor equipment</td>
<td>leverage existing investments</td>
</tr>
</tbody>
</table>

With model-driven mediation and multiple southbound device management protocols, 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

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

- Network Services Director (NSD) for model-driven service automation and network management
- Network Resources 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.
Network Services Director

Network Services Director (NSD) provides model-driven service automation and network management. 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 (CLI) 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, it performs an inline optimal path selection through an intelligent path search within its database, which finds available paths that will best meet required bandwidth, span, latency, cost, path diversity and other constraints. Based on operator-defined policies, NSD could, for example, select links with a low link utilization in order to minimize potential congestion.

NSD allows operators to customize the binding of service connections to tunnels/paths by letting them 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 have the required characteristics), then through policy NSD can leverage the NRC module to establish a new path with the required SLA.

Network Resource Controllers

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 re-routing 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

NRC-P consists of several feature packages: Path Control, Optimization, Peer Engineering, OpenFlow Control and 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.

NRC-P is open and standards-based. It communicates with network elements like IP routers using 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 re-direction to alternate paths
- VIP-source subnet-based steering and VIP link management
- Per-Autonomous System (AS)-based traffic optimization
- Egress peer engineering
- Insight-driven automation use cases with Nokia Deepfield (e.g. quality of experience [QoE] improvement)

The Peer Engineering package provides the functionality that was formerly associated with NSP Release 17 NRC-F, which leverages protocols such as OpenFlow and Border Gateway Protocol (BGP) to perform intelligent traffic steering and automation using policy-based redirection as needed, at the granularity of flows or routes. It intelligently steers traffic onto 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 feature package enables identified flows to be re-directed under congestion scenarios.

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

Network Resource Controller – Transport

NRC-T manages the creation of a transport path connection for Layer 1 optical transport networks and Layer 0 wavelength division multiplexing (WDM) networks. 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 NRC-T are documented in optical specific materials. Contact your Nokia optical sales representative for more information.
Network Resource Controller – X
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 in optimal quality. The base NRC-X functions include topology discovery and correlation as well as multilayer analysis, for example, to identify shared risk. 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
NFM-P enables IP network and service management across all domains of IP/MPLS and Carrier Ethernet and microwave networks across access, aggregation, metro and core. It 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.

NFM-P provides an advanced scripting framework to enable customized programmatic control for automation of network deployment, audits and bulk maintenance changes. Its golden configuration and snapshots application bring enhanced integrity to network deployment that reduces misconfigurations. It provides multivendor route analytics through its Control Plane Assurance Manager (CPAM) application. 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
NFM-T centralizes and consolidates multiple functions for the management of optical networks from access to metro to core. 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.

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 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 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, and forward-compatibility for supporting new devices and service models is inherently provided within 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 within the management system code-base by vendor software designers. In many cases there were also further delays in waiting for the new release to be made available within the next upcoming vendor release cycle cadence.

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 the Nokia NSP model-driven management, we can significantly reduce these many-month-long deployment delays down 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 is becoming predominant in modern IP networks. Literally, with the YANG model being hot-deployed, management support can be ready within NSP applications as soon as the YANG model is made available and deployed using MDM. This is 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 layer 2 and layer 3 service models. And a web GUI for provisioning and RESTCONF northbound APIs is also auto-generated from YANG models.

### 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 Carrier SDN use cases. To bring Carrier SDN from lab trials to live deployment, assurance and analytics with automated actions and abstracted day-to-day operations visibility will be critical.

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. Those 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, services) and common data models. These closed-loop assurance capabilities leverage KPIs and analytics to drive automated policy-based optimization to improve overall service health and network efficiency from initial delivery to day-to-day operations.

An example is using NSD for service provisioning to enable IP/MPLS network-aware path placement automation with service validation. In addition, service/network supervision visibility is given for operators to 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, 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 that optimal use of IP/optical assets is made. To avoid network congestion that causes latency and performance degradation, traffic flows can be redirected, new multi-layer paths established, or existing paths resized dynamically, as dictated by policy. Dynamic tuning of network resources, such as re-directing traffic flows and services onto alternate paths, will also free up assets to generate additional revenue for carriers.

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

**Multi-tenancy for Network-as-a-Service (NaaS)**

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. It allows for the independent existence of multiple tenants on a single physical infrastructure.

In addition, each enterprise on the operator’s network can also have its own virtual network, distinct, secure and independent of other enterprises’ services and of the operator’s own production network.

The enterprise has complete end-to-end visibility of its services and the ability to monitor SLAs, turn up new services, change bandwidth between sites, re-route 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.

### Technical specifications

**NSP**
- Hardware platform: x86 Quad Core, 64 Gb RAM
- Hypervisors: Linux Kernel-based Virtual Machine (KVM)
- OS: Red Hat® Enterprise Linux® RHEL 7.0
- Database: PostgreSQL
- Topology Graph DB: Neo4j
- Messaging: Apache Kafka®
- Logging: elastic
- Registry: Apache Zookeeper
- Single Sign-On (SSO): Apereo Central Authentication Service (CAS)
- 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 Model-Driven Mediation (MDM) framework supporting:
  - Vendor-agnostic device modeling through developed adapters that are hot deployable
  - Out-of-box supported YANG models, e.g., OpenConfig, IETF standards, SR OS support
  - Web GUIs for provisioning and RESTCONF northbound APIs auto-generated from YANG models
  - Flexibility of development using Python, JavaScript, Apache VTL, Java
  - NSP Developers Portal 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 and network management (fulfillment and assurance), for example for:
  - Virtual private network (VPN) services
    - Layer 2 (VPLS, 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 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

NRC-P (Packet)

- IP/MPLS PCE based on IETF standards
- PCEP standards compliance

- PCE leveraging Nokia Service Router Operating System (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 – 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
- Support for disjoint paths
- Support for 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) GMPLS Wavelength Routing Engine (WRE) technology
- Layer 0 and Layer 1 tunnel/path computation

NRC-X (Cross-domain)

- Cross-domain IP/optical network topology and planning visibility
- 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
Nokia Network Services Platform

**NFM-P (Packet)**
- IP/MPLS network management for:
  - IP access, aggregation, metro, core (including VNFs)
  - Carrier Ethernet
  - Mobile backhaul
  - Mobile packet core (including Nokia cloud-based EPC solution)
  - IP/microwave
- See NSP NFM-P datasheet for more information.

**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
  - Functions 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
  - Monitoring protocols supported include SNMP, IPFIX, gRPC
- Service and network supervision and assurance, including:
  - Health and KPI summary dashboards
  - Threshold configuration
  - Network and service topologies
  - 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

**Carrier SDN 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-1s-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-routing-extensions-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 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: Common YANG Data Types
• 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 related NSP application notes and technical papers
• Video channel for Network Services Platform – includes NSP demo videos and product tours