Nokia Network Services Platform (NSP)
Release 17 — Module: Network Functions Manager (NFM-P)

The Nokia Network Services Platform (NSP) enables IP network and service management across all domains of IP/MPLS and Carrier Ethernet networks — delivering unified operations, whether network services are running in a virtualized environment or on specialized hardware platforms. The NSP helps operators to quickly maximize operational efficiencies through fast provisioning and troubleshooting, proactive assurance and flexibility to ease integration into the network.

The NFM-P module, formerly known as the Nokia 5620 Service Aware Manager (SAM), provides comprehensive IP infrastructure management for configuration, provisioning, assurance and mediation of IP network devices, domains and services across IP access, aggregation, metro and core. This includes mobile management from backhaul to packet core (including the latest Nokia cloud-based EPC solution), as well as IP/microwave transmission.

Continuous collection of key performance indicators (KPIs) enables monitoring of network-wide performance and service health. Advanced troubleshooting and service assurance help to resolve problems fast, before they impact end users or applications. Unique multivendor route analytics capabilities provide proactive control plane assurance and deliver visibility into the dynamic IP/MPLS routing plane and services. Ease of integration within the existing operational environment helps network operators get the most from their existing operations support system (OSS) and business support system (BSS) investments.

The NFM-P module, formerly 5620 SAM, is a proven solution that is widely deployed worldwide in over 600 service provider networks for mobile, enterprise, residential and converged services delivery.

With the addition of a software-defined networking (SDN) controller for the WAN, namely the Nokia Network Services Platform (NSP), operators gain multivendor IP/optical resource connectivity management. This further simplifies service delivery through Carrier SDN abstraction and control. The NSP unifies service provisioning automation with on-demand network engineering to deliver network-aware service deployment that is continuously optimized to better meet bandwidth needs as traffic patterns fluctuate. With the NSP, comprehensive multivendor KPIs and analytics from the NFM-P module enable operators to set up automatic triggering of NSP policies to adapt and optimize network services in real time.
### Data Sheet

**Nokia Network Services Platform - Release 17 - NFM-P module**

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common network management across managed devices accelerates configuration tasks through consistent, easy-to-use GUIs</td>
<td>Minimized time and costs associated with the errors that commonly occur when multiple network management systems or command-line interfaces (CLIs) are used.</td>
</tr>
<tr>
<td>Scripting-based deployment automation and control for network upgrades, configuration, provisioning and performance validation</td>
<td>Rapid introduction of new services across IP/MPLS and Carrier Ethernet network domains.</td>
</tr>
<tr>
<td>Common provisioning for different service types (Layer 2 and Carrier Ethernet, Layer 3 MPLS VPNs and MPLS-TE)</td>
<td>Reduced cost of delivering multi-technology network services by minimizing the risk of misconfigurations through consistent workflows.</td>
</tr>
<tr>
<td>Efficient collection of network statistics, OAM diagnostics and state KPIs along with optional analytics for network service health monitoring</td>
<td>Proactive prevention of potential service-affecting problems before they impact end users and applications.</td>
</tr>
<tr>
<td>Powerful fault correlation and advanced troubleshooting visualization that help to quickly pinpoint the root cause of problems</td>
<td>Simplified problem isolation to quickly understand services-impact, diagnose problems and resolve them.</td>
</tr>
<tr>
<td>Comprehensive open interface enables integration with northbound applications, such as a web portal, OSS/BSS, or service orchestrator</td>
<td>Increased productivity and flexibility with a management solution that easily adapts to allow cost-effective integration into the existing operational environment, enhancing workflows and processes.</td>
</tr>
</tbody>
</table>

### IP infrastructure and services management

NFM-P IP infrastructure management provides base Fault, Configuration, Accounting, Performance and Security (FCAPS) management with many advanced extensions for IP/MPLS tunnel management, templates and automated creation. This includes management of policies for device configuration, including for physical and logical resources, buffers, queuing, QoS marking/forwarding and access control lists (ACLs).

IP infrastructure and services management provides centralized views for listing physical inventory, IP/MPLS paths and services. These views also provide an easy starting point for performing maintenance and troubleshooting that includes search filters, status indicators, and in-context cross-navigation to configuration forms and topology maps.

The NFM-P provides topology views for both physical and logical network layers. Physical topologies support IEEE 802.1ab link adjacencies using Link Layer Discovery Protocol (LLDP). All topology maps include a variety of status indicators allowing cross-navigation to alarm management with fault correlation, OAM test-suites, integrated multivendor route analytics and a wide range of apps for network operations. Specifically for fault management, topology overlays provide alarm status and additional troubleshooting information, such as port and link utilization statistics, or OAM test results with trace highlighting after point-and-click execution from a map.

IP/MPLS control plane visualization is also available through multivendor route analytics capabilities that enable the ability to show hop-by-hop paths taken by Layer 2 and Layer 3 services across the multivendor Interior Gateway Protocol (IGP) topology. This is particularly useful for investigating routing issues.

The NFM-P provides support for a broad range of multi-technology network services for point-to-point, point-to-multipoint, hub-and-spoke or tree service architectures; this includes services for Layer 2 Ethernet (VPWS/VLL, VPLS), Layer 3 IP VPNs, multicast, IEEE 1588v2 Precision Time Protocol (PTP) synchronization, and subscribers.

Service topologies help operators to proactively detect and troubleshoot service-affecting problems, from simple to complex. The NFM-P provides visualization for both Layer 2 and Layer 3 service topologies. Composite services can be created to enable better end-to-end service assurance for more complex service architectures that combine multiple service technologies. OAM diagnostics may also be enabled to allow service level agreement (SLA) validation right from the service topology map using service tests with views of result summaries.
**Scripting-based deployment automation**

The advanced NFM-P scripting framework enables programmatic control to automate deployment of IP infrastructure, significantly reducing misconfigurations so services can be delivered faster and more reliably. Automation eliminates the need to individually configure each device in the service path — including everything from network and quality of service (QoS) policy configuration, to device operating system upgrades, to provisioning.

The NFM-P scripting framework also enables service provisioning automation to accelerate time-to-market for new services. Everything can be automated from service creation to QoS policy assignment to service accounting policy setup for even the most complex end-to-end services spanning multiple technology domains.

After deployment, automated setup of comprehensive OAM diagnostics suites can be used to validate that performance requirements are met and test schedules created to insure SLAs are continuously monitored. For ongoing day-to-day operations, bulk maintenance changes can also be automated. Scripts can be triggered after the discovery of a network element, or they can be scheduled or run on-demand (see Figure 1).

![Figure 1. Automation through NFM-P scripts](image)

**IP network service provisioning**

The NFM-P accelerates service deployment with service templates and scripts for provisioning, rules-based QoS and accounting policy assignment, and automated SLA validation. External systems are able to access service management functionality through an open OSS interface.

NFM-P service templates and workflows enable point-and-click service creation. Operators are guided step-by-step as they set up complex services for rapid provisioning and fewer errors. Templates also enable operators to customize and standardize their provisioning workflow to match internal processes. Layer 2 and Layer 3 services are provisioned in the same way, reducing delivery costs for different service types.

Newly activated services can be validated using a service test suite. Tests are automatically extended as services expand so test coverage does not drop off over time. Individual component tests for the newly provisioned entity are automatically created and include detailed test results.
Network auditing
The NFM-P can automate network auditing and perform mass validation of configuration and policies distributed across many network elements. Differences can be detected from device-specific configuration against a common “golden” configuration or policy. Managed CLI scripting is used to compare configuration on third-party devices. For example, comparison tools may be used after changing device operating system release versions to ensure that the previous configuration remains the same.

Service accounting
The NFM-P collects accounting statistics from network elements to meet a wide range of billing requirements. Setup is accelerated by per-service accounting policy assignment that controls statistics collection for related service access ports. Third-party billing systems can also benefit from aggregated accounting statistics that are grouped per service, since integration effort is simplified through use of the NSP OSS interface.

Multivendor route analytics
The Control Plane Assurance Manager (CPAM) delivers multivendor route analytics to proactively assure the network and isolate potential problems before they affect services. The CPAM provides simplified control plane management through its real-time and historical visualization, troubleshooting, and analysis. With the CPAM, unprecedented end-to-end IP/MPLS infrastructure visibility and analysis enable an understanding of how the control plane topology and protocol changes impact IP routing, MPLS paths, service infrastructure and services (see Figure 2).

The CPAM provides health monitoring for IGP (OSPF and IS-IS) and MPLS paths as well as troubleshooting tools to understand how paths are routed using the IGP topology to perform path highlights using Shortest Path First (SPF) and Constrained SPF (CSPF) algorithms. It also automates path and service tunnel OAM testing on IP or MPLS path changes to alert operators when performance issues emerge after re-routes occur. Protocol configuration audits combine IP/MPLS protocol configuration data with change history tracking information to enable detection of misconfigurations.

Failures and configuration changes can lead to non-optimal routing changes, which cause services to diverge from the fastest or best path that can be taken through the network. If undetected, these dynamic routing changes can impact the performance of IP-based services significantly, leading to an unsatisfactory customer experience or SLA violations. Moreover, reconciling service performance changes associated with IP routing events can be a very time-consuming, labor-intensive process without the multivendor IP/MPLS routing analytics offered by the CPAM.
The CPAM allows operators to automate and scale service integrity monitoring by providing automated, event-driven path validation through its auto-OAM feature, whenever a path event occurs. Auto OAM alerts operators immediately if a dynamic routing change has caused an undesirable condition, such as jitter or delay on a path. It provides near-real-time detection of routing events and their impact. It automatically generates and executes NFM-P OAM tests — dynamically triggered tests that directly monitor and alert operators of performance issues for affected paths through threshold crossing alerts (TCAs) that are correlated to the appropriate paths and services.

CPAM can be setup to monitor multiple BGP autonomous systems (AS) using a path view topology that enables operators to see the number of routes originating from and passing through each external AS path displayed. This view can be used to determine whether new peering points should be established for a growing AS that is currently passing traffic through an adjacent AS.

Through maintaining historical data for each monitored BGP AS, the CPAM enables operators to detect BGP-related issues before they impact services. When an issue is detected, an historical impact analysis may be performed to easily make changes visible and understand their impact. The CPAM provides an in-depth analysis including significant trend indicators (such as prefix stability/health, multi-exit discriminator [MED] changes, and AS path or next-hop/originator switches) to deliver an unprecedented level of visibility that helps operators to easily diagnose emerging issues.

For more information on CPAM functionality, please refer to the CPAM data sheet.

Infrastructure health and performance monitoring

Highly scalable collection of real-time and historical statistics (such as for equipment and interfaces) provides comprehensive information needed to detect and troubleshoot performance issues. OAM test suites can be scheduled and compared to configurable parameters — such as jitter, delay and packet-loss metrics — to proactively detect network and service degradation. Rules-based alarm notifications, such as TCAs and escalating test failure alerts, further automate assurance and adherence to performance and QoS objectives. OAM testing supports IEEE 802.1ag/ITU-T Y.1731 standards-based Ethernet OAM, Two-Way Active Measurement Protocol (TWAMP) and TWAMP Light and MEF 35 service OAM performance monitoring.

Infrastructure-specific fault summary views and supervision dashboards enable operators to see fault trends, KPIs, OAM test results and other summary health indicators that enable proactive monitoring at a glance. Operators may also run on-demand OAM tests from supervision views to investigate further (see Figure 3).

Figure 3. Infrastructure health and performance supervision with NSP
Fault management and root cause visualization

With NFM-P fault management, operators can quickly pin-point the root cause of a problem and determine which users are affected through sophisticated visual insight. This root cause visualization is made possible through a comprehensive service-aware infrastructure model and an advanced alarm correlation rules engine that ties network infrastructure events to impacted services. Correlation rules combined with assurance visualization enable easy impact assessment of faults to help identify priority for investigation and accelerate troubleshooting.

Assurance visualization allows better insight into the magnitude and impact of faults within massive volumes of assurance data to help eliminate manual troubleshooting. Operators may also view events on a timeline to gain visibility into the sequence of when specific infrastructure configuration or state changes, and when OAM test failures and faults occur in relation to each other.

At-a-glance network-wide alarm distribution views group correlated alarms to independent problems, giving an understanding of problems with the most impact. This helps operators to determine which fault to investigate first by indicating which problems have the largest magnitude of impact. Problem diagnosis is greatly simplified through clear views that show the root cause of a fault, including an impact tree of correlated faults (see Figure 4).

Fault impact visualization is also available through network hierarchy views that give an understanding of affected infrastructure, and provide a simpler approach for accelerating problem resolution using efficient cross-navigation workflows to configuration forms.

Third-party fault management OSS integrations, enabled through the NSP OSS interface, also benefit from configurable alarm suppression capabilities.

Analytics for application assurance (optional)

Analytics enables insight into network infrastructure, service utilization, subscriber traffic analysis and quality of experience through a variety of reports and dashboards for residential and Wi-Fi® services. Data is analyzed using business intelligence software and presented in graphical or tabular reports that are viewable using the browser-based NFM-P analytics application.

Figure 4. Fault management visualization with NSP

NFM-P analytics reports and dashboards enable a network operator to quickly determine the overall status of network functions and to monitor trends, for example, to identify the top subscribers in terms of overall network traffic or based on application usage. The analytics browser-based application allows a user to specify the reporting period, the
resource types on which to report, and the desired view. Third-party OSS integrations for performance and SLA management also benefit from the data processing and aggregation capabilities of NFM-P analytics for application assurance.

**NFM-P Premium**

A Premium version of the NFM-P extends the classic NFM-P with an enhanced feature-set. NFM-P Premium contains a full suite of advanced applications that are catered toward various user groups for network configuration, network security, service operations, network analytics, IP control plane monitoring and troubleshooting, control plane change impact analysis and simulation, multicast management, subscriber management and virtual network functions management (VNFM). (See Table 1 for NFM-P Premium feature summary.)

**Golden configurations and snapshots**

The content of IP/MPLS network configuration is becoming more complex and more dynamic. To address the integrity of the network configuration, the NFM-P golden configurations and snapshots application provides capabilities for creating backups of network element configuration at any point in time, with the ability to retain a number of these backups for various points in times. This enables network operators to have an easy and robust application for displaying the current and past configuration of network elements, with configuration auditing capabilities to compare the current configuration against snapshots or golden configurations that have been created in the past.

**Network group encryption security**

The NFM-P module delivers an innovative network group encryption (NGE) security tool for the Nokia 7705 Service Aggregation Router (SAR), which provides comprehensive protection of both IP and non-IP traffic seamlessly at the MPLS layer. NSP management of NGE minimizes operational overhead and complexity while delivering a powerful management tool for security and MPLS services.

**Service assurance**

The NFM-P module delivers comprehensive service assurance from continuous SLA, service health and performance monitoring, service topology visualization, and service impact fault visualization, as well as correlated service-to-infrastructure troubleshooting.

Extensive collection of service performance statistics and comprehensive SLA monitoring tools let operators verify end-to-end services as well as individual service segments. Service test suites can simultaneously test every aspect of a group of services, including multi-layer OAM validation of service infrastructure performance. Test suites can also be set up to provide continual scrutiny of KPIs across various technology layers. In addition, performance monitoring thresholds set on activating OAM test suites and statistics counters enable operators to be alerted as issues emerge.

Third-party OSS integrations for service performance management benefit from highly scalable statistics collection enabled through the NSP OSS interface.

At-a-glance dashboards for services and service group monitoring provide web-based summaries as well as detailed supervisory views for monitoring service health using fault trends, KPIs and OAM service validation. Operators may also run on-demand OAM service validation tests from service supervision views to investigate further. Service Routing maps can be used to highlight service paths on an IGP topology in order to investigate routing issues with potential services impact (see Figure 5).
The NFM-P module allows operators to quickly pinpoint the root cause of a problem and determine which users are affected through sophisticated visual insight. This service impact visualization is made possible through a comprehensive service-aware infrastructure model and an advanced alarm correlation engine that ties network infrastructure events to impacted services. Service correlation rules combined with advanced fault management visualization enable easy service impact assessment of faults to help identify priority for investigation and accelerate troubleshooting. At-a-glance network-wide alarm distribution views give an understanding of problems with the most services impact.

**Network and service analytics**

Analytics enables insight into IP network infrastructure and services. This includes reporting for infrastructure health and performance monitoring, such as for ITU-T Y.1731 standards-based Ethernet OAM test reporting, and bandwidth utilization per port or per service access point. Third-party OSS integrations for performance and SLA management also benefit from the data collection, storage, processing and aggregation capabilities of NFM-P network and service analytics.

**Traffic monitoring and visualization**

To proactively assure the IP/MPLS network, operators need to monitor for traffic hot spots within the network to insure that no continuous bottlenecks emerge that would lead to service degradation and SLA violations. The NSP link utilization app provides web-based monitoring apps for monitoring and visualizing IP/MPLS traffic utilization and reserved link capacity, including for label-switched paths (LSPs) traversing specific interfaces. Dashboard style views enable monitoring for both IP and MPLS interfaces and their traffic statistics for bandwidth utilization, clearly drawing operator attention through use of threshold-based status colors for increasing load levels. The IGP topology map provides traffic utilization overlays that act as a “heat” or “weather” map. It shows current link capacity (based on bandwidth reservation) using link thickness and actual bandwidth utilization by changing the color of the link based on configured thresholds; for example, coloring the link red for a high utilization threshold if utilization is over 80 or 90 percent (see Figure 6).

**BGP monitoring**

Operators can monitor the health of BGP IP prefixes and trigger proactive threshold crossing alerts on significant BGP route changes to detect route removal and instability, route flapping, redundancy loss and high watermarks. It detects and alerts operators of corrupted BGP updates that are often difficult to diagnose as BGP sessions are dynamically shutdown and restarted.

The CPAM also allows network operators to receive alarms for a variety of route issues. For example, alarms are generated if the number of external routes changed will threaten network stability,
or if the number of removals/additions or next-hop changes cross a predefined threshold (route flapping, high watermarks).

For more information on CPAM BGP functionality, please refer to the CPAM data sheet.

**RCIA for live networks**

The CPAM Root Cause and Impact Analysis (RCIA) is used for impact analysis in the live network. When real events occur in the network, RCIA can be used to validate against SLA requirements. Should the reroute result in a violation of SLA parameters, an alarm is raised and affected customers can be retrieved.

**RCIA for offline simulations**

Offline simulation tools are also a part of CPAM RCIA to enable planned changes to be validated before being made in the live network and reduce the risk of maintenance or upgrades impacting performance due to unexpected routing behavior. This helps operators that are about to make a potentially high-impact configuration change in the network to ensure their changes will yield the expected results. It simulates typical operations, such as adding an adjacency, or taking down a node for routine maintenance or upgrades to verify the impact to IP paths and LSPs.

If paths are rerouted according to plan and no failed paths are recorded, the operator can pursue the configuration change with peace of mind. If some paths fail, the underlying cause can be found before the change is made. If an upgrade is planned and the affected IP paths and LSPs are known, the operator can investigate the related tunnels, services and customers that will need to be notified.

For more information on CPAM RCIA functionality, please refer to the CPAM data sheet.

**Troubleshooting and assuring multicast-based services**

With residential triple play video distribution and business VPN applications, service providers face a growing need to troubleshoot customer problems with multicast-based services. However, the extensive use of protocols and complex configurations make troubleshooting these services very difficult. Moreover, multicast data is typically not centralized. It is distributed across multiple network nodes, requiring browsing of routing tables and processing of complex configurations on each node.

The CPAM Multicast Manager Application (MMA) simplifies availability assurance and problem diagnosis for multicast services. It gives service providers an overall view of the multicast domain superimposed on the IGP domain. All crucial multicast objects can be quickly identified and relationships among the objects easily queried. The CPAM MMA can also graphically display the multicast tree for a given group, including a group with multiple sources. The tree discovery method uses SNMP queries or OAM tests to verify the actual path and attached leaf routers.

For more information on CPAM MMA functionality, please refer to the CPAM data sheet.

**Subscriber management dashboard**

Network operators and network planners benefit from the efficiency of a unified approach to monitoring their fixed residential or Wi-Fi networks. The NFM-F module provides a centralized subscriber management dashboard that enables network-wide monitoring through a customizable KPI and alarms view. This helps operators understand the state of the network and take preemptive actions to resolve current or potential problems. Troubleshooting capabilities allow a drill-down view into each individual subscriber and end device. A variety of tests can be used to help the operator (or support staff) to identify and resolve end-user issues.
Virtual Network Functions Manager

Operators seeking to accelerate the deployment of Nokia Virtual Service Router (VSR) and Evolved Packet Core (EPC) virtual network functions (VNFs) will welcome the addition of a carrier-grade VNF manager (VNFM) to the widely adopted Nokia Network Services Platform (NSP). The NFM-P module delivers out-of-the-box VNFM integration, thus simplifying the fit of the Nokia IP Routing and EPC VNF solution into OpenStack-based network functions virtualization (NFV) and management and orchestration (MANO) architectures.

For more information on the NFM-P module’s VNFM functionality, please refer to the VNFM application note.

Table 1. NFM-P Premium feature summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>• Gain additional applications along with all the classic NFM-P capabilities</td>
</tr>
<tr>
<td></td>
<td>• Premium applications deliver specialized GUIs catered to roles and responsibilities of specific user groups</td>
</tr>
<tr>
<td>Golden configuration/snapshots</td>
<td>• Audit network element configurations to compare the current configuration against snapshots or golden configurations</td>
</tr>
<tr>
<td></td>
<td>• Create backups of network element configuration at any point in time</td>
</tr>
<tr>
<td></td>
<td>• Retain a number of backups for various points in times</td>
</tr>
<tr>
<td>NGE security</td>
<td>• Encrypt MPLS-based user traffic end to end without the need to manage a mesh of IPSec tunnels</td>
</tr>
<tr>
<td></td>
<td>• Deliver comprehensive protection of both IP and non-IP traffic seamlessly at the MPLS layer</td>
</tr>
<tr>
<td></td>
<td>• Manage network group encryption for Layer 2 and 3 services to minimize operational overhead and complexity</td>
</tr>
<tr>
<td></td>
<td>• Enable simplicity in performing key creation, distribution and re-keying in large-scale networks</td>
</tr>
<tr>
<td>Service assurance</td>
<td>• Monitor service health with summaries and detailed supervisory views showing fault trends, KPIs and OAM service validation</td>
</tr>
<tr>
<td></td>
<td>• Validate performance and SLAs for end-to-end services as well as individual service segments</td>
</tr>
<tr>
<td></td>
<td>• Investigate routing issues with potential services impact by highlighting service paths on an IGP topology</td>
</tr>
<tr>
<td></td>
<td>• Easily assess fault impact on services with advanced visualization showing service-to-network alarm correlation</td>
</tr>
<tr>
<td>Network and service analytics</td>
<td>• Monitor IP network infrastructure and service health and performance</td>
</tr>
<tr>
<td></td>
<td>• Report on ITU-T Y.1731 standards-based Ethernet OAM testing</td>
</tr>
<tr>
<td></td>
<td>• Report on bandwidth utilization per port or per service access point</td>
</tr>
<tr>
<td></td>
<td>• North-bound interface for OSS integrations with third-party performance and SLA management applications</td>
</tr>
<tr>
<td>Traffic monitoring and visualization</td>
<td>• Traffic utilization statistics (current and historical) for IP and MPLS interfaces (for RSVP-based LSPs) and IP/MPLS aggregate summaries</td>
</tr>
<tr>
<td></td>
<td>• Threshold-based status lists for utilization levels</td>
</tr>
<tr>
<td></td>
<td>• Lists bandwidth (current or historical) for all LSPs traversing over specific MPLS interfaces</td>
</tr>
<tr>
<td>BGP monitoring</td>
<td>• BGP IP prefix monitoring with prefix health indicators</td>
</tr>
<tr>
<td></td>
<td>• Tracking of application reachability with alarms for monitored prefixes that do not exist or are removed</td>
</tr>
<tr>
<td>Root-Cause and Impact Analysis</td>
<td>• Live network impact analysis automates LSP change impact analysis (auto OAM and alarm on LSP changes)</td>
</tr>
<tr>
<td>(RCIA)</td>
<td>• Simulated impact analysis</td>
</tr>
<tr>
<td></td>
<td>– Simulates a saved simulated topology or a checkpoint from the current topology</td>
</tr>
<tr>
<td></td>
<td>– Simulates addition, deletion or status of routers, adjacencies and/or modified IGP attributes</td>
</tr>
<tr>
<td></td>
<td>– Compares paths — before and after simulation — across multiple areas</td>
</tr>
<tr>
<td></td>
<td>– Uses SPF and CSPF functions in a simulated network</td>
</tr>
</tbody>
</table>
Category: Multicast Manager Application (MMA)
- Centralized management for channel/group, source, rendezvous points (RPs), bootstrap routers (BSRs) and Protocol Independent Multicast (PIM)/IGMP relationships
- Lists all groups with router membership, all source and related RPs, all RPs (elected and candidate), routers in anyicast RPs
- Visualizes PIM/IGMP protocol configuration on IGP topology using different icons to quickly see misconfigurations
- Highlights the topology of the candidate and elected BSRs or RPs, the source for a given group, or the best RP for a given group
- Auto-generates multicast tree for group/source combination using network data
- Auto-generates multicast OAM tests from a set of routers for a given group and source
- Stores each trace in an historical record for future comparison
- Correlates between PIM and point-to-multipoint (P2MP) within IP VPNs
- RSVP mVPNs support monitors P2MP LSP paths and traces them on IGP topology with highlight overlays

Category: Subscriber management dashboard
- Centralizes network-wide monitoring and takes preemptive actions to resolve current or potential problems
- Customizes views on KPIs and alarms to better understand the state of the network
- Troubleshoots issues with drill-down views into individual subscribers and end devices
- Performs diagnostics to identify and resolve end-user issues

Category: Virtual network functions manager (VNFM)
- Integrated carrier-grade VNF manager accelerates deployment of Nokia VSR and EPC VNFs
- Integrated lifecycle management includes VNF catalog-based instantiation, to VNF configuration, scaling and healing
- Converged NMS-VNFM functions deliver operational consistency for management and assurance across both physical and virtual network functions (PNFs and VNFs)
- Continuous monitoring of service quality and network health across both PNFs and VNFs to alert operators proactively
- Dynamically provide more capacity to match unforeseen demand using threshold-based automation to scale additional VNFs up (or down)

Platform summary
The Nokia Network Services Platform provides the architecture, security and other facilities utilized by all applications. It also provides a north-bound interface for OSS/BSS application integration. (See Table 2 for the platform feature summary.)

Table 2. Nokia Network Services Platform platform feature summary for NFM-P

<table>
<thead>
<tr>
<th>Category</th>
<th>Features</th>
</tr>
</thead>
</table>
| Architecture              | • Distributed, high-availability architecture for redundancy and fast system failover  
                             • Server virtualization options using VMware vSphere and Linux KVM hypervisors                                                  |
| Network discovery         | • Network discovery and data collection using various south-bound interfaces, such as: SNMP, NETCONF, CLI, (S)FTP, OpenFlow  
                             • Subnet-based auto-discovery of in-band and out-of-band network elements  
                             • Real-time synchronization with network element changes  
                             • Configurable MIB polling policies and schedules — for accounting statistics or OAM tests, for example  
                             • Highly scalable alarm and SNMP statistics collection                                                  |
| Security                  | • Operator profile management, including for controlled user access to NMS functions and network resources  
                             • User/OSS client activity logs  
                             • Server hardening to industry-standard best practices (for port use, protocol use, authentication, authorization, and so on)  
                             • RADIUS/TACACS+ authentication  
                             • SNMPv3 trap authentication  
                             • SSHv1/v2 to device and SFTP from device  
                             • Database error monitoring to scan for SQL injection attacks                                                 |
OSS/BSS integration

- Open, bidirectional REST, RESTconf, XML and Java Messaging Service (JMS) interfaces
- Allows many simultaneous operational OSS clients
- Software development kit with sample code and developer's guide
- Custom OSS web application interfaces developed through the Nokia Service Portal
- Nokia NSP Connected Partner Program certifies integration between the NSP and market-leading OSS applications

Scalable, secure and flexible system architecture

High availability, system redundancy and fast system failover options allow operators to implement a highly secure network operations environment. The distributed architecture enables support for the largest networks and a massive volume of statistics.

Server virtualization

The NSP virtualized server deployment enables NMS or IT administrators to easily integrate the NSP into their standardized environment, reducing OPEX and taking advantage of generic solutions for redundancy and backup/restore. And virtualized server deployment can leverage existing IT technologies such as storage area network (SAN) capabilities for data replication, as well as hypervisor monitoring and maintenance tools.

The NSP supports service virtualization options using VMware vSphere and Linux KVM hypervisors, including image-based instantiation through OpenStack.

User security with scope of command and span of control

Scope of command allows network administrators to define each operator's access to operations and commands. The definition of “workspaces” facilitates the assignment of areas of responsibility to operator groups. With span of control, network administrators can subdivide network resources and assign operators clear ownership, based on security privileges for their geographic location, organizational group, job function or individual responsibilities.

OSS/BSS integration

Full access to NFM-P module functionality and network infrastructure/service management data is provided through an open OSS interface. All NSP applications, including the CPAM, share this common north-bound API accessible from a single platform.

External applications may integrate using a REST/RESTconf API or request-based XML queries, which provide XML results for efficient parsing, as well as JMS notifications to trigger event-driven behavior. OSS integrations may also maximize efficiency by triggering NFM-P scripts for pre-processing. External applications subscribed to events through the OSS interface may trigger scripts based on these events. (See Figure 1 for more details on automation through NFM-P scripts.)

Typical OSS/BSS integrations would include applications for service activation/provisioning, fault management, performance reporting, SLA management, billing, traffic engineering and network capacity planning.

Nokia NSP Connected Partner Program

The Nokia NSP Connected Partner Program further reduces OSS integration time and costs by certifying integration of the Nokia NSP with applications from industry-leading independent software vendors.
Technical specifications

Operating environment
The Nokia NSP NFM-P, Release 17, operates on the following:

• Main, database, auxiliary servers and clients
  - x86 platforms supported: HP® Intel-based
  - Operating systems supported: Red Hat® Enterprise Linux® (RHEL) 6
  - Databases supported: NFM-P Database embeds installation of Oracle® Database 12c

• Virtualization: VMware vSphere ESXi 5.0, 5.1, 5.5 and 6.0 and Linux KVM on RHEL 6.3/6.4/6.5/6.6/6.7 using QEMU version 0.12.1.2 (OpenStack instantiation enabled through QCOW image)

• Additional clients:
  - Microsoft® Windows® 7 and 8 Professional (32-bit and 64-bit editions)
  - Microsoft® Windows® Server 2008R2/2012 (also for client delegate servers; including support for Citrix XenApp 6.5 and 7.6)

Minimum hardware requirements for Nokia NSP, Release 17

<table>
<thead>
<tr>
<th>Applications</th>
<th>X86 platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFM-P main server:</td>
<td>1 quad core CPU</td>
</tr>
<tr>
<td>• It is recommended that the NFM-P server be installed on a workstation separate from that of the NFM-P database for large-scale deployments.</td>
<td>24 GB RAM</td>
</tr>
<tr>
<td></td>
<td>4 disk drives, minimum 146 GB each</td>
</tr>
<tr>
<td>NFM-P database (Oracle Database 12c):</td>
<td>1 quad core CPU</td>
</tr>
<tr>
<td>• Stores network objects and configuration</td>
<td>16 GB RAM</td>
</tr>
<tr>
<td>• NFM-P server can be installed on a workstation separate from that of the NFM-P database for large-scale deployments</td>
<td>4 disk drives recommended, minimum 146 GB each</td>
</tr>
<tr>
<td>• RAID 0 and 1+0 technologies are supported</td>
<td></td>
</tr>
<tr>
<td>• SAN storage is supported with 4 GB or faster optical connections with dedicated Fibre Channel connection between hosts and storage arrays or iSCSI over 10G</td>
<td></td>
</tr>
<tr>
<td>NFM-P auxiliary statistics collector server:</td>
<td>4 quad core CPUs</td>
</tr>
<tr>
<td>• Dedicated server required for large-scale deployments</td>
<td>16 GB RAM</td>
</tr>
<tr>
<td>• For NFM-P logToFile large-scale collection</td>
<td>8 disk drives, minimum 146 GB each</td>
</tr>
<tr>
<td>• Dedicated server required for call trace and debug trace data collection</td>
<td></td>
</tr>
<tr>
<td>NFM-P Java client:</td>
<td>1 CPU, 2 GHz or higher</td>
</tr>
<tr>
<td>• GUI presentation front end</td>
<td>1 GB dedicated RAM</td>
</tr>
<tr>
<td>• Only one client should be installed per platform</td>
<td>1 GB available disk space</td>
</tr>
<tr>
<td></td>
<td>1280 × 1024 display resolution</td>
</tr>
<tr>
<td>NFM-P client delegate and third-party remote display server:</td>
<td>4 CPU cores</td>
</tr>
<tr>
<td>• Single client install for multiple GUIs for multiple users</td>
<td>24 GB dedicated RAM</td>
</tr>
<tr>
<td>• Citrix is recommended third-party remote display software</td>
<td>1 GB available disk space</td>
</tr>
<tr>
<td>• X11 protocol and native X displays supported</td>
<td>For a maximum of 15 concurrent GUIs. Increased hardware specifications are required as number of concurrent GUIs increases.</td>
</tr>
</tbody>
</table>

Note: Hardware recommendations may vary depending on scale of deployment. Contact your Nokia representative for the Nokia Network Services Platform NFM-P module Planning Guide for hardware requirements and platform sizing recommendations.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

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

Product code: PR160802Z122EN (October)