Junos Space Network Director

Product Overview

Whether in the data center or the campus, today's network managers are learning to overcome many new challenges. Data center network and cloud administrators face the rapid adoption of virtualization, dynamic and on-demand cloud services, and virtual network deployments. In the campus, wireless devices are increasing at a rapid rate, attacks and threats are evolving, and wireless networks demand mission-critical uptime.

Junos Space Network Director is a next-generation network management solution that allows users to visualize, analyze, and control the entire enterprise network—data center and campus, physical and virtual, wired and wireless—through a single pane of glass.

Your ideas. Connected.™

Product Description

Juniper Networks® Junos® Space Network Director provides a smart, comprehensive, and automated network management solution that enables network and cloud administrators to visualize, analyze, and control their entire enterprise network—data center and campus, physical and virtual infrastructure, virtual overlay networks, and wired and wireless—through a single pane of glass. In the data center, Network Director helps administrators manage, visualize, and troubleshoot physical and virtual environments by providing correlated visibility between overlay and physical networks, as well as flow analysis, visualization, and synchronization of network policies as virtual machines (VMs) move from server to server. In the campus, Network Director automates routine management tasks such as network provisioning and troubleshooting, dramatically improving operational efficiency and reliability.

Network Director incorporates key functions that address the challenges posed by the rapid adoption of virtualized, dynamic, and on-demand cloud services across data center and cloud deployments. In addition, Network Director offers sophisticated end-to-end network visibility and flow path analysis in conjunction with the Juniper Networks Cloud Analytics Engine, providing flow-aware performance analysis to improve application performance and availability by associating flows/applications across the physical and virtual infrastructure, improving the ability to quickly roll out new applications and troubleshoot problems.

These smart network management capabilities are delivered through the following key features.

Automate

- **Zero touch provisioning** (ZTP) simplifies the deployment of networks without requiring user intervention, providing policy-driven plug-and-play provisioning and network bring-up operations for both fabrics and individual devices.
- **Bulk provisioning** enables faster service rollout and activation while protecting against configuration errors with profile-based and pre-validated configurations. Bulk operations can be performed at logical (access, aggregation, core) or location (site, building, floor, rack) levels.

Analyze

- **Performance Analyze**r provides real-time and trended monitoring of hosts, VMs, fabrics, and ports, as well as high-frequency monitoring that gathers valuable performance data for tracking queue depth and heat-map visualization. Network Director analyzes the entire network, using heat-maps to identify over- and under-utilized ports, latency, and top VMs, users, devices, and ports.
- **Flow Path Analyzer** provides operational and diagnostic capabilities that trace connectivity between applications and flows by correlating network telemetry data with the application. Flow Path Analyzer visualizes network paths between leaf and

spine switches for a given flow/application, correlating congested ports with high-latency events and identifying impacted or unhealthy VMs, applications, and hosts.

- **Overlay and Underlay Analyzer** provides full visibility, performance management, and troubleshooting capabilities for physical and virtualized overlay networks in VMware Virtual Extensible LAN (VXLAN) environments. It provides a consolidated and correlated view of VMs, hosts, fabrics, and overlay and underlay networks with full end-to-end network and flow visibility and analysis.
- **VM Analyzer** provides real-time physical and virtual topology views, tracks vMotion activity including virtual machine creation, deletion, and moves, and maintains complete virtual network inventory.
- **Fabric Analyzer** monitors and analyzes the health of the entire network fabric, including IP Fabric, Virtual Chassis Fabric configurations, and Juniper Networks QFabric® System, increasing service availability.

Features and Benefits

End-to-End Network Visibility and Flow Path Analysis

Working in conjunction with the Cloud Analytics Engine, Network Director provides network data analysis to improve application performance and availability by associating flows with specific applications across the physical and virtual infrastructure, improving the ability to quickly roll out new applications and troubleshoot problems (see Figure 1).

Network Director analyzes and visualizes application flows running on VMs and bare-metal servers in the data center, reporting the specific path a flow takes through the network, the latency encountered at each hop, and traffic statistics for every network device in the path. Users can start flow analysis on selected active flows on a specific VM or a non-virtualized host on demand and view the results. When users place a critical VM or non-virtualized host on a watch list, Network Director will automatically initiate analysis on all flows running on that device.

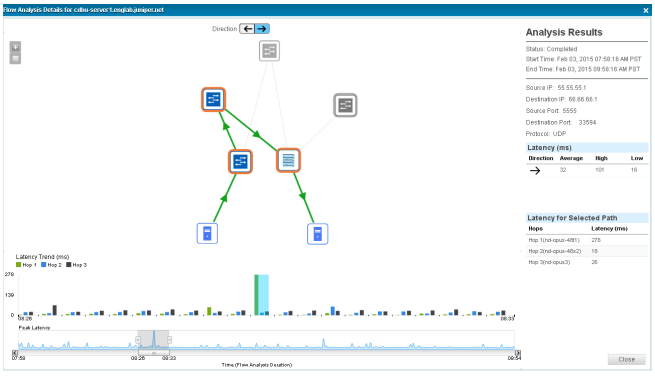

Figure 1: Flow path analysis

Integration with Virtualized and Cloud Infrastructure

Network Director integrates with virtualized and cloud infrastructure tools, providing network and cloud administrators with a comprehensive view of the complete data center infrastructure. Network Director also provides holistic and correlated visibility into enterprise and private cloud data centers comprised of physical switch fabrics and virtual networks (overlay) (see Figure 2), as well as virtualized and non-virtualized hosts encompassing the following deployments:

- **VMware vCenter**—Network Director unifies physical and virtual networks, providing a comprehensive view of the complete end-to-end virtual-to-physical network infrastructure. It integrates with VMware vCenter, delivering a combined solution that benefits from both vendors' innovation and from Juniper's orchestration solutions to discover, visualize connectivity between virtual and physical networks, orchestrate, and monitor VMware vSphere environments.
- **VMware NSX Multi Hypervisor and OpenStack**—Network Director integrates with cloud infrastructure controlled by VMware NSX Multi Hypervisor SDN Controller environments and OpenStack. Through this integration, Network Director provides complete and correlated visibility between virtualized overlay and physical networks as well as virtual machines, VXLAN, virtual tunnel endpoints, and OpenStack networks with full end-to-end network and flow visibility and analysis (Figure 2).

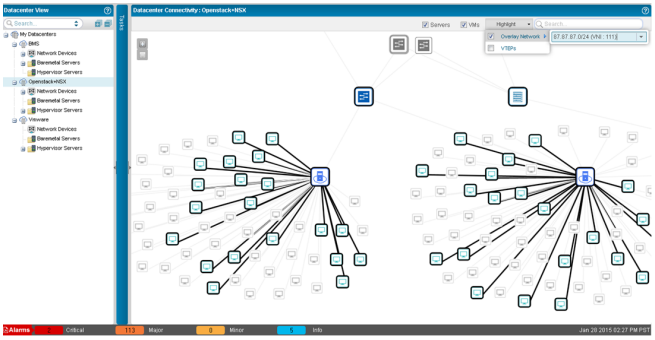

Figure 2: Overlay and underlay network visibility

In addition to virtualized and cloud infrastructure deployments mentioned above, Network Director also includes support for non-virtualized servers (also called bare-metal servers).

Fabric Automation and Management

Network Director provides comprehensive pre- and post-deployment fabric automation and management for Layer 2 and Layer 3 fabric topologies. It fully automates the provisioning, configuration, and deployment of complex fabric topologies comprised of multistage spine-and-leaf switches, eliminating errors associated with manual deployment (see Figure 3). As part of the pre-deployment automation process for Layer 3 fabrics, Network Director provides simple-to-use workflows to set up fabric switches, assign protocol settings, perform BGP IP address configuration and cabling, and set up ZTP servers.

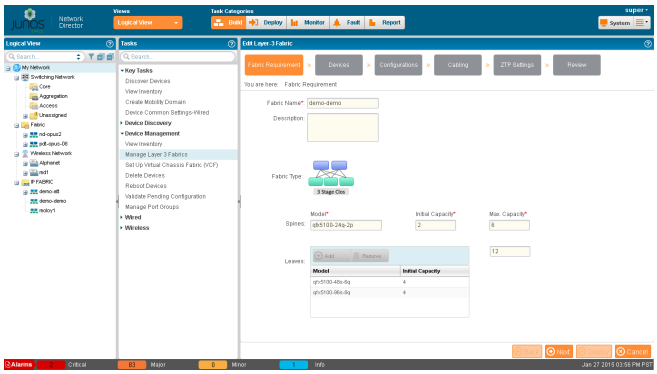

Figure 3: Fabric automation

Network Director also automates the discovery of fabrics and all of their associated switches. In addition, it performs cabling checks to ensure that all devices are connected per the initial design.

Multipoint Navigation and Views

Network Director improves operational efficiency by allowing users to manage the network from different views, groupings, and perspectives. It includes a customizable dashboard that provides a visual indication of overall network usage and network consumers, including VMs, hosts, top virtual networks, flow analysis, utilization, latency, top talkers, and alarms—all presented as part of a color-coded heat map representing devices and ports. Each device is color coded to convey the level of port utilization and latency; "cooler" colors indicate lower port utilization and latency while "hotter" colors indicate higher port utilization and latency (see Figure 4).

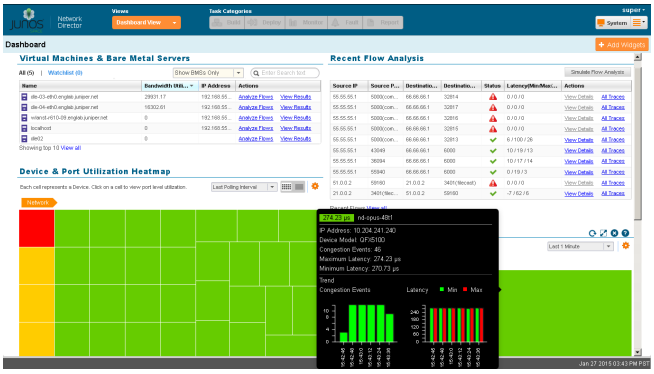

Figure 4: Dashboard view

In addition, Network Director Topology view shows all discovered devices in the network on a map where the devices are located across sites, buildings, floors, closets, and racks, along with their physical connections to other devices in the network. Topology view also shows the physical and logical connectivity between various discovered interconnected devices. Topology view allows users to zoom in or out of a site, see how a device is connected to its immediate neighbors, including VMware hosts connected to the switch, or view alarm details, bandwidth of links, and real-time link data and state of the devices. Network Director also enables devices to be rearranged across buildings on the map.

Complete Life Cycle Management

Network Director fully integrates all life cycle management functions into a single application, lowering operational and capital expenditures by eliminating the need for multiple platforms to perform configuration, monitoring, or fault management for a wired and wireless management solution.

Each life cycle stage is represented as a mode in Network Director (see Figure 5).

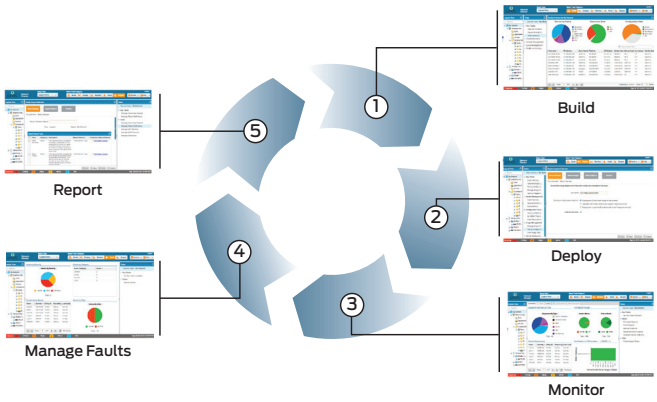

Figure 5: Full life cycle management

Build Mode

Network Director Build mode is used to discover network devices and create and manage device configurations. Build mode also allows devices to be organized into hierarchal groupings based on logical relationships or physical locations.

- In Network Director, bulk configuration is performed through profiles. Profiles are used to configure common parameters across the network using wizards that seamlessly handle various configuration elements that are easily associated with a device, collection of devices, port, logical entities, or even physical locations.
- Network Director supports existing deployments. As devices are discovered, their configurations are parsed for various elements to map the configuration data to profiles. Multiple devices with the same configuration will have a single profile created that is associated with those devices.

Deploy Mode

In Deploy mode, device-related changes such as image management, configuration pushes, and reconciliations are applied. As with other modes, actions can be performed on a device, a group of devices, or a location.

- Simplify network deployments: ZTP simplifies the deployment of networks without requiring user intervention, while providing policy-driven, plug-and-play bootstrap and network bring up operations.
- Manage software images: Network Director maintains a repository of software images that have been uploaded. Multiple software images from the repository can be deployed

in a single action even when they are on multiple devices. Devices can be selected based on location, device model, or the role of the device in the network. The staging of the image—that is, downloading the software package to the device—can be separated from the actual installation of the package. Both the individual steps of staging and the upgrade can be performed immediately or as a scheduled event.

- Initiate, schedule, and track configuration deployment: Changes to a device's configuration performed in Build mode result in the device being added to a list of devices with pending changes. Pending changes can be applied to the device in Deploy mode. Network Director offers both auto and manual approval modes; in manual approval mode, device configuration changes must be explicitly approved before they can be deployed.
- Resynchronize device configuration: Network Director will automatically detect if a configuration on a device is out of sync. The administrator has the option of keeping the current configuration or changing the Network Director configuration database to reflect what has been observed in the network.
- Restore and back up device configuration: Ethernet switch or WLAN device configurations can be backed up in Network Director. Network managers can restore an archived configuration at a later date.

Monitor Mode

Monitor mode provides detailed visibility into network status and performance by collecting information from devices and maintaining that information in a database (see Figure 6). The Monitor life cycle offers graphs that are easy to understand and tables that can be sorted and filtered, allowing users to quickly visualize the state of the network, spot trends developing over time, and review important details. The Monitor life cycle divides monitoring activity into the following categories:

- **Traffic Monitoring:** The Traffic Monitoring view provides information for analyzing traffic on Ethernet switches, QFabric Systems, Virtual Chassis Fabrics, IP Fabrics, and WLAN devices. It provides an overview of the traffic on each device such as the proportion of multicast, unicast, or broadcast traffic on the network or a trend in packet errors. Tasks provide detailed views of traffic on individual ports or VLANs, as well as access and trunk port utilization.

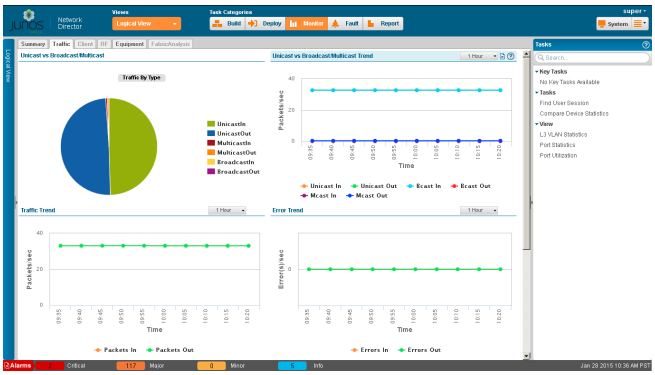

Figure 6: Monitor mode view

- **Client Monitoring:** The Client Monitoring view provides information about clients and sessions on the network such as mobile devices, VoIP phones, laptops, printers, and security cameras. It also provides overall client session activity, including total number of sessions, sessions consuming the most bandwidth, and trends in the number of sessions. In addition, detailed information about each client such as media access control (MAC) address, IP address, user name (802.1X clients), client VLAN and port, or the access point (AP) providing access to a wireless client, can be viewed.
- **Equipment Monitoring:** The Equipment Monitoring view provides resource usage and status information for network devices. It provides CPU and memory usage, power supply, fan status, port status, and general device information for Ethernet switches (including Virtual Chassis connected switches) and WLAN controllers and access points.
- **Fabric Analyzer:** The Fabric Analyzer provides health, connectivity, and topology information of the selected Virtual Chassis Fabric configuration or QFabric System. It performs redundancy, minimum connectivity, and minimum component checks as part of an overall health analysis, as well as providing control plane connectivity information, data plane connectivity information, and general health of the system. The Topology views lay out QFabric System components or Virtual Chassis Fabric deployments configured in spine-and-leaf mode (see Figure 7).

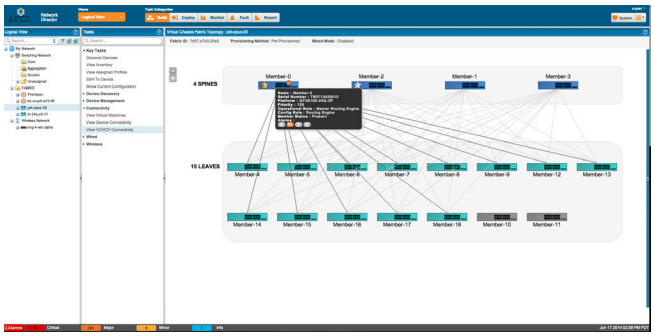

Figure 7: Virtual Chassis Fabric topology

Monitoring Mode features include:

- High-frequency statistics data collected and analyzed from Juniper Networks QFX Series switches to create network heat maps and monitor latency
- Virtual Chassis Fabric health, connectivity, and topology views
- QFabric System control and data plane connectivity and health check
- QFabric System control and data plane topology views
- IP Fabric spine-and-leaf switches aggregated, and device-level traffic and port utilization statistics
- Monitoring and alarms for network elements
- Summary of alerts and network traffic by infrastructure (port, device, VMs, network) and location

- Device, virtual controller cluster, and Virtual Chassis status and availability
- Top N devices by port utilization
- Access vs. trunk port utilization
- Comparison statistics between different interfaces
- Detailed user and device information and distribution by mobile device type (iPhone, Android, etc.)
- Finding users and end nodes in the network
- Up to one year of trended data
- User-centric features that include:
  - User statistics and session status
  - Device profiling
  - Session-related alarms (authentication and authorization failures, threshold crossing, invalid IP address, etc.)
- Security features that include:
  - Wireless intrusion detection and prevention system (WIDS/WIPS) alarms
- RF views that include:
  - RF parameters (signal-to-noise ratio, utilization, etc.)
  - Spectrum management

Fault Mode

Fault mode provides visibility into unexpected network events and manages network faults or exceptions, which appear as alarms in Network Director. Network Director collects, analyzes, and correlates these low-level events into alarms, allowing network administrators to view current active alarms, summaries of categorized alarms, and alarm details, including the individual events that are correlated to an alarm. Fault mode features include:

- Status, performance, and threshold views
- Ability to apply de-duplication and correlation with monitoring
- Threshold, outage, and trend views
- Ability to receive SNMP traps directly from devices
- Event and alarm generation and display
- Alarm acknowledgement, escalation, and resolution
- Device fault detection based on collected data
- Virtual networking alarms from VMware

Report Mode

Report mode enables administrators to run reports on collected data that is stored on a server. Network Director can set up report definitions that specify the format of the report (HTML, PDF, CSV), the historical time frame that the report covers, and the report contents. Users can choose between predefined report content for reporting on alarms, Network Director activity, device inventory, sessions, traffic, and radio frequency (RF) information. Scope can be selected around a device, a location, or a group of devices. Reports can be scheduled to run at a specified time in the future or on a recurring basis.

Generated reports are stored and are available for downloading. Reports can be delivered through e-mail or archived to an SCP file server when the report definition is created.

Aruba Airwave Integration

Network Director integrates with the Aruba Airwave management platform to provide simplified network management. Juniper's wired technologies such as switching collaborate with the wireless LAN technologies of Aruba Networks to enable you to monitor and configure wireless networks. The integration of these two management platforms enables you to use Network Director to:

- View the Aruba wireless device inventory in Build, Monitor, Report, and Fault modes of Network Director to view all of the Aruba wireless devices connected to Juniper switches and proactively identify impacted wireless devices for fault conditions
- Launch the context-sensitive feature on Aruba Airwave application pages (for all Aruba wireless devices or individual wireless devices connected to Juniper Networks switches) from within Network Director to manage Aruba wireless devices

Specifications

Navigation Model

- Use task-based navigation based on the network management life cycle

Network View and Device Selection

- View devices organized by logical relationships, locations, device type, custom group view, data center view, or topology view
- Select logical, location, device-type, custom group, virtual, or topology view groupings to perform tasks on multiple devices simultaneously
- Search for devices in the network
- Define filters to selectively view specific logical, location, device-type, custom group, virtual, or topology groupings

User Preferences

- Set user preferences, such as whether time is shown in the client time zone or server time zone

Table 1. Supported Platforms

Supported Platforms	Operating System
QFX Series Ethernet Switches: QFX5100 Virtual Chassis Fabric	Junos OS releases 14.1X53-D15, 13.2X51-D20
QFX5100	13.2X51-D25, 14.1X53-D16
QFX3500/QFX3600 (non ELS) QFX3500/QFX3600 ELS and Virtual Chassis	12.3X50-D35 and 12.3X50-D40
QFabric Systems (QFX3000-G and QFX3000-M)	14.1X53-D15, 13.2X52-D20
EX Series Ethernet Switches: EX2200, EX2200-C EX3200 EX3300: Standalone and with Virtual Chassis technology EX4200: Standalone and with Virtual Chassis technology EX4500: Standalone and with Virtual Chassis technology EX4550: Standalone and with Virtual Chassis technology Mixed EX4200, EX4500, EX4550 Virtual Chassis configurations EX6200 EX8200: Standalone and with Virtual Chassis technology	Junos OS releases 11.4, 12.1, 12.2, 12.3, 13.2X50-D10, 13.2X50-D15, 13.2X51-D15, 13.2X51-D20, 13.2X51-D30, 14.1X53-D15
EX Series Ethernet Switches with ELS: EX4300 Standalone and with Virtual Chassis technology	Junos OS releases 13.2X51-D15, 13.2X51-D20, 13.2X51-D30
EX4600 Standalone and with Virtual Chassis technology	Junos OS release 13.2X51-D25
EX9200	Junos OS releases 13.2R1, 13.2R2, 13.3R2, 14.1R4, 14.2R2
MX Series 3D Universal Edge Routers MX240, MX480, MX960 (ELS)	Junos OS releases 13.2R2.4, 14.1R4, 14.2R2
MX80, MX104, MX240, MX480, MX960 (non-ELS)	Junos OS release 14.1R4
Cloud Infrastructure support VMware vCenter Server	VMware ESX versions 4.0 and 4.1
VMware Host	VMware ESXi versions 5.0, 5.1, and 5.5
OpenStack	Supported release—Icehouse
VMware NSX -MH	Version 4.1 or 4.2
WLC Series Wireless LAN Controllers: WLC2 WLC8 WLC100 WLC200 WLC800 WLC880 WLC2800	MSS releases 7.7 and 8.0 for WLC2 MSS releases 7.7, 8.0, 9.0 and 9.1 for other controllers
Juniper Networks Firefly Perimeter	MSS releases 9.0 and 9.1
WLA Series Wireless LAN Access Points: WLA321, WLA322 WLA422, WLA432 WLA522, WLA522E WLA532, WLA532E WLA620, WLA622 WLA632	MSS releases 7.7, 8.0, 9.0, and 9.1
Aruba Airwave	Aruba Airwave version 8.0.7

Virtualization Management

- Set up and view data center networks and topologies
- Discover virtual networks
- Automatically orchestrate physical switches based on vMotion
- View hosts, virtual switches, machines, overlay networks, and virtual tunnel end points (VTEPs)
- View connectivity between VMs, virtual switches, physical switches, and overlay networks
- View vMotion history, VM and host bandwidth utilization
- Compatible with VMware vCenter versions 4.1, 5.0, 5.1, and 5.5
- Compatible with VMware vSphere versions 4.0, 4.1, 5.0, 5.1, and 5.5
- Compatible with VMware NSX4.2
- Compatible with OpenStack Icehouse

Build Mode Features

- Discover and manage devices
- Automate and manage fabrics
- Discover devices to be managed by Network Director
- View inventory of devices for selected logical, location, or device-type groupings
- Launch command-line interface (CLI SSH session), Junos Web interface (switches), or Web View interface (wireless LAN controllers)
- View physical inventory for a switch or a WLAN controller
- Add and configure access points in your wireless network (with existing AP configuration imported during device discovery)
- Assign switches to core, aggregation, or access roles for logical view
- Reboot switches, wireless LAN controllers, and access points
- View a device's current configuration
- View profiles assigned to a device
- Validate pending configuration on a device
- Set up QFabric System and Virtual Chassis Fabric

Configuration Profiles

- Create, edit, or delete the following profiles:
  - Access profile (EX Series Ethernet Switches and WLC Series Wireless LAN Controllers)
  - Authentication profile (EX Series and WLC Series)
  - Authorization profile (WLC Series)
  - Class-of-service (CoS) profile (EX Series, QFX Series, QFabric System, and WLC Series)
  - Device basic settings profile (EX Series, QFX Series, QFabric System, and WLC Series)
  - Filter profile (EX Series, QFX Series, QFabric System, and WLC Series)
  - Port profile (EX Series, QFX Series, and QFabric System)
  - Radio profile (WLC Series)
  - VLAN profile (EX Series, QFX Series, QFabric System, and WLC Series)
  - WLAN service profile (WLC Series)

- Assign authorization, device basic settings, port, radio, and VLAN profiles to network objects
- Import existing configuration into system created profiles during device discovery and have profiles automatically assigned to devices

Wireless Network Domains

- Create mobility domain, network domain, and enable Smart Mobile Virtual Controller clustering
- Import existing mobility domain and cluster configurations during device discovery
- Manage for location
- Create sites, buildings, floors, closets, aisles, racks, and outdoor areas for organizing "location" view
- Assign devices to locations
- Leverage Aruba Airwave wireless management integration

Deploy Mode Features

- Configuration changes
  - View pending configuration changes and validate changes before deploying configuration on devices
  - Automatically deploy changes on selected devices immediately or at a scheduled time
  - Manual Approval mode requires device configuration changes to be explicitly approved
  - View deployment results and manage configuration deployment jobs
- Software images
  - Maintain a repository of software images for switches and wireless LAN controllers
  - Deploy selected images on selected devices immediately or at a scheduled time
  - View deployment results and manage image deployment jobs
- Resynchronize configuration
  - Resynchronize the saved device configuration with the configuration on the device
- Configuration file management
  - Back up and restore device configuration files

Monitor Mode Features

- Data capture
  - Set polling periods for collecting different kinds of data
- Traffic monitoring (view the following for traffic on switches and wireless LAN controllers):
  - Current mix of unicast, multicast, and broadcast packets, and trends over time
  - Packet error trend
  - Port traffic trend
  - Current port utilization and trend
  - VLAN traffic trend on switches
  - Virtual Chassis Control Protocol (VCCP) statistics
  - Fabric Analyzer for Virtual Chassis Fabric and QFabric System
  - Top VMs by bandwidth utilization
  - Host network interface card (NIC) bandwidth utilization
  - Virtual switch summary by version
  - VM bandwidth utilization trend
  - Distribution of mobile devices
- Mobile Analyzer: Client session monitoring
  - Search for client session and view session history
  - View the following for wireless and wired clients:
    - Top bandwidth clients by MAC address (wireless clients only)
    - Current session count and session trend
    - Client session details—user name, MAC address, device type, device group, device profile, AP name, service set identifier (SSID) VLAN
    - Top APs by traffic and session
    - Current SSID statistics
- Mobile Analyzer: Radio frequency (RF) monitoring (view the following):
  - Throughput, packet error, and retransmit trends
  - Signal-to-noise ratio trend
  - RF interference sources
  - RF spectrogram (2.4 and 5 GHz)
  - RF neighborhood
- Equipment status
  - System information (view the following):
    - Device status and information
    - CPU and memory usage
    - Fan and power supply status
    - Port status
    - Logical interface information and status
    - Virtual Chassis topology
    - Access point and radio status

Fault Mode Features

- Alarm monitoring
  - Correlate low-level faults into easy-to-understand alarms
  - View current counts of critical, major, and minor alarms (always visible in user interface)
  - View alarms for selected scope by category, severity, and state
  - View individual alarm details
  - Search for an alarm
- Alarm management
  - Select which alarms are enabled and select the severity level for alarms
  - Configure the length of time that alarms are kept on the server
  - Acknowledge, assign, annotate, and clear alarms
  - Receive and respond to alarm notifications

Report Mode Features

- Report content (available report types):
  - Fabric analyzer
  - IP Fabric
  - Client details
  - Network usage
  - Security alarms
  - Alarm summary
  - Alarm history
  - Network Director audit trail

  - Device inventory
  - Top 10 bandwidth users
  - Active user sessions
  - Network device traffic
  - Network neighborhood for access point radios
  - VM inventory
  - VM vMotion history
  - RF interference detail
- Select time frame and scope covered by report (report options):
  - Run reports immediately, or at a specified time, or on a recurring schedule
  - Select report format (PDF, HTML, or CSV)
  - Send reports in e-mail or send them to an SCP server for archiving
- Report management
  - View, delete, download generated reports

System Mode Features

- Audit trail and job management
  - View audit trail of Network Director user and system activity
  - View and manage all jobs
- Troubleshooting support
  - Generate a compressed file of logs and other data to send to Juniper Networks for analysis

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services/.

Ordering Information

Network Director uses a very simple perpetual licensing model and is licensed by the number of devices that it manages, including EX Series Ethernet Switches and WLA Series Wireless LAN Access Points. Whether the device is a wireless LAN access point or an Ethernet switch, it is counted as a device. Wireless LAN controllers are not counted towards the device count. Select any quantities and any combination of the following SKUs for the number of devices you plan to manage.

Table 2. Junos Space Network Director Ordering Information

Model Number	Description
JS-NETDIR-10	Junos Space Network Director for 10 devices
JS-NETDIR-25	Junos Space Network Director for 25 devices
JS-NETDIR-100	Junos Space Network Director for 100 devices

Network Director is part of Junos Space and requires Junos Space Network Management Platform (JS-PLATFORM) to be installed.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

1000428-005-EN Feb 2015