

LN2600 Rugged Secure Router



Product Overview

Scalable, interoperable, high-performance networks with security built in enable energy, utility, water, railroad, first responders, and military organizations to build networks that support mission critical applications. Building out their network infrastructure and scaling to remote locations, however, requires a new ruggedized solution. Juniper Networks LN2600 rugged secure router provides the advanced routing and security technology required to secure remote locations, and it meets the requirements of IP64 for dust-proof and splash-proof environments. The conduction cooled, fan-less LN2600 design can operate in extreme temperature ranges from -40C to +71C.

Product Description

Juniper Networks® LN2600 rugged secure router provides perimeter security, content security, application visibility, tracking and policy enforcement, role-based access control, and network-wide threat visibility and control. Using zones and policies, network administrators can configure and deploy the LN2600 quickly and securely. With the ongoing deployment of IP/MPLS networks, mission critical Supervisory Control and Data Acquisition (SCADA) applications are now being transported over the IP/MPLS network. The security of these control systems is critical, and prioritization of control applications is extremely important for minimizing delay and packet loss. The LN2600 uses the proven Juniper Networks Junos® operating system software for stateful firewalls, intrusion detection and prevention, and IPsec encryption to protect remote locations from unauthorized access, and to protect mission critical control applications from remote locations to the centralized control center.

The LN2600 rugged secure router is a 1 U high 19 inch rack or wall-mountable chassis that supports 8 Gigabit Ethernet small form-factor pluggable transceiver (SFP) interfaces. It includes a single -48 VDC power supply with dual power inputs. It meets IP64, IEEE 1613 Class 2, and IEC 61850-3 requirements. The LN2600 operates in harsh environments with extreme operating temperature ranges supported with no vents and no fans. Hardware based hierarchical quality of service (QoS) capabilities enable mission critical SCADA traffic to be prioritized over the network. Dual boot root partitions and a Non-Volatile Memory Read-Only (NVMRO) option enable more reliable operations and protection against modifications and theft in remote unmanned locations.

As energy and utility companies build out the Smart Grid around the world, IP/MPLS networks will enable them to control, manage, and troubleshoot the distribution of power more efficiently, proactively, and reliably. However, this new communications infrastructure will also require state-of-the-art security to ensure the protection and integrity of the information on the network. The LN2600 rugged secure router will enable the secure, two-way communication required in Smart Grids to enable easier integration with renewable power sources and micro-grids in very harsh environments. Developed for critical infrastructure that supports electricity, oil, gas, water transmission and distribution, the LN2600 is extremely rugged. Combined with the Junos OS security software capabilities, it meets the compliance requirements for North American Electric Reliability Corporation Critical Infrastructure Protection (NERC/CIP).

Architecture and Key Components

Key components of the LN2600 are high-performance routing for remote locations and mobile networks, security features that include a firewall, encryption, and intrusion prevention system (IPS) in a fan-less, vent-less, splash proof system capable of performing in extreme temperatures and harsh environments. The LN2600 can be rack or wall mounted, and it runs the powerful Junos operating system.

Table 1: LN2600 Key Components

Key Components	Description
Ruggedized chassis	<ul style="list-style-type: none"> Fan-less and vent-less 1 U high 19 inch rack or wall mountable chassis with dual -48 VDC power inputs to a single power supply. All Interfaces and cabling are on one side of the chassis and protected by a sealed plexiglass cover. The chassis meets the International Protection profile of IP64 for dust proof and splash proof environments. The conduction cooled fan-less design can operate in extreme temperature ranges from -40C to +71C. The system is NEBS compliant and meets the requirements for GR-3108 Class C environments, IEEE 1613 Class 2, and IEC 61850-3.
8 GbE SFP interfaces	<ul style="list-style-type: none"> The LN2600 supports 8 GbE SFP interfaces, which are purchased separately. The environmentally hardened SFP options are SX, LX, LH, and T.
RS232 console port	<ul style="list-style-type: none"> The RS232 console port can be used to externally monitor operational status as well as to run the Junos OS command-line interface (CLI) while the router is in operation.
IPv4 and IPv6 support	<ul style="list-style-type: none"> Includes support for forwarding of IPv4/IPv6 packets, IPv4/IPv6 firewall, and IPS to ensure scalability on the world's largest networks.
Protocol (4938bis)	<ul style="list-style-type: none"> Allows the LN2600 to communicate to a radio card for uplink using a Point-to-Point Protocol over Ethernet (PPPoE) extension (RFC 4938bis). Support for the protocol enables the LN2600 to monitor available bandwidth on a per-hop basis, and adjust routing tables and message queues to ensure that traffic is transported effectively and efficiently.
QoS	<ul style="list-style-type: none"> The LN2600 will support eight queues per virtual, logical, or physical interface. Each queue can have four random early detection (RED) classes applied to it. The hardware-based QoS capability ensures consistent routing performance across all 8 x 1 Gbps Ethernet ports whether QoS is enabled or not.
Network management	<ul style="list-style-type: none"> The LN2600 is supported by Junos Space Network Activate and Security Director applications
Memory	<ul style="list-style-type: none"> The LN2600 includes 2 GB of RAM and 4 GB of Flash.
Performance	<ul style="list-style-type: none"> 500,000 packets/sec at 64 byte packet size without services enabled 200,000 packets/sec at 64 byte packet size with all services enabled (multicast, QoS, firewall, IDS)

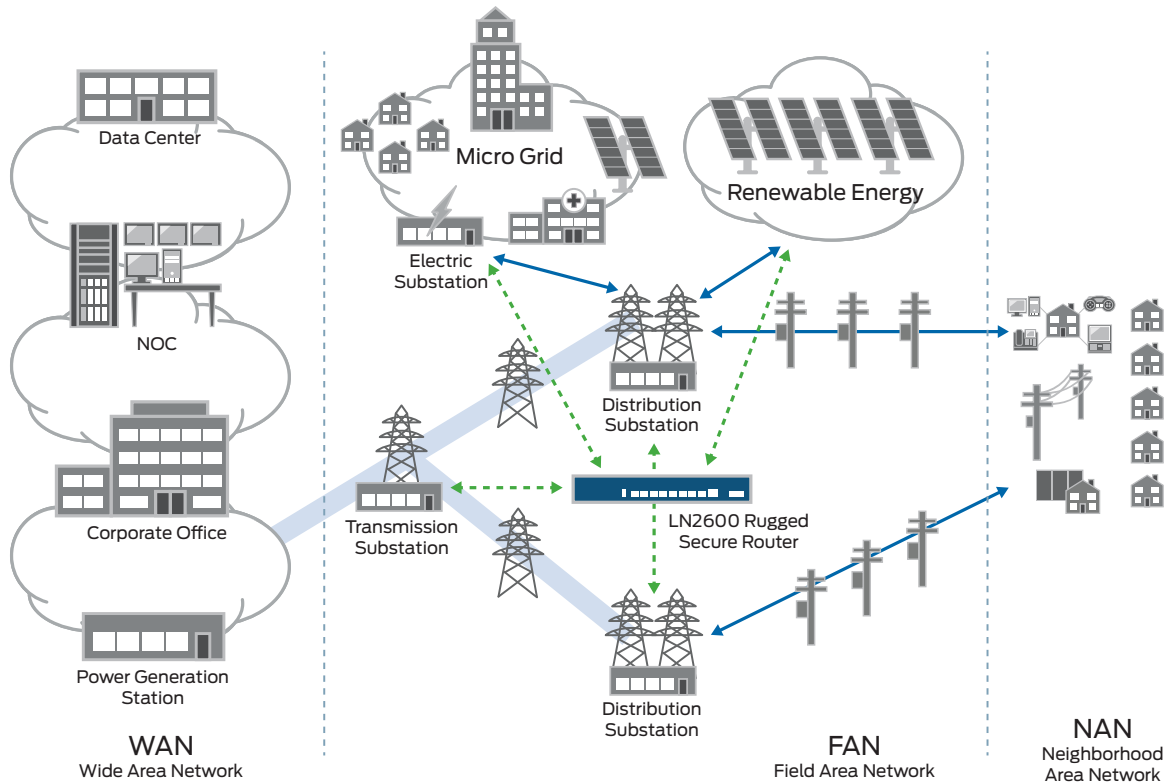


Figure 1: LN2600 in Smart Grid

Features and Benefits

Routing

As a Juniper router, the LN2600 is deployed with Juniper routing hardware, ensuring industry-leading forwarding and routing support even under the harshest network traffic loads. The high-performance routing capabilities of the LN2600 include radio router protocol support. This enables it to overcome difficult mobile networking issues, such as establishing a mesh network configuration using extensions to OSPFv3 routing protocol to include other mobile devices as well as land-based receivers.

The LN2600 also has hardware-based QoS support, which provides consistent routing performance across all 8 x 1 Gbps network interfaces. This hardware-based QoS will support a QoS hierarchy that provides up to eight queues of four precedence levels, delivering classification for up to 32 unique DiffServ code point (DSCP) values. QoS hierarchy support can be used in SCADA, first responder, and military networks to provide differentiated classifications of service based on the location and type of application.

Security

The LN2600 provides a hardware assisted stateful firewall, IPsec VPN encryption, and IPS solution that is based on the capabilities provided in the industry-leading Juniper Networks SRX Series Services Gateways. As a network edge device, the security capabilities within the LN2600 provide network access protection for critical Infrastructure—whether in a substation, subway, gas or water line, on an oil rig, or on the battlefield.

The firewall, encryption, and IPS capabilities in the LN2600 provide denial of service (DoS) attack and network disruption protection in various environments. The primary and secondary root partitions and memory sanitization capability provide protection in case of memory corruption, hacker manipulation, or if a device is lost or stolen.

Firewall

- Stateful firewall, access control list (ACL) filters
- Firewall, zones, screens, policies
- Network attack detection
- DoS and distributed denial of service (DDoS) protection
- TCP reassembly for fragmented packet protection
- Brute force attack mitigation
- SYN cookie protection
- Zone-based IP spoofing
- Malformed packet protection
- Replay attack and anti-replay protection

IPsec

- Data Encryption Standard (DES) (56-bit), triple Data Encryption Standard (3DES) (168-bit), and Advanced Encryption Standard (AES) (256-bit)
- Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA1) authentication
- IPsec Network Address Translation (NAT) traversal

Intrusion Prevention System (IPS)

- Protocol anomaly detection
- Stateful protocol signatures
- IPS attack pattern obfuscation
- Customer signatures creation
- Frequency of updates (daily and emergency)

VPN Tunnels

- Generic Routing Encapsulation (GRE)
- IP-in-IP
- IPsec

User Authentication and Access Control

- Third-party user authentication (RADIUS)
- RADIUS accounting
- XAUTH VPN, web-based, 802.X authentication
- Public key infrastructure (PKI) certificate requests (PKCS 12)
- Certificate authorities supported: VeriSign, Entrust, Microsoft, RSA Keon, iPlanet, (Netscape), Baltimore, DoD PKI

Address Translation

- Source NAT with Port Address Translation (PAT)
- Static NAT
- Destination NAT with PAT

IP Address Assignment

- Static
- Dynamic Host Configuration Protocol (DHCP), Point-to-Point over Ethernet (PPPoE) client
- Internal DHCP server
- DHCP relay

Traffic Management Quality of Service (QoS)

- Guaranteed bandwidth
- Maximum bandwidth
- Ingress traffic policing
- Priority bandwidth utilization
- DiffServ code point marking

Routing

- IPv4 and IPv6 support
- Static routes
- RIPv2
- OSPFv2/v3
- OSPFv3 address family support
- BGP

- IS-IS
- Source-based routing
- Policy-based routing
- Equal-cost multipath (ECMP)
- Reverse path forwarding (RPF)
- MPLS
- Layer 2 VPN (VPLS)
- Layer 3 VPN
- LDP
- RSVP
- Circuit cross-connect (CCC)
- Translational cross-connect (TCC)

Multicast

- Internet Group Management Protocol (IGMP v1, v2, and v3)
- IGMP Multicast Listener Discovery (MLD) proxy
- Protocol Independent Multicast (PIM) sparse mode (SM)
- PIM dense mode (DM)
- PIM source-specific multicast (SSM)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Source specific
- Multicast inside IPsec tunnel

Encapsulations

- Generic routing encapsulation (GRE)
- Point-to-Point Protocol (PPP)
- PPPoE
- Ethernet (media access control and tagged)

Quality of Service

- Packet classification based on IP precedence, DSCP, 802.1p
- 8 queues per logical entity
- 4 drop profiles per queue using Tail RED
- 32 queues per interface
- Weighted round-robin (WRR) scheduling
- 4 priority levels with strict order
- Packet marking by precedence, DSCP

Radio Router Protocols

- RFC 4938
- RFC 4938 – BIS (using rate information to control flows)
- UDP-based radio router protocol (ground to satellite radio)

Command-Line Interface

- Junos OS CLI

Specifications

Dimensions (W x H x D)

- 18.7 x 1.72 x 12 in
- (47.5 x 4.4 x 30.5 cm)

Weight

- 15 lbs

Weight with rack mount kit

- 21 lbs

Weight with wall mount kit

- 42 lbs

Mounting

- 19 in rack mount or wall mount

Input voltage (DC)

- -48 VDC

Input voltage (AC)

- N/A

Maximum power required

- 60 W

Input current

- 1.25 A at -48 VDC

Cooling

- Conduction cooled with no fans and no vents

Continuous operating temperature

- -40° to 71°C (-40° to 160°F)

Type test for 100 hours

- -40° to 85°C (-40° to 185°F)

Nonoperating temperature

- -50° to 100°C (-58° to 212°F)

Humidity noncondensing

- 0 to 100%

Altitude

- 4,000 meters

Regulatory Compliance

Substation compliance

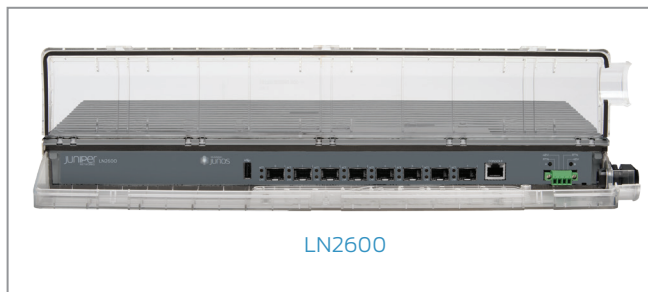
- IEEE 1613: 2009 + 1613a (2011) - Communications Networking Devices Installed in Electric Power Substations, International.
- IEC 61850-3 ed 1, 2002-01-16 - Communication networks and systems in substations, International.

Railway EMC

- EN 50121-4

Safety approvals

- CAN/CSA-C22.2 No. 60950-1 (2007)
- UL 60950-1 (2nd Ed.)
- EN 60950-1 (2006 + A11:2010)
- IEC 60950-1 (2005 + A1:2009)
- EN 60825-1 (2007)



LN2600

Immunity

- EN 50121-4:2006; Part 4 - Railway applications. Europe.
- EN 300 386 V1.5.1(2010-10)
- CISPR 24:2010
- TS 61000-6-5, ed1.0 (2001-07) - Immunity for power station and substation environments, International.

EMC certifications

- FCC Part 68 (Telecom)
- CISPR 22:2008, Class A
- FCC 47CFR , Part 15 Class A (2009) USA Radiated Emissions
- EN 55022 (2010) Class A EN 55024 (2010) (CISPR24: 2010)
KN 24 (2011-9)

ETSI

- ETSI EN 300 386 V1.6.1 (2012)
- ETSI EN 300 019: Environmental Conditions & Environmental Tests for Telecommunications Equipment
- ETSI EN 300 019-2-1 v2.1.2 (2000) - Storage, Class T1.2
- ETSI EN 300 019-2-2 v2.1.2 (1999) - Transportation, Class T2.3
- ETSI EN 300 019-2-3 v2.2.2 (2003) - Stationary Use at Weather-protected Locations, Class T3.2
- EN 300 132-2 (2011) - Environmental Engineering

Country Specific

- Canada - ICES-003 Issue 5(2012)
- Japan - VCCI V-3/2012.04 and V-4/2011.04, (Class A)
- Taiwan - BSMI Safety CNS 14336-1(99)
- Taiwan - BSMI EMC CNS 13438 and NCC C6357 (2006)
- India - TEC/EMI/TEL-001/01/FEB-09, Class A
- Australia/New-Zealand - AS/NZS CISPR22:2009
- South Korea - KN 22 (2009-12)

Customer-Specific Requirements

- GR-63-Core Issue 4 (2012) Network Equipment, Building Systems (NEBS) Physical Protection
- GR-1089-Core Issue 6 (2011) EMC and Electrical Safety for Network Telecommunications Equipment
- GR-3108-CORE Issue 3 (2009) Network Equipment in the Outside Plant (OSP), class 3
- SR-3580 NEBS Criteria Levels (Level 3)
- ETS 300753 (1997) - Acoustic noise emitted by telecommunications equipment
- ATT-TP-76200 Issue 17 (2012) Network Equipment Power, Grounding, Environmental, and Physical Design Requirements
- ATIS-0600015.03.2009 Energy Efficiency for Telecommunication Equipment: Methodology for Measurement & Reporting for Router and Ethernet Switch Products.
- ATIS-0600015.2009 Energy Efficiency for Telecommunication Equipment: Methodology for Measurement & Reporting – General Requirements.
- Verizon TPR.9305 Issue 5 (2012) Verizon NEBS Compliance: NEBS Compliance Clarification Document

- VZ.TPR.9205 Verizon NEBS Compliance: Energy Efficiency Requirements for Telecommunications Equipment.
- DT TR9 (2012) - Equipment used in Telecommunications Networks, Deutsche Telekom.
- BT GS7, Mobile Radiated Immunity E-field Requirements (2007)
- IBM C-S 2-0001-005, 2008: Electrostatic Discharge (ESD) Immunity Levels and Test Methods, IBM.
- IBM C-S 2-0001-012, 2008: Radio Frequency Electromagnetic Susceptibility (RES) Immunity Limits and Test Practice, IBM.
- IBM C-H 1-9711-005 2008-04: Packaged IBM Products, Testing for shipment, Sections 6.1 and 6.2

Performance

Maximum performance and capacity

- Firewall + routing pps (64 byte): 200 Kpps
- AES256+SHA-1/3DES+SHA-1 VPN performance: 250 Mbps
- IPsec VPN tunnels: 1,000
- IPS: 250 Mbps
- Connections per second: 9,000
- Maximum concurrent sessions: 128,000
- Maximum security policies: 4,096
- Maximum users supported: Unrestricted

Network connectivity

- Fixed I/O: 8 x 1 Gbps

Routing

- BGP instances: 20
- BGP peers: 32
- BGP routes: 64K
- OSPF instances: 20
- OSPF routes: 64K
- RIP v1 / v2 instances: 20
- RIP v2 routes: 64K
- Static routes: 64K

IPsec VPN

- Concurrent VPN tunnels: 1,000
- Tunnel interfaces: 128

Virtualization

- Maximum number of security zones: 32
- Maximum number of VLANs: 512

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

Model Number	Description
LN2600-DC48-8SFP	LN2600 Rugged Secure Router with 8 GE SFP interfaces. Includes one -48 VDC power supply (dual inputs). SFP optics sold separately. Rack and Wall mount kits sold separately.
LN-RACK-KIT	LN2600 or LN2800 19" rack mount kit.
LN-WALL-KIT	LN2600 or LN2800 wall mount kit
LN-IDP-1	1 Year Subscription for IDP Updates for LN-Series
LN-IDP-2	2 Year Subscription for IDP Updates for LN-Series
LN-IDP-3	3 Year Subscription for IDP Updates for LN-Series
LN-APPSEC-1	1 year Subscription for Application Security and IPS updates for LN-Series
LN-APPSEC-2	2 year Subscription for Application Security and IPS updates for LN-Series
LN-APPSEC-3	3 year Subscription for Application Security and IPS updates for LN-Series
LN-BGP-ADV-LTU	Advanced BGP License for Route Reflector functionality. All other BGP functionality is included in the base system JUNOS software at no additional charge.
LN-IDP-1-R	1 Year Subscription renewal for IDP Updates for LN-Series
LN-IDP-2-R	2 Year Subscription renewal for IDP Updates for LN-Series
LN-IDP-3-R	3 Year Subscription renewal for IDP Updates for LN-Series
LN-APPSEC-1-R	1 year Subscription renewal for Application Security and IPS updates for LN-Series
LN-APPSEC-2-R	2 year Subscription renewal for Application Security and IPS updates for LN-Series
LN-APPSEC-3-R	3 year Subscription renewal for Application Security and IPS updates for LN-Series
LN-SMB4-CS	One year security subscription for Enterprise - includes Kaspersky AV, Enhanced WF, Sophos AS , Appsecure and IDP on LN Series products.
LN-SMB4-CS-3	Three year security subscription for Enterprise - includes Kaspersky AV, Enhanced WF, Sophos AS , Appsecure and IDP on LN Series products.

Model Number	Description
LN-SMB4-CS-5	Five year security subscription for Enterprise - includes Kaspersky AV, Enhanced WF, Sophos AS , Appsecure and IDP on LN Series products.
LN-SMB4-CS-R	One year renewal security subscription for Enterprise - includes Kaspersky AV, Enhanced WF, Sophos AS , Appsecure and IDP on LN Series products.
LN-SMB4-CS-3-R	Three year renewal security subscription for Enterprise - includes Kaspersky AV, Enhanced WF, Sophos AS , Appsecure and IDP on LN Series products.
LN-SMB4-CS-5-R	Five year renewal security subscription for Enterprise - includes Kaspersky AV, Enhanced WF, Sophos AS , Appsecure and IDP on LN Series products.
LN-RAC-5-LTU	Dynamic VPN Service: 5 simultaneous users
LN-RAC-10-LTU	Dynamic VPN Service: 10 simultaneous users
LN-RAC-25-LTU	Dynamic VPN Service: 25 simultaneous users
LN-RAC-50-LTU	Dynamic VPN Service: 50 simultaneous users
LN-RAC-100-LTU	Dynamic VPN Service: 100 simultaneous users
SRX-SFP-1GE-T-ET	Extended Temperature Small Form Factor Pluggable 1000Base-T Gigabit Ethernet Module
SRX-SFP-1GE-SX-ET	Extended Temperature Small Form Factor Pluggable 1000Base-SX Gigabit Ethernet Optic Module
SRX-SFP-1GE-LX-ET	Extended Temperature Small Form Factor Pluggable 1000Base-LX Gigabit Ethernet Optic Module
SRX-SFP-1GE-LH-ET	Extended Temperature Small Form Factor Pluggable 1000Base-LH Gigabit Ethernet Optic Module

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

Copyright 2015 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos and QFabric are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

JUNIPER
 NETWORKS