AX411 Access Point

Use the instructions in this guide to help you install the AX411 Access Point. For details, see the *AX411 Access Point Hardware Guide* and the *JUNOS Software WLAN Configuration and Administration Guide* at http://www.juniper.net/techpubs/a072.html.

For translated documentation in Arabic, German, Spanish, French, Chinese, Korean, Russian, and Japanese, see the URL below.

للاطلاع على الوثائق المُترجمة، يُرجى زيارة عنوان URL الوارد أدناه.

翻訳された文書については、下の URL にアクセスしてください。

Übersetzte Dokumentation finden Sie unter folgender Webadresse.

번역본은 아래의 URL을 방문하세요.

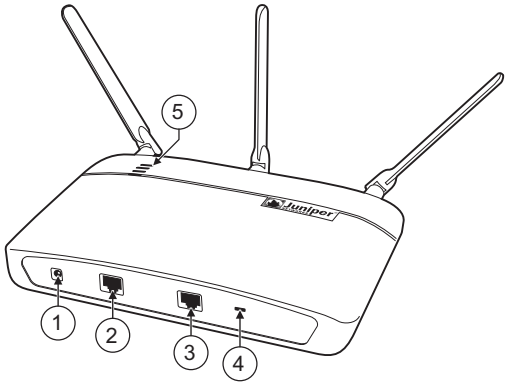
Para obtener la documentación traducida, visite el URL a continuación.

Переведенная версия документации доступна по указанному ниже адресу.

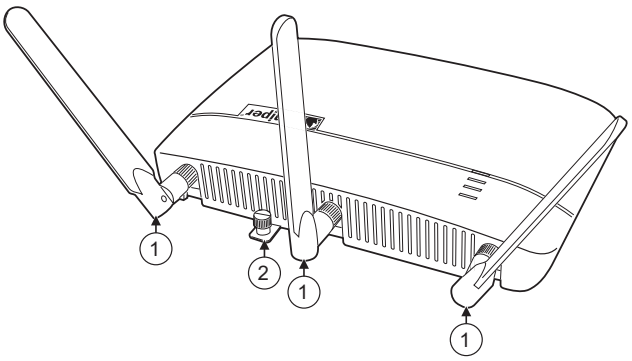
Pour de la documentation traduite, consultez l'adresse URL ci-dessous.

要获取已翻译的文档，请访问以下 URL。

http://www.juniper.net/techpubs/a073.html



AX411 Access Point Front Panel	
1. Power Connector 2. PoE Ethernet Port 3. Console Port 4. Lock Slot	5. LEDs: • Power (Green = Power OK) • Status (Green = Managed) • 5 GHz Radio (Blue = Enabled) • 2.4 GHz Radio (Green = Enabled)



AX411 Access Point Rear Panel
1. Antennas (3) 2. Mounting Bracket Locking Screw

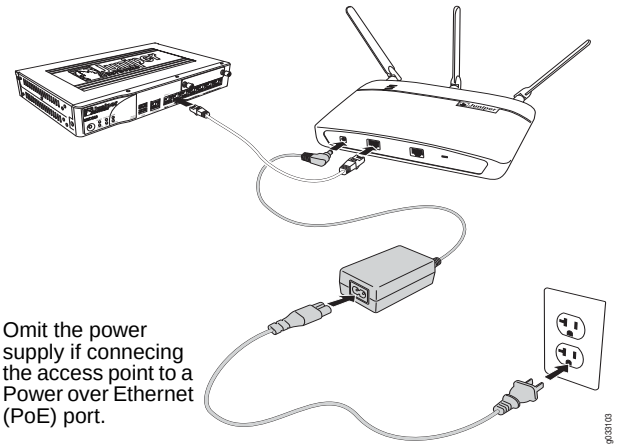
CONNECTING THE ACCESS POINT AND CONFIGURING THE SRX SERIES DEVICE

Use the instructions below to connect the AX411 Access Point to the SRX Series Services Gateway that manages it and to configure the SRX Series device.

Step 1

Install the antennas and connect the access point to an Ethernet port on the SRX Series Services Gateway. If you are not using a Power over Ethernet (PoE) port on the services gateway, also connect the device to the optional power supply.

Note: The services gateway must be running JUNOS Software Release 10.0 or later.



Omit the power supply if connecing the access point to a Power over Ethernet (PoE) port.

Step 2

Configure the services gateway to recognize the access point:

1. If you are installing more than two access points, install access point licenses on the services gateway. The services gateway supports two access points by default. To install more than two access points you must install licenses. You obtain access point licenses from your Juniper Networks reseller. Access point licenses are available in increments of 2, 4, 8, and 16 access points.

   With the CLI:

   ```
   admin@srx650-tp#request system license add
     terminal
   ```

   Paste or type the license key text and type **Ctrl+D**, then commit your changes.

   With the J-Web interface:

   Choose **Maintain > Licenses**, add a new license, paste or type the license key text, and click **OK**.

2. Configure a logical interface and an IP address for the access point port.

   With the CLI:

   ```
   set interfaces ge-0/0/2 unit 0 family inet address
     192.168.1.4
   ```

   With the J-Web interface:

   a. Choose **Configure > Interfaces**.
   b. In the Interface Name column, click the physical interface to which the access point is connected.
   c. In the Logical Interfaces area, click **Add** to add a new logical interface.
   d. In the IPv4 Addresses and Prefixes area, click **Add** to add an IPv4 address to the logical interface.
   e. In the IPv4 Address and Prefix box, type the IP address for the interface.
   f. Click **OK**.

3. If necessary, add the interface that is connected to the access point to the Trust security zone. The ge-0/0/0 interface is in the Trust zone by default; for other interfaces, you must add them to the Trust zone.

   With the CLI:

   ```
   set security zones security-zone trust interfaces
     ge-0/0/2.0
   ```

   With the J-Web interface:

   a. Choose **Configure > Security > Zones**.
   b. In the Security Zone list, click the Trust zone.
   c. In the **Interfaces out of the zone** list, click the access point interface and then click the left-pointing arrow to move it into the Trust zone.
   d. Click **OK**.

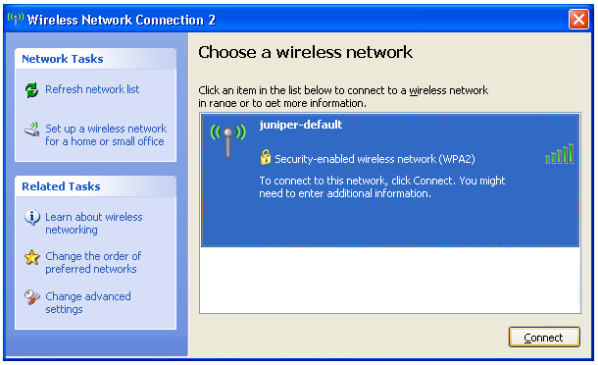
Step 3

Check functionality:

1. Check that the access point Power and Status LEDs are green. These LEDs show that the device is powered on, running properly, and being managed by the SRX Series device.
2. Check that the access point 5 GHz radio LED is blinking blue and that the 2.4 GHz radio LED is blinking green. These LEDs show that the access point radios are enabled and sending beacons.
3. Test connectivity to the WLAN.

   Use your laptop or other wireless device to scan near the AX411 Access Point for a WLAN with the following settings:

SSID	**juniper-default**
Security WPA2 Key	**juniper-wireless**
Encryption	AES



Connect to the juniper-default network. When prompted for a network key, enter **juniper-wireless**.

P/N 530-032047 Rev. 01

Juniper Networks

Security Products Safety Guide

September 2008

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Part Number: 530–014149–01, Revision 03
Published: 2009-10-21

Juniper Networks Security Products Safety Guide

Revision History
September 2008—Revision 3

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS Software has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions. Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details. For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous

agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

Part 1
Security Products Safety Overview

Chapter 1

Safety Recommendations and Warnings

This guide contains general safety recommendations and warnings about avoiding situations that could cause injury to people or devices. For specific guidelines about installing or using a device, see the hardware guide for your device.

NOTE: For translated versions of this guide, see the Documentation CD shipped with your device or the Juniper Networks Technical Documentation Web site at www.juniper.net/techpubs.

This section includes the following topics:

Definitions of Safety Warning Levels

This guide uses the following three levels of safety warnings:

NOTE: You might find this information helpful in a particular situation or might otherwise overlook it.

CAUTION: You need to observe the specified guidelines to avoid minor injury or discomfort to you or severe damage to the device.

WARNING: This symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Safety Recommendations and Warnings

Before working on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Observe these important guidelines when installing or manipulating a Juniper Networks device:

- Always disconnect all power supply connections before:
  - Removing a chassis
  - Changing a fuse
- Locate the emergency power-off switch for the area where you are working.
- Allow adequate air circulation. Do not stack devices or balance any devices or equipment over other devices or equipment. If the device is installed in a rack, the rack must be secured to the building structure. The device should be mounted at the bottom of the rack if it is the only unit in the rack.
- Look carefully for possible hazards in the work area, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Do not work alone if potentially hazardous conditions exist.
- Keep the area around the chassis clear and free from dust before, during, and after installation.
- Do not wear loose clothing or jewelry, such as rings, bracelets, or chains, which could become caught in the chassis.
- Wear safety glasses if you are working under any conditions that could be hazardous to your eyes.
- Never attempt to lift an object that is too heavy for one person to handle.
- Never install or manipulate wiring during electrical storms.
- Replace fuses only with fuses of the same type and rating.
- Do not open or remove chassis covers or sheet-metal parts unless instructions for doing so are provided in the hardware guide for this device. Such an action could cause severe electrical shock.
- Do not push or force any objects through any opening in the chassis frame. Such an action could result in electrical shock or fire.
- Avoid spilling liquid onto the chassis. Such an action could cause electrical shock or damage the chassis.
- Avoid touching uninsulated electrical wires or terminals that have not been disconnected from their power source. Such an action could cause electrical shock.
- Always ensure that all modules, power supplies, and blank panels are fully inserted and that the installation screws are fully tightened.

Safety Warnings

For your protection, and the protection of people around you, ensure that you adhere to the following set of safety warnings.

Installation

WARNING: Read the cabling instructions before you connect the device to its power source. See the hardware guide for your device.

Power Disconnection

WARNING: Before working on a device that has a switch, switch the circuit to the OFF position and disconnect the power cord to all power supplies.

For DC power supplies, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the DC circuit breaker to secure it in the OFF position.

Disconnecting Power from the Device

WARNING: Some devices have more than one power supply connection. All connections must be removed completely to shut off power from the unit.

User-Serviceable Parts

WARNING: The chassis of some devices are tamperproof. Do not open the chassis of a tamper-proof device under any circumstances. Doing so will void the warranty.

Other devices have user-serviceable parts such as fuses, memory modules, processor modules, and application modules, which require the chassis to be opened. You can replace these components when necessary. Make sure to return the components to the manufacturer for service or replacement. For more information about user-serviceable parts, see the hardware guide for your device.

Circuit Breaker—Maximum Voltage

WARNING: The device relies on the building's safety features for protection against short-circuit, over-current, and earth (grounding) fault. Ensure that the building's safety features are properly rated for the device. Depending on which type of power—AC or DC—the device uses, the phase conductor (or all current-carrying conductors) should use a fuse or breaker that has the maximum voltage specified for the device. See the hardware guide for your device.

SELV Circuit

Juniper Networks devices support Ethernet 10BaseT, 100BaseT, 1000BaseT, serial, console, and auxiliary ports, which contain safety extra-low voltage (SELV) circuits. To find out which cable to use with which interface, see the hardware guide for your device.

CAUTION: Do not connect the Ethernet 10BaseT, 100BaseT, or 1000BaseT ports to a telephone line or any Telco line (for example, T-1, T-3, or RJ-48 lines).

Lightning Activity

WARNING: Do not work on the device, or connect or disconnect the device, during lightning activity.

Lithium Battery

WARNING: Return the device to the manufacturer for battery replacement. Moreover, a tamperproof chassis should not be opened under any circumstances. Doing so will also void the warranty.

Handling the Battery

WARNING: Replacing the battery incorrectly might result in an explosion. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Chapter 2

General Site and Installation Requirements

CAUTION: For the safe installation and operation of your device, ensure that your site is properly prepared before beginning the hardware installation.

The following information will help you ensure that the site is properly prepared:

- Check the power at your site to ensure that you are receiving clean power (free of spikes and noise). Install a power conditioner if necessary.
- Choose a site that maintains an ambient temperature of 32 to 104°F (0 to 40°C). The device is intended for use in a normal office environment. For more extreme conditions, verify that temperature, humidity, and power conditions meet the specifications for each Juniper Networks device. For specifications, see the hardware guide for your device.
- The device relies on the building's safety features for protection against short-circuit, over-current, and earth (grounding) fault. Ensure that the building's safety features are properly rated for the device.
- Ensure that the device is installed in a secure location where access to the device is limited to authorized personnel.

Observe the following guidelines and warnings before and during device installation:

Onsite Precautions

NOTE: You can place the device on a desktop, on a wall or mounted in a rack. The location of the chassis and the layout of your equipment rack or wiring room are extremely important for proper system operation. Equipment placed too close together will cause inadequate ventilation, as well as render areas of the device inaccessible for system maintenance during any system malfunctions and shutdowns.

When planning your site layout and equipment locations, follow these precautions described below to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are experiencing shutdowns or unusually high errors with your existing equipment, these precautions may help you isolate the cause of the failures and prevent future problems.

- Ensure that the room in which you operate your system has adequate air circulation. Electrical equipment generates heat. Natural air temperature might not be sufficient to cool the equipment to acceptable operating temperatures without an additional ventilation system.
- Choose a site with a dry, clean, well-ventilated and air-conditioned area.

Qualified Personnel Warning

WARNING: Only trained and qualified personnel should install or replace the device.

Restricted Access Area Warning

WARNING: The device is intended for installation in restricted access areas. A restricted access area is an area to which access can be gained only by service personnel through the use of a special tool, lock and key, or other means of security, and which is controlled by the authority responsible for the location.

Installation Instructions Warning

WARNING: Read the installation instructions before you connect the device to a power source.

Rack-Mounting Requirements and Warnings

The following information will help you plan an acceptable equipment-rack configuration.

WARNING: To prevent bodily injury when mounting or servicing the device in a rack, take the following precautions to ensure that the system remains stable. The following directives help maintain your safety:

- Ensure that the equipment rack into which the device is installed is evenly and securely supported to avoid the hazardous condition that could result from uneven mechanical loading.
- If the device is installed in a rack, the rack must be secured to the building structure.
- The device should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting the device in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the device in the rack.
- Do not stack devices or balance any devices or equipment over other devices or equipment.
- Install the device in an open rack whenever possible. If you install the device in an enclosed rack, ensure that the device has adequate ventilation and that the rack allows adequate clearance for both airflow and maintenance. Ensure that the rack is not overly congested because each unit generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake or exhaust ports. If the chassis is installed on slides, check the position of the chassis when it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, excessive heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack, which can be found by experimenting with different arrangements.

Fire Safety Requirements

In the event of a fire emergency involving devices and other network equipment, the safety of people is the primary concern. Establish procedures for protecting

people in the event of a fire emergency, provide safety training, and properly provision firecontrol equipment and fire extinguishers.

In addition, establish procedures to protect your equipment in the event of a fire emergency. Juniper Networks devices should be installed in an environment suitable for electronic equipment. We recommend that fire suppression equipment be available in the event of a fire in the vicinity of the equipment, and that all local fire, safety, and electrical codes and ordinances be observed when installing and operating your equipment.

Fire Suppression and Fire Suppression Equipment

In the event of an electrical hazard or fire, first turn off power to the equipment at the source. Then use a Type C fire extinguisher to extinguish the fire. Type C fire extinguishers use noncorrosive fire retardants such as carbon dioxide (CO_2) and Halotron™ and are most effective for suppressing electrical fires. Type C fire extinguishers displace the oxygen from the point of combustion to eliminate the fire. For extinguishing fire on or around equipment that draws air from the environment for cooling, use this type of inert oxygen displacement extinguisher instead of an extinguisher that leave residues on equipment.

Do not use multipurpose Type ABC chemical fire extinguishers (dry chemical fire extinguishers) near Juniper Networks equipment. The primary ingredient in these fire extinguishers is monoammonium phosphate, which is very sticky and difficult to clean. In addition, in minute amounts of moisture, monoammonium phosphate can become highly corrosive and corrodes most metals.

Any equipment in a room in which a chemical fire extinguisher has been discharged is subject to premature failure and unreliable operation. The equipment is considered to be irreparably damaged.

NOTE: To keep warranties effective, do not use a dry chemical fire extinguisher to control a fire at or near a Juniper Networks device. If a dry chemical fire extinguisher is used, the unit is no longer eligible for coverage under a service agreement.

We recommend that you dispose of any irreparably damaged equipment in an environmentally responsible manner.

Chapter 3

Power Considerations and Electrical Safety Guidelines and Warnings

This section includes the following topics:

Power Considerations

AC and DC power supplies, and an optional redundant power supply, are available for some devices.

CAUTION: Do not overload the wiring; be careful when connecting devices to the supply circuit.

NOTE: See your hardware guide for AC and DC power specifications and cabling information and for redundant power-supply availability.

WARNING: Use only power cord sets that are certified by the local authorities to meet local regulations and building codes.

IT Power Statement

WARNING: The device is designed to work with IT power systems.

Power Cable Warning (Japanese)

WARNING:

注意

附属の電源コードセットはこの製品専用です。
他の電気機器には使用しないでください。

Translation:

Warning: The attached power cable is only for this product. Do not use the cable for another product.

Warning Statement for Norway and Sweden

WARNING: The equipment must be connected to an earthed mains socket-outlet.

Advarsel Apparatet skal kobles til en jordet stikkontakt.

varning! Apparaten skall anslutas till jordat nätuttag.

For Devices That Support AC Power

WARNING: Juniper Networks devices are designed for connection to IT power systems. A IT power system is a power distribution system with one point connected to earth through an impedance. The exposed conductive parts of the installation are connected to protective ground conductors.

Ensure that the plug-socket combination is accessible at all times, because it serves as the main disconnecting device.

Ensure that the device is connected to an AC power source equipped with a surge protection device.

For Devices That Support DC Power

WARNING: Connect DC-input power supplies only to a DC power source that complies with the safety extra-low voltage (SELV) requirements in the UL 60950-1, CSA 60950-1, EN 60950-1, and IEC 60950-1 standards.

Incorporate a freely accessible two-poled disconnect device in the fixed wiring.

Ensure that there is no power in the DC circuits before installing or removing power supplies. As a precautionary measure, you can tape the switch handle of the DC circuit breaker to secure it in the OFF position.

Use only copper conductors to connect to a DC terminal block.

When stranded wiring is required, use approved wiring terminations such as closed-loop or spade-type lugs. These terminations should be the appropriate size for the wires and should clamp both the insulation and the conductor.

Ensure that no exposed portion of the DC-input power source wire extends from the terminal block plug. An exposed wire can conduct a harmful level of electricity. If you remove the cover on the DC terminal block for any reason, make sure that you replace the cover when you are done.

DC Power Wiring Sequence Warning

WARNING: Wire the DC power supply using the appropriate lungs. When connecting the power, the proper wiring sequence is ground to ground, + RTN to + RTN, then – 48V to – 48V. While disconnecting power, the proper wiring sequence is – 48V to –48V, + RTN to + RTN, then ground to ground. Note that the ground wire should always be connected first and disconnected last.

Redundant Power Considerations

If your device includes an optional redundant power supply, connect each of the two power supplies to different input power sources. Failure to do so makes the device susceptible to total power failure in the event that one of the power supplies fails.

WARNING: If you need to disconnect the device to perform servicing, disconnect both power supplies. Otherwise, system components such as plug-in Input/Output Cards (IOCs) could be damaged.

In Case of Electrical Accident

If an electrical accident results in an injury, take the following actions in this order:

1. Use caution. Be aware of potentially hazardous conditions that could cause further injury.
2. Disconnect power from the device.
3. If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, then call for help.

General Electrical Safety Guidelines and Warnings

Observe the following guidelines when working on a device powered by electricity:

- Locate the emergency power-off switch for the room in which you are working so that if an electrical accident occurs, you can quickly turn off the power.
- Do not work alone if potentially hazardous conditions exist anywhere in your workspace.
- Never assume that power is disconnected from a circuit. Always check the circuit before starting to work.
- Carefully look for possible hazards in your work area, such as moist floors, ungrounded power extension cords, and missing safety grounds.
- Operate the device within marked electrical ratings and follow product usage instructions.
- For the device and peripheral equipment to function safely and correctly, use the cables and connectors specified for the attached peripheral equipment, and make certain they are in good condition.

Compliance Statement for Electrical Codes

Install the device in compliance with the following local, national, or international electrical codes:

- United States—National Fire Protection Association (NFPA 70), United States National Electrical Code
- Canada—Canadian Electrical Code, Part 1, CSA C22.1
- Other countries—International Electromechanical Commission (IEC) 60364, Part 1 through Part 7
- Evaluated to the IT power system

Chapter 4

Handling Devices

This section includes the following topics:

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) damage occurs when electronic cards or components are mishandled and can result in complete or intermittent failures.

Many devices are sensitive to damage from static electricity. Some components can be impaired by voltages as low as 30 V. You can easily generate potentially damaging static voltages whenever you handle plastic or foam packing material or if you move components across plastic or carpets. Observe the following guidelines to minimize the potential for electrostatic discharge damage, which can cause intermittent or complete component failures:

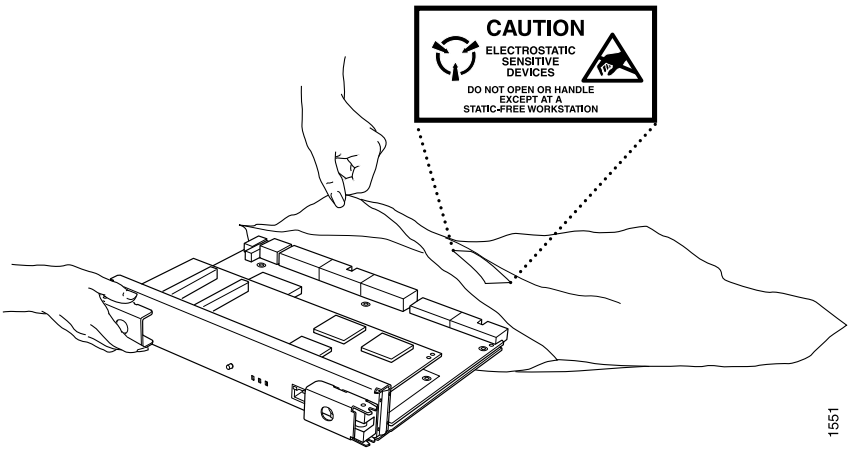
- Always use an ESD-preventive wrist strap or ankle strap when handling electronic components, and verify that it is in direct contact with your skin.

CAUTION: For safety, periodically check the resistance value of the ESD strap. The measurement should be in the range of 1 to 10 Mohms.

- When handling any component that is removed from the chassis, verify that the equipment end of your ESD strap is attached to one of the ESD points on the chassis. See the hardware guide for your device.
- Avoid contact between the component and your clothing. The wrist strap only protects the card from ESD voltages on the body; ESD voltages emitted from clothing can still damage components.

- Always handle cards by the faceplates and edges only; avoid touching the printed circuit board and connector pins.
- When removing or installing a component, always place it component-side up on an antistatic surface, in an antistatic card rack, or in an electrostatic bag (see Figure 1 on page 16). If you are returning a component, place it in an electrostatic bag before packing it.

Figure 1: Placing a Component in to an Electrostatic Bag



General Laser Safety Guidelines

Some Juniper Networks devices are equipped with fiber-optic ports, which emit radiation that may be harmful to the human eye. Be aware of the following.

Fiber-optic ports (for example, GBIC and mini-GBIC) are considered Class 1 laser or Class 1 LED ports.

When working around PICs, observe the following safety guidelines to prevent eye injury:

- Do not look into unterminated ports or at fibers that connect to unknown sources.
- Do not examine unterminated optical ports with optical instruments.
- Avoid direct exposure to the beam.

WARNING: Unterminated optical connectors can emit invisible laser radiation. The lens in the human eye focuses all the laser power on the retina, so focusing the eye directly on a laser source—even a low-power laser—could permanently damage the eye.

Class 1 Laser Product Warning

WARNING: Class 1 Laser product.

Class 1 LED Product Warning

WARNING: Class 1 LED Product.

Laser Beam Warning

WARNING: Do not stare into the laser beam or view it directly with optical instruments.

Invisible radiation might be emitted from the aperture of the port when no fiber cable is connected.

These products have been tested and found to comply with Class 1 limits of IEC 60825-1, EN 60825-1, and 21CFR1040.

Radiation from Open Port Apertures Warning

WARNING: Because invisible radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures.

Telecommunication Line Cord Warning

WARNING: To reduce the risk of fire, use only No. 26 AWG or larger UL-listed or CSA-certified telecommunication line cord.

Preventing Electromagnetic Interference

NOTE: When you run wires for any significant distance in an electromagnetic field, electromagnetic interference (EMI) can occur between the field and the signals on the wires. Note the following information:

- Bad plant wiring can result in radio frequency interference (RFI).
- Strong EMI, especially when it is caused by lightning or radio transmitters, can destroy the signal drivers and receivers in the system and can even create an electrical hazard by conducting power surges through lines and into the system.

To prevent and remedy strong EMI, consult RFI experts.

Covering Empty Slots

Ensure that all cards, faceplates, and covers are in place. Blank faceplates and cover panels are used for the following reasons:

- Preventing exposure to hazardous voltages and currents inside the chassis
- Helping contain electromagnetic interference (EMI) that might disrupt other equipment
- Directing the flow of cooling air through the chassis

Jewelry Removal

WARNING: Before working on equipment that is connected to power lines, remove jewelry, including rings, necklaces, and watches. Metal objects heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Operating Temperature Warning

WARNING: To prevent the device from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 104°F (40°C). To prevent airflow restriction, allow at least 6 in. (15.2 cm) of clearance around the ventilation openings.

Chapter 5

Agency Approvals and Compliance Statements

This section includes the following topics:

Agency Approvals

The security device complies with the following standards (for specific version of the standard relevance to the product, please refer to individual product manual) :

- Safety
  - CSA 60950-1 Safety of Information Technology Equipment
  - UL 60950-1 Safety of Information Technology Equipment
  - EN 60950-1 Safety of Information Technology Equipment
  - IEC 60950-1 Safety of Information Technology Equipment (with country deviations)
  - EN 60825-1 Safety of Laser Products - Part 1: Equipment Classification
- EMC
  - EN 300 386 Telecom Network Equipment - EMC requirements
- EMI
  - FCC Part 15 USA Radiated Emissions
  - EN 55022 European Radiated Emissions
  - VCCI Japanese Radiated Emissions
- Immunity
  - EN 55024 Information Technology Equipment Immunity Characteristics
  - EN-61000-3-2 Power Line Harmonics
  - EN-61000-3-3 Power Line Voltage Fluctuations
  - EN-61000-4-2 Electrostatic Discharge

- EN-61000-4-3 Radiated Immunity
- EN-61000-4-4 Electrical Fast Transients
- EN-61000-4-5 Surge
- EN-61000-4-6 Immunity to Conducted Disturbances
- EN-61000-4-11 (2004) Voltage Dips and Sags

Compliance Statements

Industry Canada Statement

The following is applicable to devices with wireless interfaces:

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 5 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding.

Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

Federal Communications Commission Interference Statement

The following is applicable to devices with wireless interfaces:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Taiwan DGT

The following is applicable to devices with wireless interfaces:

(1) 經審驗合格之射頻電信終端設備，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

(2) 射頻電信終端設備之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。所謂合法通信，係指依電信法規定作業之無線電信。

(3) 輸入、製造射頻電信終端設備之公司、商號或其使用者違反本?法規定，擅自使用或變更無線電頻率、電功率者，除依電信法規定處罰外，電信總局並得撤銷其審驗合格證明。

VCCI Compliance

The following VCCI compliance information applies to security products that meet VCCI Class A or Class B limits. See the specifications section in the hardware guide for your device to determine whether the product meets Class A or Class B limits.

クラスＡ情報技術装置
この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準
に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波
妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ず
るよう要求されることがあります。

Translation:

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

クラスＢ情報技術装置
この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準
に基づくクラスＢ情報技術装置です。この装置は，家庭環境で使用すること
を目的としていますが，この装置がラジオやテレビジョン受信機に近接して
使用されると，受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

Translation:

This is a Class B product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this product is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

Wireless Connections for Products with Wireless Interfaces

WARNING: In countries other than the United States or Japan, you must set the correct country code with the set wlan country-code command to avoid violating local radio spectrum laws. This command sets the selectable channel range and transmit power level so that a WLAN connection can be established. For more information about country codes, see the hardware guide for your device.

Product Reclamation and Recycling Program

Juniper Networks is committed to environmentally responsible behavior. As part of this commitment, we work to comply with environmental standards such as the European Union's *Waste Electrical and Electronic Equipment* (WEEE) Directive and *Restriction of Hazardous Substances* (RoHS) Directive.

These directives and other similar regulations from countries outside the European Union regulate electronic waste management and the reduction or elimination of specific hazardous materials in electronic products. The WEEE Directive requires electrical and electronics manufacturers to provide mechanisms for the recycling and reuse of their products. The RoHS Directive restricts the use of certain substances that are commonly found in electronic products today. Restricted substances include heavy metals, including lead, and poly-brominated materials. The RoHS Directive, with some exemptions, applies to all electrical and electronic equipment.

In accordance with Article 11(2) of Directive 2002/96/EC (WEEE), products put on the market after 13 August 2005 are marked with the following symbol or include it in their product documentation: a cross-out wheeled waste bin with a bar beneath.

Juniper Networks provides recycling support for our equipment worldwide to comply with the WEEE Directive. For recycling information, send e-mail to recycling@juniper.net indicating the type of Juniper Networks equipment that you wish to dispose of and the country where it is currently located, or contact your Juniper Networks account representative.

Products returned through our reclamation process are recycled, recovered, or disposed of in a responsible manner. Our packaging is designed to be recycled and should be handled in accordance with your local recycling policies.

Compliance Statement for Environmental Requirements

This section describes the Compliance Statements for Environmental Requirements:

Lithium Battery

Batteries in this product are not based on mercury, lead, or cadmium substances. The batteries used in this product are in compliance with EU Directives 91/157/EEC, 93/86/EEC, and 98/101/EEC. The product documentation includes instructional information about the proper method of reclamation and recycling.

Compliance Statements for Acoustic Noise (Germany)

Maschinenlärminformations-Verordnung - 3. GPSGV, der höchste Schalldruckpegel beträgt 70_dB(A)oder weniger gemäss EN ISO 7779.

Translation:

The maximum emitted sound pressure level is 70_dB(A) or less per EN ISO 7779.

Federal Communications Commission Interference Statement

Country Code Statement
For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

Industry Canada Statement

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numerique de la classe B est conforme a la norme NMB-003 du Canada.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology.

The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.

The maximum antenna gain permitted (for devices in the band 5725-5825 MHz) to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

IMPORTANT NOTE:
IC Radiation Exposure Statement:
This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Part 2
Index

Index