

AX411 Access Point Release Notes

May 2010
Revision 03

These release notes accompany the release of the Juniper Networks AX411 Access Point. They describe the access point and also describe known and resolved issues with the hardware and accompanying software and documentation.

You can also find these release notes on the Juniper Networks Technical Publications webpage at <http://www.juniper.net/techpubs/>.

Contents

Hardware Features—AX411 Access Point	2
General Notes	2
Resolved Issues	3
Outstanding Issues for the AX411 Access Point	3
Junos Documentation and Release Notes	6
Requesting Technical Support	6
Self-Help Online Tools and Resources	6
Opening a Case with JTAC	7
Revision History	7

Hardware Features—AX411 Access Point

The AX411 Access Point provides network access for wireless clients such as laptop or desktop computers, personal digital assistants (PDAs), and any other device equipped with a Wi-Fi adapter. The AX411 Access Point supports the new IEEE 802.11n wireless networking standard with backward compatibility for IEEE 802.11a/b/g standards.

The AX411 Access Point is managed by an SRX210, SRX240, or SRX650 Services Gateway. You manage and configure access points from the SRX Series device through the Junos operating system (JUNOS OS) command-line interface (CLI), J-Web interface, and Network and Security Manager (NSM).

To deploy a wireless network with AX411 Access Points, you install one or more access points throughout your site and connect them to Ethernet ports on the services gateway. You can provide power to the access points using Power over Ethernet (PoE) by connecting them to SRX210, SRX240, or SRX650 Services Gateway ports that have PoE capability. You can also power the access points using either optional external power supplies or PoE adapters.

You can connect and use up to two AX411 Access Points to the SRX210, SRX240, and SRX650 Services Gateways without obtaining access point licenses. To connect and use additional access points, you must install one or more licenses on the services gateway. Each of these licenses specifies the number of access points that can be configured and managed in addition to the two that are automatically supported on the device:

- 2-access point license
- 4-access point license
- 8-access point license
- 14-access point license

You can install multiple licenses to increase the number of access points supported on the SRX Series device.

To configure the AX411 Access Point, use the `[edit wlan]` hierarchy.

[Junos OS WLAN Configuration and Administration Guide]

General Notes

The following items describe expected behaviors for the AX411 Access Point:

- When using WEP/TKIP security in 802.11n mode, performance is reduced. This is due to aggregation being disabled in these security modes.
- Multicast traffic has limited performance compared to unicast in 802.11 networks, mainly due to the lack of ACK packets in the 802.11 protocol for multicast packets.
- Voice frames are not subject to 802.11n frame aggregation. This allows for low latency of each voice frame.

- When in 802.11n mode, “No Ack” is not supported.
- Disabling 802.11d prevents the country code from being broadcast in the beacons. However, this only applies to radios configured to operate in the 802.11g (2.4 GHz) band. For radios operating in the 802.11a (5 GHz) band, the access point software configures support for 802.11h. When 802.11h is supported, the country code information is broadcast in the beacons.

Resolved Issues

The following items describe the resolved issues for the AX411 Access Point. Where applicable, the software and firmware versions in which the issue is resolved are listed. For information on upgrading access point firmware, see the section “Upgrading Access Point Software (J-Web Configure)” in the *Junos OS WLAN Configuration and Administration Guide*.

- For access points running firmware version 10.1.3.7, the access point sometimes does not allow wireless clients to reconnect to the network. The client would connect with the network through an SSID on the access point, receive an IP address through DHCP, and then later disconnect. When the client returned after a period of about 24 hours, the access point would not issue the client an IP address with DHCP, and the client could not connect with the network. This issue is resolved in access point firmware version 10.1.3.9. [PR/300708]
- For access points running firmware version 10.1.3.7, it is possible to create an access point cluster containing access points with different band plan settings, for example FCC and ETSI. However, in such a cluster the access points change their country-specific settings unpredictably. Access point firmware version 10.1.3.9 resolves this issue by requiring that all access points in a cluster have the same band plan. An access point with a different band plan setting would not be allowed into the cluster.

Outstanding Issues for the AX411 Access Point

The following items describe the outstanding issues for the AX411 Access Point:

- On SRX210, SRX240, and SRX650 devices, when you commit changes to the WLAN hierarchy in the command-line interface (CLI) or apply changes on the Wireless LAN tab of the J-Web interface, it might take up to several minutes before the new settings are reflected on the access point. The actual delay depends on the number of access points connected and the number of virtual access points (VAPs) configured on the access points. [PR/450230]
- On SRX210, SRX240, and SRX650 devices, when you use the CLI to commit changes to WLAN settings, the services gateway might not respond immediately to the queries while it delivers the configuration to the access point. This might result in the following error message in response to **show** commands:

```
the wireless-lan-service subsystem is not responding to management requests
```

The device responds correctly after it finishes delivering the configuration to the access point. This process takes between 5 to 50 seconds, depending on the complexity of the access point configuration changes. [PR/460736]

- On SRX210, SRX240, and SRX650 devices, when more than one AX411 Access Point is connected, both the J-Web and CLI interfaces show incorrect license usage information. The Licenses Used column correctly shows 0 if no access points are connected. However, if any access points are connected, this column always shows 1 even if two or more access points are connected. [PR/464268]
- On SRX Series devices configured for Layer 3 mode, when the DHCP router is configured outside the DHCP pool, disconnecting one of the access points can cause continuous rebooting of the other access points. The workaround for this issue is to reconfigure DHCP so that the DHCP router is within the DHCP pool, as shown in the following configuration:

```
root@silver# show system services
dhcp {
  pool 10.1.1.1/24 {
    router {
      10.1.1.1;
    }
  }
}
```

[PR/464296]

- On SRX210 devices with the default Power over Ethernet (PoE) configuration, a fourth access point connected to the services gateway does not boot. The workaround for this issue is to configure all PoE ports for a maximum power of 12.4 watts using the following command:

```
root@silver# set poe interface all maximum-power 12.4
```

[PR/465307]

- When you are configuring a VAP with security that requires RADIUS authentication and the RADIUS server is not specified for the VAP, attempting to commit the configuration results in the following error message:

```
Missing mandatory statement: 'radius'
```

The workaround for this issue is to specify the RADIUS server in the VAP configuration. [PR/482040]

- Depending on the country code setting, the AX411 Access Point supports different channel and bandwidth settings per radio. In the current software there is no restriction to avoid an incorrect setting. If the radio is set incorrectly, it might behave erratically or might not function at all. Use the procedures described in the section "Setting the AX411 Access Point Country-Specific Settings" in the *AX411 Access Point Hardware Guide* to apply settings that comply with regulations for radio frequency usage in your country. [PR/498374]
- The access point prioritizes data traffic over management traffic.

- When many VAPs are enabled (with the radios on) and/or the DHCP client needs to be restarted, the Web response times can fluctuate. Occasionally the browser might incompletely load a page and might not accept form submissions. This issue can be resolved by clearing the browser cache and reloading the page.
- As additional VAPs are enabled, performance is impacted because of the additional control traffic.
- With a large number of VLANs and clients, network users might experience client disassociations. The workaround is to increase the Group Key Timeout setting or to set it to zero.
- The WPA2-AES/PSK fragmentation is 16 bytes larger than the configured threshold. The IEEE802.11-2007 standard allows +8 bytes.
- When the access point is highly loaded (high data traffic volume, maximum number of VAPs, and maximum number of clients), a decrease in performance can result. This can include high management response times, slow data management retrieval, and generally slow access point operation.
- The access point does not always randomize UDP source port numbers.
- When the country code is set to IE, the power levels sent in the beacons are incorrect.
- When the access point is heavily loaded with traffic, the J-Web interface on the services gateway that manages the access point becomes very slow.
- The IEEE802.1X broadcast key refresh also sends the EAPOL frame tagged 'session' key.
- The beacon interval might vary by up to +/-5 milliseconds from the expected 100 milliseconds.

Junos Documentation and Release Notes

For a list of related JunosJunos documentation, see <http://www.juniper.net/techpubs/software/junos/> .

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at <http://www.juniper.net/support/requesting-support.html>

Revision History

29 October 2009—Revision 01 Initial Release

21 January 2010—Revision 02 Add procedures and tables for country-specific settings

21 May 2010—Revision 03 Remove procedures that are incorporated in AX411 Access Point Hardware Guide, add Resolved Issues section

Copyright © 2010, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.