

JumpStart for Wireless™ Open Source Test Plan

*Document Version 1.0
Date Last Updated 06/23/05*

This document and the specifications contained herein are confidential and proprietary. They are the property of Atheros Communications, Inc. This document and its contents may not be distributed without the written permission of Atheros Communications, Inc.



Document Review/Modification History

Name	Revision	Date	Comment
	1.0	06/23/05	Initial Open Source Release



Table of Contents

1	Introduction.....	4
2	Approach.....	4
3	Resource Requirements	4
4	Features to be Tested	4
5	Test Details	5
5.1	AP and STA Initial Pairing	5
5.2	Incremental Addition of STA	5
5.3	More than one STA configuring JSW AP	6
5.4	Cycle through list of P1 APs.....	6
5.5	No JSW AP available.....	7
5.6	Invalid Confirmation Click.....	7
5.7	Invalid Password for Incremental Addition of STA.....	7
5.8	Timeout in LED Confirmation.....	8
5.9	Timeout in Password Collection.....	8
5.10	JS with client that supports WPAv1 only	9
5.11	JS with AP WPAv1 only.....	9
5.12	JS Password Change	9
5.13	Exposing PMK.....	10



1 Introduction

- The JumpStart for Wireless™ suite by Atheros Communications allows autoconfiguration of wireless devices and performs its tasks in a secure way, utilizing industry-standard and well-analyzed secure algorithms. JumpStart for Wireless™ requires a minimum of information to be garnered from the user and requires a minimum of input clicks.

2 Approach

- A direct and complete black-box testing of all available code paths.
- Negative testing to prove compatibility with extant interfaces.

3 Resource Requirements

These tests require APs with JumpStart for Wireless™ capabilities and a JumpStart client. The client as described is a Windows laptop PC with an NDIS 5.1 driver installed and the JumpStart Windows application. The same concept can be applied, with small procedural changes, for a new device based on the JumpStart Linux Client code.

4 Features to be Tested

- Protocol 1: Initial configuration of AP and client
- Protocol 2: Incremental addition of clients
- Legacy integration support (expose the PMK so legacy devices can use it).



5 Test Details

5.1 AP and STA Initial Pairing

Purpose: Verify the proper functioning of JumpStart ‘AP and STA initial Pairing’.

Reference: None

Description: Verify that security association between the AP and STA.

Test Setup: Use a laptop computer with a clean installation of the OS and a compatible WLAN PC card inserted and AP with JumpStart enabled and configured for protocol 1.

Test Procedures:

- 1- Run setup.exe from the install CD.
- 2- Click ‘Yes’ to JumpStart your network.
- 3- Start the JumpStart for Wireless.
- 4- Choose ‘Create a new wireless network’ option and click ‘Next’.
- 5- Confirm the LED state.
- 6- Enter password and confirm password and click ‘Next’.
- 7- Click ‘Finish’.

Expected Results:

- JumpStart complete message is “Jumpstart has enabled your secure wireless network”.
- Device status of the client adapter is, “This device is working properly.”
- The ACU runs on reboot and connected to the JumpStart AP.
- Link Status of the ACU shows ‘Authenticated’.
- Data Encryption type shows TKIP or AES.
- Wireless ping passes between the AP and the client.
- Mcast and FTP traffic passes.

5.2 Incremental Addition of STA

Purpose: Verify the incremental addition of AP to the STA.

Reference: None

Description: Verify that AP, which has been previously affinitized using protocol, can readily accept the new STA in the network provided the new STA knows the network password.

Test Setup: Use a laptop computer with a clean installation of the OS and a compatible WLAN PC card inserted and AP with JumpStart enabled and configured for protocol 2.

Test Procedures:

- 1- Run setup.exe from the install CD.
- 2- Click ‘Yes’ to JumpStart your network.
- 3- Start the JumpStart for Wireless.
- 4- Choose ‘Connect to an existing wireless network’ option and click ‘Next’.
- 5- Enter password and click ‘Next’.
- 6- Click ‘Finish’.

Expected Results:

- JumpStart complete message is “Jumpstart has enabled your secure wireless network”.



- The ACU runs and connected to the JumpStart AP.
- Link Status of the ACU shows 'Authenticated'
- Data Encryption type shows TKIP or AES.
- Wireless ping passes between the AP and the client.
- Mcast and FTP traffic passes.

5.3 More than one STA configuring JSW AP

Purpose: Verify JumpStart AP configuration with more than one STA at the same time.

Reference: None

Description: Verify that AP should not crash if more than one STA is attempting to configure.

Test Setup: Use two laptop computers with a clean installation of the OS and a compatible WLAN PC card inserted and AP with JumpStart enabled and configured for protocol 1.

Test Procedures:

- 1- Run setup.exe from the install CD in both the STA same time
- 2- Click 'Yes' to JumpStart your network.
- 3- Start the JumpStart for Wireless.
- 4- Choose 'Create a new wireless network' option and click 'Next'.

Expected Results:

- Only one STA is allowed to configure the AP.
- The other STA given an error message that 'Failed to associate with any JumpStart AP.'

5.4 Cycle through list of P1 APs

Purpose: Verify JumpStart STA can discover and connect to multiple APs. This connection should be done on response to a user input.

Reference: None

Description: Verify STA is able to negotiate Diffie Hellman with multiple APs while running Protocol 1.

Test Setup: Set up one laptop with JumpStart CD. 2 APs with JumpStart preinstalled and configured for Protocol 1.

Test Procedures:

- 1- Run setup.exe from the install CD.
- 2- Click 'Yes' to JumpStart your network.
- 3- Start the JumpStart for Wireless.
- 4- Choose 'Create a new wireless network' option and click 'Next'.
- 5- See that the client displays the LED confirmation screen for some AP. Verify the LED is in the success state for one of the 2 APs in the testbed.
- 6- Indicate the STA should search for the other AP by pressing 'No' in the panel.
- 7- Client should search and display the LED confirmation screen again, but now the LED on the opposite AP should be in the success state.
- 8- Repeat steps 5-7 a total of 2 times.

Expected Results:



- Client visits each AP running Protocol 1.
- It does not matter which AP is visited first, but they must all be visited.

5.5 No JSW AP available

Purpose: Verify JumpStart configuration with no JumpStart enabled AP available.

Reference: None

Description: Verify that JumpStart should notify if there is no JumpStart AP available to configure.

Test Setup: Use two laptop computers with a clean installation of the OS and a compatible WLAN PC card inserted and no AP with JumpStart enabled.

Test Procedures:

- 1- Run setup.exe from the install CD in both the STA same time
- 2- Click 'Yes' to JumpStart your network.
- 3- Start the JumpStart for Wireless.

Expected Results:

- The STA given an error message that 'Failed to associate with any JumpStart AP.'

5.6 Invalid Confirmation Click

Purpose: Verify JumpStart configuration with invalid confirmation.

Reference: None

Description: Verify that JS should not crash or hang if invalid confirmations are made.

Test Setup: Use two laptop computers with a clean installation of the OS and a compatible WLAN PC card inserted and AP with JumpStart enabled and configured for protocol 1.

Test Procedures:

- 1- Run setup.exe from the install CD in both the STA same time
- 2- Click 'Yes' to JumpStart your network.
- 3- Start the JumpStart for Wireless.
- 4- Choose 'Create a new wireless network' option and click 'Next'.
- 5- Give an invalid Confirmation to the LED state.

Expected Results:

- The STA given an error message that 'Failed to associate with any JumpStart AP.'
- JS should not crash or hang.

5.7 Invalid Password for Incremental Addition of STA

Purpose: Verify Incremental addition with invalid network password.

Reference: None

Description: Verify that STA should not allowed to connect to the AP and if the password is invalid.

Test Setup: Use two laptop computers with a clean installation of the OS and a compatible WLAN PC card inserted and AP with JumpStart enabled and configured for protocol 2.



Test Procedures:

- 1- Run setup.exe from the install CD in both the STA same time
- 2- Click 'Yes' to JumpStart your network.
- 3- Start the JumpStart for Wireless.
- 4- Choose 'Connect to the existing wireless network' option and click 'Next'.
- 5- Give an invalid password.

Expected Results:

- The STA given an error message that 'Failed to associate with any JumpStart AP.'
- JS should not crash or hang.

5.8 Timeout in LED Confirmation

Purpose: Verify the time out in LED confirmation screen during STA and AP initial Pairing.

Reference: None

Description: Verify that JS and AP should not crash or hang when timeout exercise in the various stages of STA and AP initial pairing.

Test Setup: Use two laptop computers with a clean installation of the OS and a compatible WLAN PC card inserted and AP with JumpStart enabled and configured for protocol 1.

Test Procedures:

- 1- Run setup.exe from the install CD in both the STA same time
- 2- Click 'Yes' to JumpStart your network.
- 3- Start the JumpStart for Wireless.
- 4- Choose 'Connect to the existing wireless network' option and click 'Next'.
- 5- Give timeout at 'Confirm LED state' (Do not click either 'Yes' or 'No' for 5 min).

Expected Results:

- The STA given an error message that 'Confirmation time out has occurred'
- Able to restart the JS protocol operation.

5.9 Timeout in Password Collection

Purpose: Verify the time out in Password Collection screen during STA and AP initial Pairing.

Reference: None

Description: Verify that JS and AP should not crash or hang when timeout exercise in the various stages of STA and AP initial pairing.

Test Setup: Use two laptop computers with a clean installation of the OS and a compatible WLAN PC card inserted and AP with JumpStart enabled and configured for protocol 1.

Test Procedures:

- 6- Run setup.exe from the install CD in both the STA same time
- 7- Click 'Yes' to JumpStart your network.
- 8- Start the JumpStart for Wireless.
- 9- Choose 'Connect to the existing wireless network' option and click 'Next'.
- 10- Confirm 'LED' state.



11- Give timeout at 'Enter Password' (for 5 min).

Expected Results:

- The STA given an error message that 'Password time out has occurred'
- Able to restart the JS protocol operation.

5.10 JS with client that supports WPAv1 only

Purpose: Verify the JS operation with WPA only supported driver.

Reference: None

Description: Verify that JS should work with WPAv1 and select correct cipher only supported driver even if AP support both the versions.

Test Setup: Use two laptop computers with a clean installation of the OS and a compatible WLAN PC card inserted and AP has not yet configured with JumpStart enabled.

Test Procedures:

- 1- Replace the driver with 3.1 (WPA1 only supported) driver.
- 2- Run the JumpStart for Wireless.

Expected Results:

- Both AP and STA configured successfully.
- Appropriate cipher selection appears.
- Ping passes successfully.

5.11 JS with AP WPAv1 only

Purpose: Verify the JS operation with WPA only supported AP.

Reference: None

Description: Verify that JS should work with WPA1 supported AP and select correct cipher on the AP and STA.

Test Setup: Use two laptop computers with a clean installation of the OS and a compatible WLAN PC card inserted and AP has not yet configured with JumpStart enabled.

Test Procedures:

- 1- Load AP with JS WPA1 only supported (some private build)
- 2- Run the JumpStart for Wireless.

Expected Results:

- Both AP and STA configured successfully.
- Appropriate cipher selection appears.
- Ping passes successfully.

5.12 JS Password Change

Purpose: Verify the JS operation after changing the JS P2 password.

Reference: None

Description: Verify that incremental addition of STA should work with new password after changing the JS P2 password in the AP.



Test Setup: Use two laptop computers with a clean installation of the OS and a compatible WLAN PC card inserted and AP has not yet configured with JumpStart enabled.

Test Procedures:

- 1- Run JS P1.
- 2- Login to the AP.
- 3- Change the JS P2 password.
- 4- Run JS P2 with the changed password.

Expected Results:

- Incremental addition of STA successful.
- Both AP and STA configured successfully.
- Appropriate cipher selection appears.
- Ping passes successfully.

5.13 Exposing PMK

Purpose: Verify the JS operation with the exposed PMK.

Reference: None

Description: Verify that user should able to add the STA to the AP with the exposed PMK with out running JS P2.

Test Setup: Use two laptop computers with a clean installation of the OS and a compatible WLAN PC card inserted and AP has not yet configured with JumpStart enabled.

Test Procedures:

- 1- Run JS P1.
- 2- Login to the AP.
- 3- Get the PMK by Get JSP2PhassPhrase.
- 4- Create a profile with that pass phrase.
- 5- Activate the profile.

Expected Results:

- Incremental addition of STA successful.
- Ping passes successfully.