# Converting Cisco IOS APs to LWAPP

## AirWave Best Practices Guide

## Overview

Many Cisco customers are now considering whether to convert the software on some or all of their existing 'autonomous' IOS-based Cisco Aironet access points to LWAPP. The AirWave Wireless Management Suite™ is a flexible, multi-architecture software solution that allows IT to manage Cisco autonomous APs, 'thin' LWAPP access points, and Airespace controllers from the same console.

In deciding whether to convert existing APs, you need to consider several factors:

- Does your organization have budget to complete the conversion to a 'centralized architecture with Airespace controllers (once converted to LWAPP, the access points cannot function without a centralized controller)?
- Does your network architecture permit wireless traffic to be centralized or do you need autonomous APs in certain environments?
- Do your wireless applications require fast roaming and other functionality provided via a centralized architecture or are your existing autonomous access points providing the capabilities you require?
- Are all your existing autonomous APs capable of being upgraded via a software conversion? If not, will you replace the hardware or continue to operate the remaining 'thick' APs?
- Is completing a software update to your access points an acceptable risk for your organization in all locations?

If you have questions or concerns about converting your autonomous Cisco access points, you may contact Aruba Support/

The remainder of this Best Practices Guide is intended to help organizations who have already decided to convert some or all of their autonomous IOS APs to LWAPP make the transition as seamlessly as possible with the AirWave Wireless Management Suite.

## Conversion Process

The entire process for converting Cisco IOS APs to LWAPP includes four steps:

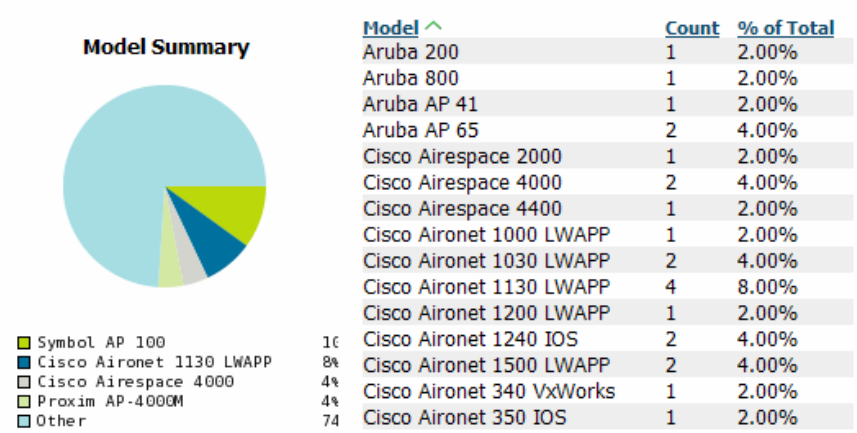


### Step One: Inventory Your Existing WLAN Infrastructure

The first step in converting your autonomous access points to LWAPP is to ensure that you have an accurate inventory of your existing infrastructure.

1. Determine whether any of your IOS devices cannot be converted to LWAPP. The following image shows sample output for the Model Summary report. This report can assist in determining your inventory.

**Figure 1** *Model Summary Report*




| Model | Count | % of Total |
|---|---|---|
| Aruba 200 | 1 | 2.00% |
| Aruba 800 | 1 | 2.00% |
| Aruba AP 41 | 1 | 2.00% |
| Aruba AP 65 | 2 | 4.00% |
| Cisco Airespace 2000 | 1 | 2.00% |
| Cisco Airespace 4000 | 2 | 4.00% |
| Cisco Airespace 4400 | 1 | 2.00% |
| Cisco Aironet 1000 LWAPP | 1 | 2.00% |
| Cisco Aironet 1030 LWAPP | 2 | 4.00% |
| Cisco Aironet 1130 LWAPP | 4 | 8.00% |
| Cisco Aironet 1200 LWAPP | 1 | 2.00% |
| Cisco Aironet 1240 IOS | 2 | 4.00% |
| Cisco Aironet 1500 LWAPP | 2 | 4.00% |
| Cisco Aironet 340 VxWorks | 1 | 2.00% |
| Cisco Aironet 350 IOS | 1 | 2.00% |

Third-party (non-Cisco) access points cannot be converted to LWAPP. In addition, many existing Cisco Aironet access points may not be convertible. At present, the following IOS devices DO NOT support LWAPP conversion:

- Aironet APs with 802.11b radios (350, 1200, and 1100)
- Aironet 1200 Series Access Points that contain first generation 802.11a radios
- Aironet 1100 Series Access Points that contain first generation 802.11g radios
- Aironet 1300 Series Access Points operating in Bridge Mode

The following IOS devices DO support LWAPP conversion

- Aironet 1240AG Series Access Points
- Aironet 1230AG Series Access Points
- Aironet 1200 Series Access Points containing the second generation802.11g radios (MP21G and MP31G) and second-generation 802.11a radios (RM21A and RM22A)
- Aironet 1130 AG Series Access Points
- Aironet 1100 Series Access Points that contain 802.11g
- Aironet 1300 Series Access Points operating in AP mode

Check the Cisco web site at www.cisco.com for any updates on conversion capabilities.

The AirWave Management Platform's Inventory Report provides a summary of your existing WLAN infrastructure, by vendor and model. You can use this list to identify and further investigate those devices on your network that might not be convertible. You can export the Inventory Report's detailed device-by-device summary to Excel or similar programs to generate a list of equipment to be replaced (or that you will continue to manage as autonomous APs via AMP).

**Figure 2** *Hardware Replacement List created by exporting Inventory Report data*

| Device Name | MFG/Model | FW Version | IP | LAN MAC | Location | Contact | Replacement | Cost |
|---|---|---|---|---|---|---|---|---|
| EU-Sale-AP2 | Cisco Aironet 340 VxWorks | 12.04 | 10.210.1.2 | 00:40:96:35:2A:86 | Sales | Bill Fold | AIR-LAP1242AG-N-K9 | $615.00 |
| Cisco350-1 | Cisco Aironet 350 IOS | 12.3(2)JA2 | 10.200.0.19 | 00:40:96:5B:1D:E7 | Accounting | James Wood | AIR-LAP1242AG-N-K9 | $615.00 |
| Cisco1200 | Cisco Aironet 1200 IOS | 12.3(2)JA2 | 10.200.0.18 | 00:40:96:5B:2E:1A | Distributioin | John Wayne | AIR-LAP1242AG-N-K9 | $615.00 |
| | | | | | | | Total: | $1,845.00 |

2. Verify that all controllers will support APs converted from IOS to LWAPP.

   Some controllers may not support converted APs. Before beginning the conversion process, you should use AMP's Inventory Report to identify which controllers are on your network and verify that they will all support converted APs.

   At present, the following IOS devices DO NOT support LWAPP-converted APs:

   - 3500 Series Wireless LAN Controllers
   - 4000 Series Wireless LAN Controllers
   - 4100 Series Wireless LAN Controllers

At present, the following IOS devices DO support LWAPP-converted APs:

- 2000 series controllers
- 4400 series controllers
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Controller Network Modules within Cisco 28/37/38xx Series Integrated Services Routers
- Catalyst 3750G Integrated Wireless LAN Controller Switches

Check the Cisco web site at www.cisco.com for any updates on conversion capabilities.

## Step Two: Prepare Devices for Conversion

1. Update all firmware to the recommended versions.

   To increase the speed and reliability of the conversion process, you should ensure that all access points and controllers are running the recommended software releases prior to running the conversion tool:

   - Minimum Controller Software: Version 3.1
   - Minimum Device Software: 12.3(7)JA

   AMP's firmware management service can upgrade your existing access points and controllers to the recommended software releases prior to running the conversion tool. AMP provides:

   - Batch parallel upgrades to increase the speed of firmware distribution
   - Scheduling to enable upgrades to occur during off-hours to decrease WLAN downtime
   - Configuration for local/remote upgrade servers to provide optimal flexibility for locations with slow up-link capability
   - Alerts when firmware upgrades fail to ensure limited downtime.

2. Ensure all device settings comply with configuration policies following the firmware upgrade AMP provides a two-phase validation process to ensure that all device configuration settings remain in compliance with your policies following the firmware upgrade (some firmware upgrades may cause certain OID resets, like returning the RF channel to a default setting of "1"):

   - **Phase One:** Fetch and store all device configuration settings prior to firmware upgrade
   - **Phase Two:** Fetch and compare post-upgrade settings to the pre-upgrade settings

   If any mismatches are discovered after the firmware upgrade, AMP can automatically re-configure the device to bring its configuration back into compliance.

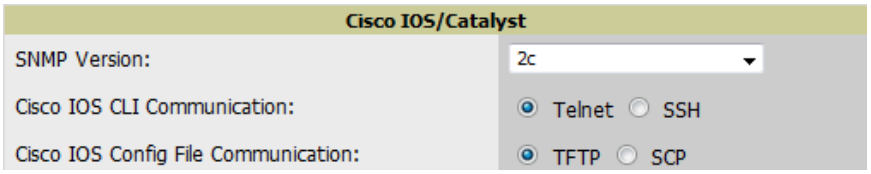
Because AMP can configure both IOS autonomous APs and LWAPP devices, it can ensure that these configuration policies remain intact through the entire conversion process.

3. Ensure the Telnet service is enabled on all APs and controllers.

   The upgrade tool utilizes telnet to create self-signed certificates on the APs by issuing a series of IOS commands. Telnet is used on controllers to accept the self-signed certificates.

   - For IOS devices, AMP provides the ability enable telnet in the template.
     - First check the Groups > Basic page to see how AMP is communicating with the IOS APs. If Telnet is selected as seen in the following figure, then proceed to the next step.

**Figure 3** ***Groups > Basic > Cisco IOS/Catalyst*** *options*



- If SSH is selected on the **Groups > Basic** page, then you will need to check the template (**Groups > Template** page) to ensure that telnet is enabled. Look for the following strings within the template. If you do not see the telnet restrictions within the template, then proceed to the next step.

```
...
access-list 111 permit tcp any any neq telnet
...
line con 0
 access-class 111 in
line vty 0 4
 access-class 111 in
 login local
line vty 5 15
 access-class 111 in
...
```

- If you see telnet restrictions within the template, then remove the **access-class** lines in each interface.

```
...
access-list 111 permit tcp any any neq telnet
...
line con 0
line vty 0 4
 login local
line vty 5 15
...
```

For controllers, you will need to access the web interface on the controller and select "**Yes**" for the **Allow New Telnet Session** option on the **Management > Telnet-SSH** page.

4. Ensure that converted APs will find a controller (optional).

   Converted APs that do not find a controller is the biggest hurdle that customers face in the entire conversion process. Configuring IOS devices that have static IP addresses to use DHCP will increase the probability that the LWAPP device will 'find' a controller after conversion. It is very easy for AMP to change an AP from static to DHCP from the device management page.

   ### Thin AP's Controller Discovery Mechanisms:

   - Local Broadcast - APs broadcast a controller discovery message. This is only applicable for APs on the same subnet as the controller's management interface.
   - DHCP - Option 43 Vendor Code will provide the controller's IP in the DHCP response. The DHCP server must be configured correctly prior to upgrade. This is the optimal discovery mechanism because most APs are not located on the same subnet as the controller's management interface.
   - DNS - via resolution of CISCO-LWAPP-CONTROLLER.localdomain. This method is used for IOS APs that have a static IP address and are not located on the same subnet as the controller's management interface.

   See Cisco DHCP and DNS LWAPP discovery instructions for more information.


Ensure that a DHCP server exists that is servicing the network where the IOS devices reside.

5. Ensure that the system date and time on the APs and controllers are synchronized.

   The upgrade tool creates self-signed certificates that require date/time synchronization of APs, controllers, and the Upgrade Tool.

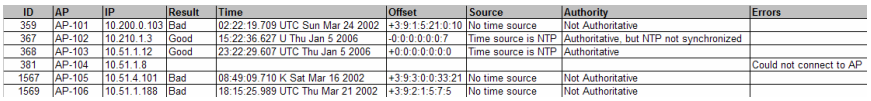
   ### IOS Devices

   a. Log in to AMP as root

   b. Type `scripts` to change to the scripts directory.

   c. Type `check_ios_time.pl > ios_time_file.txt`
   This script creates a csv file which, when imported into Excel, looks similar to the following:

**Figure 4** *IOS Time Check report*



| ID | AP | IP | Result | Time | Offset | Source | Authority | Errors |
|---|---|---|---|---|---|---|---|---|
| 359 | AP-101 | 10.200.0.103 | Bad | 02:22:19.709 UTC Sun Mar 24 2002 | +3:9:1:5:21:0:10 | No time source | Not Authoritative | |
| 367 | AP-102 | 10.210.1.3 | Good | 15:22:36.627 U Thu Jan 5 2006 | -0:0:0:0:0:0:7 | Time source is NTP | Authoritative, but NTP not synchronized | |
| 368 | AP-103 | 10.51.1.12 | Good | 23:22:29.607 UTC Thu Jan 5 2006 | +0:0:0:0:0:0:0 | Time source is NTP | Authoritative | |
| 381 | AP-104 | 10.51.1.8 | | | | | | Could not connect to AP |
| 1567 | AP-105 | 10.51.4.101 | Bad | 08:49:09.710 K Sat Mar 16 2002 | +3:9:3:0:0:33:21 | No time source | Not Authoritative | |
| 1569 | AP-106 | 10.51.1.188 | Bad | 18:15:25.989 UTC Thu Mar 21 2002 | +3:9:2:1:5:7:5 | No time source | Not Authoritative | |

### Controllers

- Navigate to the **Commands > Set Time** page to verify date and time.

### NTP Server

If required, you can use an NTP server to synchronize the IOS APs and the controllers.

- For IOS, add the following lines to each template:

```
sntp server <ip address>
```

- For controllers, navigate to **Controller > Network Time Protocol**, then add and enter the same SNTP server.

6. Create the IP file (list of APs to convert) for the Upgrade Tool

   The conversion process requires that you generate a list of the IP addresses for the APs that are to be converted. AMP generates this list for you via a script file, automatically ignoring any non-convertible IOS devices. Perform the following steps to create an IP file with AMP.

   a. Log in to AMP as root

   b. Type `scripts` to change to the scripts directory.

   c. Type `generate-ios_lwapp_list.pl` to generate multiple IP files - one per model present on your AMP.

      - 1100.ios_to_lwapp.txt
      - 1130.ios_to_lwapp.txt
      - 1200.ios_to_lwapp.txt
      - 1240.ios_to_lwapp.txt
      - 1300.ios_to_lwapp.txt

      The format is: `ap-ip-address,telnet-username,telnet-user-password,enable-password`

   d. Using putty or another scp client, 'scp' the files to the Windows machine that is facilitating the upgrade.

## Step Three: Conversion

1. Download the Upgrade Tool:

   http://www.cisco.com/public/sw-center/sw-ios.shtml

2. Install the Upgrade Tool.
   - Ensure your machine is running Windows XP, Windows 2000, or Windows 7.
   - Ensure that you have a minimum o f512 MB of RAM and 500 MB of free space on your hard drive.
   - Ensure that you are logged in as Administrator on the PC that is running the Upgrade Tool.
   - Ensure that Windows Firewall is disabled on the PC that is running the Upgrade Tool.
3. Run the Upgrade Tool import IP file.
   - **IP File:** Browse to the IP file created in by previous step.
   - **Controller Details:** Enter the IP address and the telnet user name and password.
   - **System Time Details:** If the PC that is running the Upgrade Tool matches the time of the controllers and APs, then select User Machine time. Otherwise, enter the specified date and time.
   - **Start:** Click the **Start** button to begin the upgrade.


You must close the Upgrade Tool after each model upgrade.

4. Automatic migration of the device history.

Rather than treating the converted LWAPP device as a brand new device, AMP automatically migrates historical data. This means that you do not sacrifice reporting, usage history, and other trend data when converting your access points. AMP automatically discovers the newly converted AP through its controller and automatically migrates all of that device's history.

This also enables AMP to provide accurate information on the true amount of network downtime associated with the conversion process.

5. Identify any upgrade conversion problems.

   Check AMP's "Down Device" list when the conversion is complete. During the conversion process, the old IOS access point's status will change from "up" to "down." The device status will revert to "up" when the conversion process is successfully completed. This process should typically take no more than 15 minutes. If any device being converted from IOS to LWAPP remains on AMP's Down Device list for more than 15 minutes, you should begin researching whether (and why) the upgrade failed.

## Step Four: Post-Conversion Analysis and Management

1. Assess overall downtime related to the conversion process.

   You can use AMP's "Uptime Report" to quickly assess the impact of the IOS-to-LWAPP conversion. This is particularly important if you will be converting your APs in batches: examining downtime data from the initial conversion batches will enable you to predict the impact of subsequent batches.

   Perform the following steps to gauge conversion-related downtime:

   a. Run an "Uptime Report' for the period during which the conversion took place.

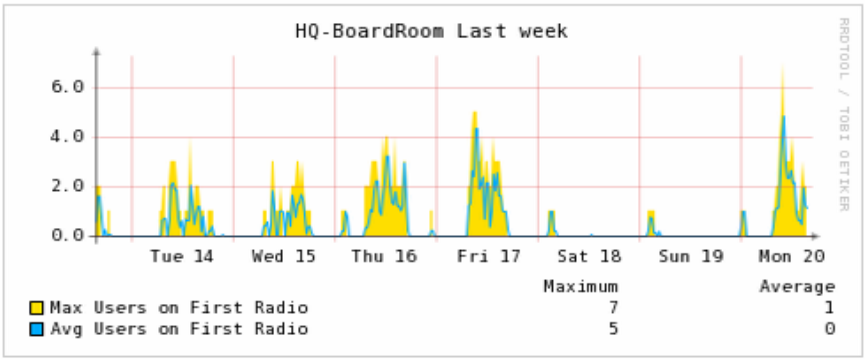
   b. Compare the data from the Uptime Report to an Uptime trend report covering the previous day, week, month, or year to assess the impact of the conversion. The Uptime Report provides summarized SNMP and ICMP uptime at a network-wide, Group, Folder, and Device level, delivering as much detailed information as you require for your analysis.

2. Compare pre-conversion and post-conversion data.

   To determine whether the conversion process had the beneficial impact you expected, you will likely want to compare post-conversion WLAN performance to pre-conversion levels. Because AMP retains historical data for all converted devices, these comparisons are easy on both a device and group level.

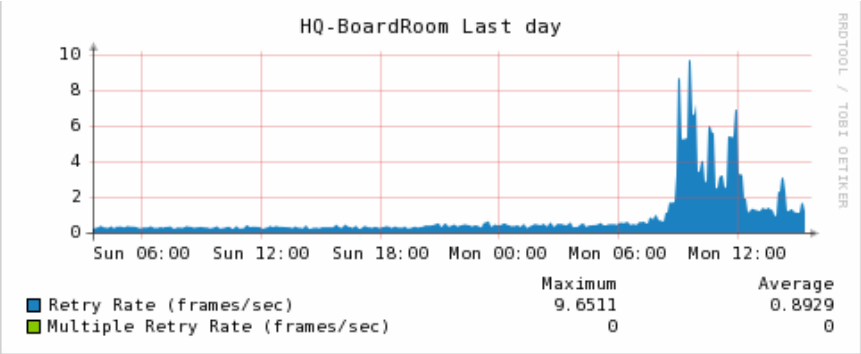
   - **Number of users per radio**: Following conversion, you can expect to see significantly smoother usage rates on a per-radio basis if the controller load-balancing algorithm is working properly. If significant usage spikes occur frequently following conversion, the algorithm may not be functioning properly.

**Figure 5** *Weekly graph of users per radio*



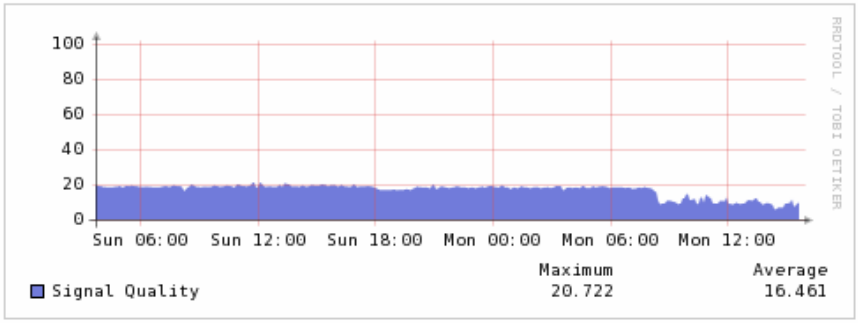

   - **Error rates**: In the following chart, is the dramatic increase in Multiple Retries related to the conversion? With AMP, you can continue to monitor trending over the next weeks and months.

**Figure 6** *Multiple Retry Rate (AP level)*




- **Signal quality**: Has the conversion had any positive or negative impact on the average signal quality received by users? In the following image, a decrease in signal quality followed the conversion.

**Figure 7** *Client Signal Quality*




3. Propagating self-signed certificates.

   Before LWAPP access points can be managed by any other non-primary controllers their self-signed certificate must be propagated to those controllers. AMP provides a very convenient method of propagating self signed certificates to other non primary controllers in your WLAN.

   a. Navigate to **Groups > LWAPP** APs page for the primary controller of the newly converted LWAP access points
   b. Locate the Self Signed Certificate Management section
   c. Select one of the following options from the Distribute Self-Signed Certificates drop down menu:
      - **Select by groups of controllers**: This enables certificate propagation to any other group that contains LWAPP controllers.
      - **Select by mobility groups**. This enables certificate propagation to all controllers in the selected mobility group
      - **By primary/secondary/tertiary controller**. This enables certificate propagation to the secondary and tertiary controllers of the newly converted LWAPP access points.