


ArubaOS 7.0.2.0



Release Note

Copyright

© 2011 Aruba Networks, Inc. Aruba Networks trademarks include , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners. Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.



www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Chapter 1	Release Overview	5
	Supported Browsers.....	5
	Related Documents	5
	Contacting Support	5
Chapter 2	What's New in this Release	7
	Features Introduced in ArubaOS 7.0.2.0	7
	Uplink Module Enhancements	7
	1050W Power Supply.....	7
	Jumbo Frames Enhancements	7
	Configuration File Format Changes	7
	DAC Cable Length	7
	Features Introduced in ArubaOS 7.0.1.0	8
	S3500-24T/48T	8
	Direct Attach Cables (DAC) Support.....	8
	Features Introduced in ArubaOS 7.0.0.0	8
	Profiles-Based Configuration	8
	Interface Groups	9
	Ethernet Link Profile	9
	Gigabit Ethernet Network Interfaces.....	10
	10 Gigabit Ethernet Uplink Interfaces	10
Chapter 3	Fixed Issues	11
	Platform	11
	Security.....	11
	Layer 2 Forwarding.....	11
	QoS	11
	WebUI, MIB, SNMP	12
Chapter 4	Known Issues.....	13
	Uplink Module.....	13
	Stacking Port Settings.....	13
	Tunneled-Node MTU Size and MTU Discovery	13
	Security	14
	Layer 2 Forwarding.....	15
	QoS.....	15
	Tunneled Node	15
	WebUI, MIB, SNMP	15
Chapter 5	Upgrade Procedures	17
	Important Points to Remember	17
	Before you Upgrade	17
	Save your Configuration	17
	Saving the Configuration in the WebUI.....	17

Saving the Configuration in the CLI	18
Upgrading from 7.0.0.0 to 7.0.2.0	18
Upgrading from the WebUI	18
Upgrading from the Command Line	18
Upgrading from your USB using the LCD.....	19
Downgrading after an Upgrade	21
Before You Call Your Support Provider.....	21

ArubaOS 7.0.2.0 is a maintenance software release that introduces new features and fixes to previously outstanding issues. For details on all of the features described in this release note, see the [Related Documents](#) section.

This release note contains the following chapters:

- [Chapter 2, “What’s New in this Release” on page 7](#) describes the new features introduced in this release
- [Chapter 3, “Fixed Issues” on page 11](#)—a listing of fixed issues in this release
- [Chapter 4, “Known Issues” on page 13](#)—a listing of known issues organized by functionality
- [Chapter 5, “Upgrade Procedures” on page 17](#)— instructions on how to upgrade your software

Supported Browsers

The supported browsers for the WebUI are:

- Microsoft Internet Explorer 8.x on Windows XP, Windows Vista, and Windows 7
- Mozilla Firefox 3.x on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari 5.x on MacOS

Related Documents

The following items are part of the complete documentation set for the Mobility Access Switch:

- *ArubaOS 7.0 User Guide*
- *ArubaOS 7.0 Command Line Reference Guide*
- *ArubaOS 7.0 Quick Start Guide*
- *Aruba S3500 Series Mobility Access Switch Installation Guide*

Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	licensing.arubanetworks.com/login.php
Wireless Security Incident Response Team (WSIRT)	arubanetworks.com/support/wsirt.php

Email Support

Americas and APAC

support@arubanetworks.com

EMEA

emea_support@arubanetworks.com

WSIRT Email

Please email details of any security problem found in an Aruba product.

wsirt@arubanetworks.com

This chapter provides a brief summary of the new features included in this release of ArubaOS.



ArubaOS 7.0.2.0 is supported on the Aruba S3500; other Aruba devices are not supported.

Features Introduced in ArubaOS 7.0.2.0

Uplink Module Enhancements

Enhancements have been made to uplink performance and support for updated PHY component on uplink module.

1050W Power Supply

ArubaOS 7.0.2.0 introduces support of the 1050W power supply.

Jumbo Frames Enhancements

ArubaOS 7.0.2.0 has added support of jumbo frames up to 9216 (9k) bytes.

Configuration File Format Changes

Beginning in ArubaOS 7.0.2.0, a configuration file to be downloaded from DHCP at bootup must meet the following two conditions or the file be ignored or the download will fail.

- The configuration file's file extension must be **.cfg**.
- The configuration file must have the following heading:

```
#  
# Configuration file for ArubaOS
```

This change does not affect any existing configuration files on your Mobility Access Switch. Those existing files are automatically configured to the new format upon upgrade to ArubaOS 7.0.2.0.

If you have any configuration files outside of your Mobility Access Switch, you must manually add the new header to any configuration files that will be installed by DHCP download. This can be done using any text editing tool.

DAC Cable Length

The DAC cable length can now be viewed using the CLI. A field has been added to the following command:

```
show interface gigabitethernet 0/1/0 transceiver  
Vendor Name           : Molex Inc.  
Vendor Serial Number  : 024930003  
Vendor Part Number    : 74752-1101  
Cable Type            : 10GBASE-DAC-P  
Connector Type        : Copper Pigtail  
Wave Length           : 0 nm
```

Cable Length : 1m



The cable length reading is an integer, so a 0.5m DAC cable will be displayed as 1m.

Features Introduced in ArubaOS 7.0.1.0

S3500-24T/48T

The S3500 series includes four models that provide varying levels of functionality (the S3500-23P/48P were introduced in Aruba 7.0). Support for the S3500-24T/48T is introduced with ArubaOS 7.0.1.0. [Table 1](#) lists basic details of all four supported models.

Table 1 Aruba Mobility Access Switch models

Model	Access Ports	PoE/PoE+ Ports	Minimum Required Power Supply	Controller Capable
S3500-24P	24x 10/100/1000Base-T	24	600W	Yes
S3500-48P	48x 10/100/1000Base-T	48	600W	Yes
S3500-24T	24x 10/100/1000Base-T	0	350W	No
S3500-48T	48x 10/100/1000Base-T	0	350W	No

Direct Attach Cables (DAC) Support

Direct attach cables (DACs) are used to connect one S3500 to another. DACs are installed in an uplink module in the same manner as an SFP module, using the 10GBASE-X Ports. For information on how to install a DAC, refer to the *Aruba S3500 Series Mobility Access Switch Installation Guide*. [Table 2](#) lists the supported cables.

Table 2 Direct Attach Cables

DAC	Description
SFP+, Direct Attach, 0.5M	50cm Direct Attach Cable; 10G SFP+ for stacking
SFP+, Direct Attach, 1M	1m Direct Attach Cable; 10G SFP+ for stacking

Features Introduced in ArubaOS 7.0.0.0

Profiles-Based Configuration

The ArubaOS WAP supports profile based configuration for interfaces, interface groups, port-channels, and VLANs. You can use profiles to apply the same configuration to multiple interfaces and VLANs. The profile-based configuration helps you to address consistency in interface parameters without having to manage large configurations. The ArubaOS WAP supports the following types of interface profiles:

- enet-link-profile—allows you to configure an Ethernet Link
- lacp-profile—allows you to configure an LACP
- lldp-profile—allows you to configure an LLDP Profile

- mirroring-profile—allows you to configure a Mirroring profile
- mstp-profile—allows you to configure an Interface MSTP
- poe-profile—allows you to configure a Power over Ethernet profile
- switching-profile—allows you to configure a switching profile
- tunneled-node-profile—allows you to configure a Tunneled Node Server profile
- voip-profile—allows you to configure a VOIP profile

Interface Groups

In the CLI configuration, it is often tedious to individually configure interfaces when there are multiple interfaces that have the same configuration. In such scenarios, you can group the interfaces together so that any interface within the group has the same configuration. When you configure an interface that is a member of an interface group, applying a specific profile to the interface takes precedence over the interface group configuration. By default, all the interfaces belong to a default interface group. To view the configuration of the default interface group, use the `show interface-group-config gigabitethernet default` command. When you create custom interface groups, the excluded interfaces continue to belong to the default interface group.

Interface group and port-channel are not the same. Interface group assigns the configuration to individual interfaces whereas the port-channel makes a group of interfaces to work as a single logical interface. You cannot have overlapping ranges of interfaces when you have multiple interface groups.

Ethernet Link Profile

You can use the ethernet link profile to configure the gigabit ethernet switching and uplink ports. The ethernet interfaces support auto negotiation from 10BaseT to 1000BaseT as per IEEE 802.3u/z standards. When you enable auto negotiation, the device that is connected to the port is automatically configured to the highest speed supported by the device in the following order (highest to lowest):

- 1000 Mbps full duplex
- 100 Mbps full duplex
- 100 Mbps half duplex
- 10 Mbps full duplex
- 10 Mbps half duplex

Auto negotiation also supports the pause capabilities, automatic Media Detection Interface (MDI), and Media Detection Interface Crossover (MDIX) cable detection. The devices exchange information using the Fast link Pulse (FLP) bursts.

The auto negotiation on the link is performed when you perform any of the following activities:

- Connect the device.
- Power on or reset the device at either end of the link.
- Make a negotiation request.

To manually set the physical interface characteristics such as speed and duplex, you can define them in a profile and apply the profile to the interface. This is beneficial when you have many interfaces that share the same characteristics where you can define the parameters in the ethernet link profile and then reference the name of the profile on the interfaces. When you need a change later, the change needs to be made only on the profiles and not on the individual interfaces.

Gigabit Ethernet Network Interfaces

The ArubaOS WAP supports 24 or 48 port gigabit ethernet interfaces mainly for switching purpose. The gigabit ethernet supports a maximum data rate of 1000 Mbps. The ArubaOS WAP provides gigabit ethernet interface ports to connect the end points to form a wired ethernet LAN network.

A network gigabit ethernet interface is referred by its `<slot>/<module>/<port>`.

- Slot—The member ID of the stack. Currently this is 0, since stacking capability is not supported in this release.
- Module—There are two modules where the first one is the front-panel network module (0), while the other one is the uplink network module (1).
- Port—The individual port number.

For example, interface `gigabitethernet 0/0/20` refers to the first stack member (0) on the front-panel network module (0) at port number (20).

10 Gigabit Ethernet Uplink Interfaces

The ArubaOS WAP supports a modular uplink module with four 10GbE SFP+ interfaces. You can use the following types of optics for the uplink interfaces:

- 10GbE fiber with SFP-10G-SR, SFP-10G-LR.
- GbE fiber with SFP-SX, SFP-LX.
- Copper with SFP-TX.

The uplink module and the optics are hot-swappable. The first two interfaces (0/1/0, 0/1/1) can be configured as uplink interfaces while the latter two (0/1/2, 0/1/3) are by default configured as stacking ports. You can also use third-party optics in the uplink modules. However, you should use only the approved optics if any issues are observed while troubleshooting. The copper SFP-TX transceiver supports only 1000 Mbps speed.

The following issues were fixed in this release.

Platform

Table 3 *Fixed Platform Issues and Limitations*

Bug ID	Description
54809	Due to a very rare timing issue, the chassis management daemon may crash.
52666	The show inventory command does not display negative temperature as expected.

Security

Table 4 *Fixed Security Issues*

Bug ID	Description
53173	mac-move does not work as expected
52903	mac-limit with drop action is not working as expected

Layer 2 Forwarding

Table 5 *Fixed Layer 2 Forwarding Issues*

Bug ID	Description
53187, 53030	L2M crashed unexpectedly during MSTP state changes

QoS

Table 6 *Fixed QoS Issues*

Bug ID	Description
52702	If a QoS profile, attached to an ACL, and both the ACL and QoS profile are both removed, DPA will still have the QoS profile. Additionally, creating the QoS profile again will cause the OID suppression of the new object.

System Logs and Alarms

Table 7 *Fixed System Logs and Alarm Issues*

Bug ID	Description
51151	Syslog for port channel link up, admin up
50794	Network facility syslog messages for LAG and LACP

WebUI, MIB, SNMP

Table 8 *Fixed WebUI, MIB, SNMP Issues*

Bug ID	Description
53537	CMICM crashed while SNMPWalk access MIBs—Interface Extend Port Table
53175	Memory leak issues with SNMP during AirWave monitoring
52930	IF-MIB counters are returned as 0 for Port channel

The following are known issues and caveats. Applicable bug IDs and workarounds are included when possible.

Uplink Module

The uplink module allows you to bring up 4 additional ports of 1GE or 10GE interfaces, or a combination depending on the inserted transceivers which are automatically detected by the software driver. The current software version supports SFP-SX, SFP-TX, SFP-LX, SFP+ SR, SFP+ LR and DAC cables (see [Table 2](#)).

The following are known issues on currently supported hardware:

- Module Hot Swap is not supported —after inserting an uplink module, you must reload your Mobility Access Switch
- The **shut** command fails to shutdown the DAC interface—An interface using DAC cables does not respond to the **shut** command as expected and fails to shutdown the port; the **shut** command only brings down the protocols associated to the interface while leaving the physical link UP. To avoid any confusion with status, do not use the **shut** command on a DAC interface.

Stacking Port Settings



Stacking is not supported at FCS, however uplinks 0/1/2 and 0/1/3 have been reserved for stacking.

The following command shows the ports reserved for stacking.

```
(host) #show stacking interfaces
Stacking ports:
-----
stk1/3   Hardware info(module:1, port:3)
stk1/2   Hardware info(module:1, port:2)
```

The following command can convert the ports reserved for stacking to normal uplink ports:

```
(host) #stacking interface delete stk 1/2
      Reboot the system to apply the changes.
(host) #stacking interface delete stk 1/3
      Reboot the system to apply the changes.
```

Tunneled-Node MTU Size and MTU Discovery

To solve the MTU size issues between a tunneled node and a controller, use the following command:

```
(host) (Tunneled Node Server profile "TEST") #mtu ?
<mtu>           MTU on path to controller [1024-1500]. Default: 1400
```

By setting this parameter, a handshake will happen between the tunneled node and controller to setup a desired MTU size. Aruba controllers have a default MTU size of 1400 bytes.

If there is a router with a default MTU size less than 1400 between your Mobility Access Switch and your controller, use the following command to discover the correct MTU size:

```
ping mtu_discovery do size mtu_size ip_address
```

If there are multiple routers with different, smaller MTU sizes between your Mobility Access Switch and controller, you may have to repeat this command multiple times to discover the MTU of the next router.

Security

Table 9 *Known Security Issues and Limitations*

Bug ID	Description
48240	Machine authentication does not work when using a device operating on Windows XP Service Pack 2 (SP2). Workaround: Upgrade to SP3 or if you do not want to upgrade from SP2, you have to enable the re-authentication under 802.1X authentication profile to make machine auth and user auth to work.
49140	Non-IP traffic is allowed when the standard ACL is configured with an any/any/permit rule. (Since the standard ACL is IP-based, all non-IP traffic should be dropped.) Workaround: None.
49254	L2 traffic is allowed to pass without a L2 ACL by default. However, L3 traffic block without a L3 ACL by default. Workaround: If you need to block L2 traffic, you must create a L2 ACL that specifically blocks all L2 traffic.
49262	If the same IP address is used by two clients on different VLANs, the S3500 will only forward traffic for one of the clients. Traffic from both clients should be forwarded. Workaround: None.
50987	In the absence of the role defined in the local-userdb, switch takes the default role configured in the aaa profile. Therefore, a local userdb entry is allowed to be created with a user role that had not be previously configured. Workaround: None. This the expected behavior.
51213, 51332	MAC authentication does not work with jumbo frames larger than 1700 bytes. Workaround: None.
52260	Auth and SSM modules consumes large amounts of CPU capacity when MAC authentication fails at 500 PPS. Workaround: Configure blacklisting of MAC users to prevent continuous MAC authentication failures.
52454	802.1X authentication fails for EAP-TLS when the S3500 is rebooted. Workaround: Use server certificate that has certificate request generated from Certificate WebUI only.

Layer 2 Forwarding

Table 10 *Known Layer 2 Forwarding Issues and Limitations*

Bug ID	Description
48692	<p>The <code>MAC-Limit</code> parameter under the command <code>show interface-config gigabitethernet</code> does not support untrusted interfaces.</p> <p>Workaround: None.</p>

Platform

Table 11 *Known Platform Issues and Limitations*

Bug ID	Description
56343	<p>Upgrading from an external USB device using the LCD screen does not work.</p> <p>Workaround: Use the CLI or WebUI to upgrade.</p>

QoS

Table 12 *Known QoS Issues and Limitations*

Bug ID	Description
47957	<p>When an interface is configured as untrusted, QoS DSCP rewrite does not work for the initial set of frames (until the user entry is added completely).</p> <p>Workaround: None.</p>

Tunneled Node

Table 13 *Known Tunneled Node Issues and Limitations*

Bug ID	Description
49278	<p>A controller will forward all broadcast traffic on all VLANs to the tunnel when the trunk port is configured as a tunneled node port on a Mobility Access Switch.</p> <p>Workaround: None.</p>
50496	<p>When there is a switch connected to a tunneled node port of a Mobility Access Switch, the Mobility Access Switch forwards the Spanning Tree BPDU generated by the switch to the controller over a GRE tunnel. However, the controller does not send its BPDU over the GRE tunnel to the tunnel.</p> <p>Workaround: None.</p>

WebUI, MIB, SNMP

Table 14 *Known WebUI, MIB, SNMP Issues and Limitations*

Bug ID	Description
50562	Interfaces on the S3500 Uplink Module are not supported by the MIB ifExtPortIfIndex. Workaround: None.
50862, 51845	The default AAA profile will not appear in the WebUI if both MAC and 802.1X are configured for a AAA profile or neither MAC nor 802.1x are configured for a AAA profile. Workaround: None. You can always view the default AAA profile in the CLI by using the <code>show aaa profile</code> command.
51945	aruba-ifext-mib, ifExtMode shows incorrect values for mirroring interfaces. Workaround: None.
52705	If you create more than one AAA profiles in a single screen (without refreshing the page or navigating away from the current page), the server group for last created AAA profile gets applied to the AAA profiles created previously. Workaround: To create more than one AAA profiles via WebUI, refresh the page or navigate to another page after you create one AAA profile and then create another AAA profile.

This chapter details the Mobility Access Switch software upgrade procedures. To optimize your upgrade experience and ensure your upgrade is successful, read all the information in this chapter before upgrading and follow all the procedures carefully.

Topics in this chapter include:

- “Important Points to Remember” on page 17
- “Before you Upgrade” on page 17
- “Save your Configuration” on page 17
- “Upgrading from 7.0.0.0 to 7.0.2.0” on page 18
- “Downgrading after an Upgrade” on page 21
- “Before You Call Your Support Provider” on page 21

Important Points to Remember

You should create a permanent list of this information for future use.

- Best practices recommends upgrading during a maintenance window. This will limit the troubleshooting variables.
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- List the devices in your infrastructure that are used to provide your wireless users with connectivity (Core switches, radius servers, DHCP servers, firewall, for example).
- Always upgrade the non-boot partition first. If something happens during upgrade, you can switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.

Before you Upgrade

You should ensure the following before installing a new image on the Mobility Access Switch:

- Make sure you have at least 60 MB of free flash space (**show storage** command).
- Run the **tar crash** command to ensure there are no “process died” files clogging up memory and FTP/TFTP the files to another storage device. To clean up any crash core file, use the **tar clean crash** command.
- Remove all unnecessary saved files from flash (**delete filename** command).

Save your Configuration

Before upgrading, save your configuration and back up your Mobility Access Switch data files. Saving your configuration will retain the **admin** and **enable** passwords in the proper format.

Saving the Configuration in the WebUI

1. Click on the **Configuration** tab.
2. Click the **Save Configuration** button at the top of the screen.

Saving the Configuration in the CLI

Enter the following command in either the enable or configuration mode:

```
(host) #write memory
```

Upgrading from 7.0.0.0 to 7.0.2.0

Read all the following information before you upgrade. Download the latest software image from the Aruba Customer Support web site.

There are three ways to upgrade your software image:

- “Upgrading from the WebUI” on page 18
- “Upgrading from the Command Line” on page 18
- “Upgrading from your USB using the LCD” on page 19

Upgrading from the WebUI

The following steps describe how to install the Aruba software image from a PC or workstation using the WebUI on the Mobility Access Switch. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Upload the new software image to a PC or workstation on your network.
2. Log in to the WebUI from the PC or workstation.
3. Navigate to the **Maintenance > Image Management** page. Select the “Upgrade using local file” radio button, then click the **Browse** button to navigate to the image file on your PC or workstation.
4. Determine which partition will be used to hold the new software image. Best practices is to load the new image onto the non-boot partition. To see the current boot partition, navigate to the **Maintenance > Boot Parameters** page.
5. Select the **Yes** radio button in the “Reboot after upgrade” field to reboot after upgrade.
6. Click **Upgrade Image**.
7. When the software image is uploaded to the Mobility Access Switch, a popup appears. Click **OK** in the popup window. The boot process starts automatically within a few seconds (unless you cancel it).
8. When the boot process is complete, log in to the WebUI and navigate to the **Monitoring > Summary** page to verify the upgraded code version.
9. Click on the **Configuration** tab.
10. Click the **Save Configuration** button at the top of the screen to save the new configuration file header.

Upgrading from the Command Line

The following steps describe how to install the ArubaOS software image using the CLI on the Mobility Access Switch. You need a FTP/TFTP server reachable from the Mobility Access Switch you are upgrading.

1. Upload the new software image to your FTP/TFTP server on your network.
2. Execute the ping command to verify the network connection from the target Mobility Access Switch to the FTP/TFTP server:

```
(host) # ping <tftphost>
```



A placeholder file with the destination filename and proper write permissions must exist on the FTP/TFTP server prior to executing the **copy** command.

3. Determine which partition to load the new software image. Best practices is to load the new image onto the backup partition (the non-boot partition). To view the partitions, use the **show image version** command.
4. Use the **copy** command to load the new image onto the Mobility Access Switch:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
or
(host) # copy tftp: <tftphost> <image filename> system: partition 1
```



When using the **copy** command to load a software image, the specified partition automatically becomes active (default boot partition) the next time the Mobility Access Switch is rebooted. There is no need to manually select the partition.

5. Execute the **show image version** command to verify the new image is loaded:

```
(host) #show image version
-----
Partition           : 0:0 (/dev/hda1)
Software Version    : ArubaOS 7.0.0.0 (Digitally Signed - Production Build)
Build number        : 28198
Label               : 28198
Built on            : Tues May 04 09:11:59 PST 2009
-----
Partition           : 0:1 (/dev/hda2) **Default boot**
Software Version    : ArubaOS 7.0.2.0 (Digitally Signed - Production Build)
Build number        : 28918
Label               : 28918
Built on            : Fri Jun 24 09:11:59 PST 2010
```

6. Reboot the Mobility Access Switch:

```
(host) # reload
```

7. Execute the **show version** command to verify the reload and upgrade is complete.

```
(host) #show version
Aruba Operating System Software.
ArubaOS (MODEL: ArubaS3500-48P), Version 7.0.2.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
...
```

8. Execute the **write memory** command to save the new configuration file header.

Upgrading from your USB using the LCD

The S3500 is equipped with an LCD panel that displays a variety of information about the mobility access switch's status and provides a menu that allows for basic operations such as initial setup and reboot. The LCD panel displays two lines of text.

Use the upper right **Menu** button to navigate through LCD functions and the lower right **Enter** button to select (or enter) a LCD function. The active line, in the LCD panel, is indicated by an arrow.

Use a USB device to transfer the upgrade image:

1. Create a folder named **arubaimage** on your USB device.

- Using your laptop, copy the new image from the support site to your USB device's folder **arubaimage**



You must download the new image to the folder **arubaimage** or the image will not upload to the Mobility Access Switch properly.

- Insert your USB device into the rear USB port (next to the console port) of your mobility access switch.
- Slowly press the **Menu** button until you reach the **Maintenance** function.
- Press the **Enter** button to enter the maintenance function.
- Press the **Enter** button at **Upgrade Image** function.
- Press the **Menu** button to locate the partition you want to upgrade.

```
partition 0
```

```
partition 1
```

Then press the **Enter** button to select the partition to upgrade.



Always upgrade the non-boot partition first. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.

- Press the **Enter** button again to confirm the partition you are upgrading (or press the **Menu** button to exit).

```
y: Enter button
```

```
n: Menu button
```

- The LCD displays an a upgrade in process acknowledgement:

```
Upgrading...
```

When the upgrade is complete, the LCD displays the message:

```
Reload to boot from new image
```



When loading a software image, the specified partition automatically becomes active (default boot partition) the next time the Mobility Access Switch is rebooted. There is no need to manually select the partition.

- From the command line, execute **show image version** to view the partitions:

```
(host) #show image version
```

```
-----  
Partition           : 0:0 (/dev/hda1)  
Software Version    : ArubaOS 7.0.0.0 (Digitally Signed - Production Build)  
Build number        : 28198  
Label               : 28198  
Built on            : Tues May 04 09:11:59 PST 2009  
-----  
Partition           : 0:1 (/dev/hda2) **Default boot**  
Software Version    : ArubaOS 7.0.2.0 (Digitally Signed - Production Build)  
Build number        : 28918  
Label               : 28918  
Built on            : Fri Jun 24 09:11:59 PST 2010
```

- Reboot the Mobility Access Switch:

```
(host) # reload
```

- Execute the **show version** command to verify the reload and upgrade is complete.

```
(host) #show version
```

```
Aruba Operating System Software.
```

ArubaOS (MODEL: ArubaS3500-48P), Version 7.0.2.0

Website: <http://www.arubanetworks.com>

Copyright (c) 2002-2011, Aruba Networks, Inc.

...

13. Execute the **write memory** command to save the new configuration file header.

Downgrading after an Upgrade

If necessary, you can return to your previous version.



Save your configuration file before and after completing your downgrade.

Before you reboot the Mobility Access Switch with the pre-upgrade software version, you must perform the following steps:

1. Set the Mobility Access Switch to boot with the previously-saved configuration file.
2. Set the Mobility Access Switch to boot from the system partition that contains the previously running image.
3. Execute the **write memory** command after the downgrade to save your configuration.

Before You Call Your Support Provider

Before you place a call to Technical Support, please follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Mobility Access Switch with IP addresses and Interface numbers if possible).
2. Provide the Mobility Access Switch logs and output of the **show tech-support** command.
3. Provide the syslog file of the Mobility Access Switch at the time of the problem.

Best practices strongly recommends that you consider adding a syslog server if you do not already have one to capture from the Mobility Access Switch.

4. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have:
 - an outage in a network that worked in the past.
 - a network configuration that has never worked.
 - a brand new installation.
5. Let the support person know if there are any recent changes in your network (external to the Mobility Access Switch) or any recent changes to your Mobility Access Switch configuration.
6. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) when the problem first occurred.
8. If the problem is reproducible, list the exact steps taken to recreate the problem.
9. Provide the Mobility Access Switch site access information, if possible.

