ArubaOS 7.1

ARUBA networks

Release Note

Copyright

© 2011 Aruba Networks, Inc. Aruba Networks trademarks include airwave, 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.

ARUBA®
networks

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1 Release Overview ... 5

Supported Browsers ... 5

Related Documents ... 5

Contacting Support ... 5

Chapter 2 What’s New in this Release ... 7

Stacking ... 7

Rapid PVST+ ... 7

Spanning Tree Modes ... 7

Static Routing ... 8

Routed VLAN Interfaces (RVI) ... 8

IPv6 on Management Interface ... 8

WebUI ... 8

Tace Options ... 8

Controller-ip ... 8

DHCP Server and DHCP Relay ... 9

IGMP ... 9

Radius Accounting ... 9

Cisco Discovery Protocol (CDP) ... 9

QoS ... 9

Time-Domain Reflectometer (TDR) ... 9

Chapter 3 Fixed Issues ... 11

Chapter 4 Known Issues ... 13

Uplink Module ... 13

Tunneled-Node MTU Size and MTU Discovery ... 13

DHCP ... 13

IGMP Snooping ... 14

IPv6 ... 14

Layer 2 Forwarding ... 14

QoS ... 15

Routing ... 15

Security ... 16

Stacking ... 17

Switch-Platform ... 18

Tunneled Node ... 18

WebUI, MIB, SNMP ... 19

Chapter 5 Upgrade Procedures 21

Important Points to Remember 21

Before you Upgrade 21

Save your Configuration 21

Saving the Configuration in the WebUI 22

Saving the Configuration in the CLI 22

Upgrading to 7.1 22

Upgrading from the WebUI 22

Upgrading from the Command Line 23

Upgrading from your USB using the LCD 24

Downgrading after an Upgrade 26

Before You Call Your Support Provider 27

Chapter 1

Release Overview

ArubaOS 7.1 is a major 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 21— 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 7.1 User Guide*
- *ArubaOS 7.1 Command Line Reference Guide*
- *ArubaOS 7.1 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 securityproblem found in an Aruba product.	wsirt@arubanetworks.com

Chapter 2

What’s New in this Release

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

NOTE

The Mobility Access Switch has a default user name (admin) and password (admin123).

Stacking

The Stacking feature enables simplified management by presenting a set of Mobility Access Switches as one entity, and reduces the operational complexity of managing multiple redundant links between access and distribution layer switches. Since the *stack* appears as one network node, loop prevention protocols are not required.

The Stack is a set of interconnected Mobility Access Switches using stacking ports to form a stack. A stacking port is a physical port provisioned to run the Aruba stacking protocol (ASP). In factory default settings for Mobility Access Switches, 10 Gigabit uplink ports 2 and 3 are pre-provisioned to be stacking ports. Once a port is provisioned for stacking, it is no longer available to be managed as a network port. A stacking port can only be connected to other Mobility Access Switches running the Aruba Stacking Protocol (ASP).

Rapid PVST+

Rapid PVST+ runs a separate spanning tree instance for each Virtual Local Area Network (VLAN). This allows the port to forward some VLANs while blocking other VLANs. PVST+ provides for load balancing of VLANs across multiple ports resulting in optimal usage of network resources. This implementation of Rapid PVST+ (Per-VLAN Spanning Tree Plus) is based on the IEEE Standards 802.1D-2004 and 802.1Q-2005 ensuring interoperability with industry accepted PVST+ protocols. In addition, Rapid PVST+ supports the loopguard, rootguard, and portfast features.

Spanning Tree Modes

To set spanning tree modes, use the spanning tree mode command. Once you change the spanning tree mode, the new spanning tree is automatically applied to all configured VLANs, including default VLAN 1.

```
(host)(config) #spanning-tree mode ?
mstp                    Multiple spanning tree mode
pvst                    Per-Vlan rapid spanning tree mode
(host)(config) #spanning-tree mode pvst
(host)(config) #
```

To verify the current spanning tree mode:

```
(host)(config) #show spanning-tree-profile

spanning-tree
-------------
Parameter           Value
---------           -----
spanning-tree-mode  pvst
```

Static Routing

The Mobility Access Switch supports static routes configuration. You can configure a default gateway and multiple static routes within the global IP-profile to route packets outside the local network. The static routes are active or added to the routing table only when the next hop is reachable, and can be removed from the static routes list only by using the no command.

Routed VLAN Interfaces (RVI)

RVIs are logical interfaces that enable routing and bridging between VLANs. You can route and bridge a protocol on the same interface. The traffic that remains in the bridge group (the bridged traffic) will be bridged among the bridged interfaces, and the traffic that needs to go out to another network (the routed traffic) will be routed internally to the appropriate output routed interface.

IPv6 on Management Interface

IPv6 is supported at outbound management interface on the Mobility Access Switch.

NOTE

IPv6 on routed VLAN interface is supported as Beta quality in this release.

WebUI

The Monitoring feature, with online Help, is supported in the WebUI. Other new WebUI features are:

- Configuring VLAN with IP
- Configure controller-ip
- Configure static routes
- Set boot parameters for each stack member

Tace Options

The tracing feature is important for debugging the sequence of events that occur inside a process or protocol, for example message processing, state machine transitions, configuration change events, or timer events.

You can control Layer 2 trace options, via the command line, enabling or disabling tracing, setting module tracing, and even configuring the Layer 2 Manager trace file size. For a complete listing of trace options commands, see the *ArubaOS 7.1 Command Line Reference Guide*

Controller-ip

The Mobility Access Switch automatically chooses the loopback IP or the first VLAN IP address as the controller-ip (also known as "Switch-IP") address during the stack initial boot. If loopback does not exist, then the Mobility Access Switch automatically chooses the first VLAN IP as the controller-ip.

Aruba best practices recommends configuring the controller-ip to the loopback interface when using Ethernet and Controller functions.

DHCP Server and DHCP Relay

The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, other servers such as time servers, and so forth. When a DHCP-configured client connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server.

DHCP Option 82 allows a DHCP Relay Agent to insert circuit specific information into a request that is being forwarded to a DHCP server. The option works by setting two sub-options:

- Circuit ID
- Remote ID

IGMP

The Mobility Access Switch supports Internet Group Management Protocol (IGMP) as defined in IETF RFC 1112 (IGMPv1) and RFC 2236 (IGMPv2).

Radius Accounting

Sending user statistics in RADIUS accounting stop and interim records is supported.

Cisco Discovery Protocol (CDP)

CDP is now supported with LLDP.

QoS

QoS support is expanded to include trust modes:

- Auto—Layer 2 + Layer 3 trust
- Dot1p—Trust only 802.1p bits
- DSCP —Trust only DSCP bits of the IP header
- None—Do not trust any incoming 802.1p/DSCP. Will be queued to Queue 0

Time-Domain Reflectometer (TDR)

Run a Time-Domain Reflectometer (TDR) diagnostic test on a specific gigabitethernet interface. TDR is a measurement technique used to characterize and locate faults in metallic cables such as twisted pair. TDR transmits a short rise electric pulse across the conducting cable and if the cable is properly terminated, the entire electric pulse is absorbed on the other end. If the any faults exist in the cable, some of the incident signal is sent back to the toward the source.

Chapter 3

Fixed Issues

The following issues were fixed in this release.

Configuration

Table 1 *Fixed Configuration Issues*

Bug ID	Description
54753	ArubaOS validates the file type and format of the configuration file before downloading it to the system.

Switch-Platform

Table 2 *Fixed Switch-Platform Issues*

Bug ID	Description
48204	Typing ctrl-S in a CLI no longer locks the session.
54809	Chassis manager due to an unknown LCD event has been fixed.
56013	Country code support has been added.
58136	The enable password is no longer set back to the default after upgrading.
57315	The Quick Setup function on the LCD display has been renamed to GUI Quick Setup.

Chapter 4

Known Issues

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.

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

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.

DHCP

Table 3 *Known DHCP Issues and Limitations*

Bug ID	Description
54911	After executing the `show ip dhcp binding` command, if multiple instances of the same lease are displayed, check for the last entry of that lease for the most recent information. **Workaround:** None.
58095	For VoIP phones on untrusted interfaces, configuring `aaa user fast-age` is not recommended. **Workaround:** None.

Table 3 *Known DHCP Issues and Limitations (Continued)*

Bug ID	Description
59718	After any configuration change, if `show ip dhcp` set of commands are run immediately, you may see the message **Module DHCP Daemon is busy. Please try later**. **Workaround:** Retry the command after a few seconds.

IGMP Snooping

Table 4 *Known IGMP Snooping Issues and Limitations*

Bug ID	Description
58360	When the host is in IGMPv3 mode, the Mobility Access Switch will not forward packets to the host. **Workaround:** Configure the switch to be in igmp-snooping proxy mode.

IPv6

Table 5 *Known IPv6 Issues and Limitations*

Bug ID	Description
56381	Login from WebUI using IPv6 address on Mozilla Firefox 7.0.1 fails with error. **Workaround:** 1) Try other browsers like Internet Explorer or Google Chrome. 2) Try an older version of Mozilla firefox as the latest version 7.0.1 has problems but previous versions work fine.
57529	Copy on IPv6 address does not work as this command is not recognized for IPv6. As a result, the scp/ftp/tftp copy over IPv6 address will not work. **Workaround:** Use an IPv4 address instead of an IPv6 or use the WebUI and try the local file management.
59922	When a new primary is elected, `show interface mgmt` may fail to display IPv6 address. **Workaround:** This is only a display issue and has no functional impact; use `show ipv6 interface` instead.

Layer 2 Forwarding

Table 6 *Known Layer 2 Forwarding Issues and Limitations*

Bug ID	Description
58248	ICMP Redirect messages are not generated on VLAN interfaces. **Workaround:** None.

Table 6 *Known Layer 2 Forwarding Issues and Limitations (Continued)*

Bug ID	Description
58962	Spanning Tree path cost is updated to match ieee spec. (802.1Q 2005, Page 189, Table 13-3—Internal Port Path Costs) **Workaround:** None.
59223	When a port-channel is running at 40 Mbps Speed, its Port Cost will be incorrectly computed at 1600000. **Workaround:** None.
59597	Spanning Tree is automatically disabled after downgrading from ArubaOS 7.1 to 7.0. **Workaround:** Manually enable MSTP after downgrading.
59879	An HSL blocked interface might be observed sending forwarding traffic under certain conditions. **Workaround:** Use the command `process restart l2m` to retsart L2M process. Only use this command in concert with your support provider.

QoS

Table 7 *Known QoS Issues and Limitations*

Bug ID	Description
47957	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). **Workaround:** None.

Routing

Table 8 *Known Routing Issues and Limitations*

Bug ID	Description
56986	VLAN interfaces do not generate network unreachable and host unreachable ICMP response packets. **Workaround:** None.
57412	There is no warning message when deleting a loopback IP address or VLAN IP address that has been automatically chosen to be the system controller-ip at boot up **Workaround:** Confirm your existing controller-ip before deleting any IP interface.
59572	Traceroute to and from a routing VLAN interface (RVI) fails if connecting to a non-primary member interface. **Workaround:** None.

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.
48692	Tthe `MAC-Limit` parameter under the command `show interface-config gigabitethernet` does not support untrusted interfaces. **Workaround:** None.
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.
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.
53844	After successful machine authentication, the client receives the VLAN and IP configured under machine-auth role. However, later upon successful dot1x authentication, the client loses the IP received earlier during successful machine-auth. **Workaround:** None.
56900	In some cases, the command `show trace-buf` might not track all `rad acct start` information. **Workaround:** None.

Table 9 *Known Security Issues and Limitations (Continued)*

Bug ID	Description
57334	If the system clock is changed while any authenticated user entries exist, the age timer of those entries are calculated incorrectly. **Workaround:** Do not change system timers while your MAS is actively running with authenticated users. If you have to, you can purge all existing authenticated users by using the `aaa user delete all` command.
57943	With VLAN Derivation configured, after a user is authenticated and redirected to a different VLAN, two user entries will remain until the idle timer ages out. **Workaround:** There is no functional impact. The original entry will be deleted automatically after the idle timer ages out. You can aslo use `aaa user delete` to remove the original VLAN entry before timeout.
59121	If an already configured aaa authentication server for management user authentication is unreachable from an S3500, even after removing the management authentication, users may observe a delay of about 6 seconds while logging on S3500. **Workaround:** None.

Stacking

Table 10 *Known Stacking Issues and Limitations*

Bug ID	Description
54760	Password recovery does not work on a re-directed console to primary or the local console of non-primary members of the stack. **Workaround:** Always recover the forgotten password over stack from the Primary member's local console session.
58585	When multiple splits occur on 3+ members stack with `no-split-detection` enabled, it may result in no Primary being elected. **Workaround:** The command `no-split-detection` is only recommended in a 2-member stack. The purpose is to prevent no active Primary if Secondary dies.
60076	Once a Primary switch reloads or switches over to the secondary, existing management users may lose ssh-pubkey certificate and will not be able to login. **Workaround:** Recreate the management user entry.
60166	Port Mirroring may not function properly after a stack split and merge back. **Workaround:** Remove and then reconfigure your port mirroring settings.

Switch-Platform

Table 11 *Known Switch-Platform Issues and Limitations*

Bug ID	Description
58584	When an AP is connected to an S3500 through a mid-span PoE injector, autonegotiation might fail. **Workaround:** Force link speed on the ports.
58708	Once the user enables the **GUI Quick Setup**, ArubaOS should only allow the user to the system via http. However, it allows the user to ssh to the system. **Workaround:** Do not SSH into the system during **GUI Quick Setup** mode.
59797	If the logging level for Network/System logs is set to informational, after rebooting S3500, <INFO> level logs are not being logged. **Workaround:** Reconfigure the logging after S3500 has rebooted.
59887	The command `show log errorlog` might show logs which are not ordered according to the time-stamp. **Workaround:** Issue tar logs commands. The resultant file logs.tar will contain errors.log displaying logs with proper timestamps.

Tunneled Node

Table 12 *Known Tunneled Node Issues and Limitations*

Bug ID	Description
49278	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. **Workaround:** None.
50496	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. **Workaround:** None.
57690	A local VLAN is not required for Tunneled-Node operation. However, to apply a switch-profile to a Tunneled-Node configuation, a local VLAN is required to activate the switch-profile. **Workaround:** None. Ignore the warning message that appears.
59976	If the primary stack member is rebooted, the tunneled-node traffic might not recover. **Workaround:** Restart the process using the `process restart l2m` command. Only use this command in concert with your support provider.

WebUI, MIB, SNMP

Table 13 *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.
58817	The CLI configuration command `syslocation` and the MIB object wlsxStackMemberSysLocation specify local system location of the entire Stack; Per member System location is available yet. **Workaround:** None.
59082	You cannot configure a loopback interface for controller-ip using the WebUI. **Workaround:** Use the CLI to configure this.
59586	The command `snmp-server trap source` does not work correctly if a nonexistent IP is used. **Workaround:** None.
59895	When using the WebUI to load a large configuration (e.g 2000+ VLANs), it may take minutes and fail to display all VLANs. **Workaround:** Use CLI to display all VLANs.
59971	In the WebUI, under **Configuration > Ports > Port Channel**, you can configured up to 8 members, but it does not display more than two members. **Workaround:** Use the CLI to view the correct number of members.

Chapter 5

Upgrade Procedures

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 21
- "Before you Upgrade" on page 21
- "Save your Configuration" on page 21
- "Upgrading to 7.1" on page 22
- "Downgrading after an Upgrade" on page 26
- "Before You Call Your Support Provider" on page 27

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.
- If you have removed the default stacking interfaces (ports 0/1/2 and 0/1/3) from 7.0.x but plan to use them for stacking purposes after upgrading to 7.1.x, you must reconfigure them for stacking.

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 to 7.1

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 22
- "Upgrading from the Command Line" on page 23
- "Upgrading from your USB using the LCD" on page 24

CAUTION

If you are upgrading from 7.0.x to 7.1 and are going to create a stack, each Mobility Access Switch in the stack must be upgrade to ArubaOS 7.1 before forming the stack.

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**. The image, once copied to the stack Primary, will be pushed down to every stack member.
7. When the software image is uploaded to the Mobility Access Switch, a popup appears. Click **OK** to reload the entire stack. The boot process starts automatically within a few seconds.
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>
   ```

NOTE

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. The image, once copied to the stack Primary, will be pushed down to every stack member:

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

NOTE

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 member all** command to verify the new image is loaded:

   ```
   ((host)#show image version member all
   Member-id: 0
   -----------------------------------
   Partition               : 0:0 (/dev/ud1) **Default boot**
   Software Version        : ArubaOS 7.1.0.0 (Digitally Signed - Production Build)
   Build number            : 30977
   Label                   : 30977
   Built on                : Fri Nov 4 16:07:32 PDT 2011
   ----------------------------------
   Partition               : 0:1 (/dev/ud2)
   Software Version        : ArubaOS 7.0.0.0 (Digitally Signed - Production Build)
   Build number            : 28198
   Label                   : 28198
   Built on                : Wed May 4 15:49:52 PDT 2011

   Member-id: 1
   ----------------------------------
   Partition               : 0:0 (/dev/ud1) **Default boot**
   Software Version        : ArubaOS 7.1.0.0 (Digitally Signed - Production Build)
   Build number            : 30977
   Label                   : 30977
   Built on                : Fri Nov 4 16:07:32 PDT 2011
   ----------------------------------
   Partition               : 0:1 (/dev/ud2)
   ```

```
Software Version        : ArubaOS 7.0.0.0 (Digitally Signed - Production Build)
Build number            : 28198
Label                   : 28198
Built on                : Wed May 4 15:49:52 PDT 2011
```

6. Reload the entire stack:

   ```
   (host) # reload
   ```

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

   ```
   (host)#show version member all
   Member-id: 0
   ------------
   Aruba Operating System Software.
   ArubaOS (MODEL: ArubaS3500-24P-US), Version 7.1.0.0
   Website: http://www.arubanetworks.com
   Copyright (c) 2002-2011, Aruba Networks, Inc.
   Compiled on 2011-11-04 at 16:07:32 PDT (build 30977) by p4build
   ...
   Member-id: 1
   ------------
   Aruba Operating System Software.
   ArubaOS (MODEL: ArubaS3500-24P-US), Version 7.1.0.0
   Website: http://www.arubanetworks.com
   Copyright (c) 2002-2011, Aruba Networks, Inc.
   Compiled on 2011-11-04 at 16:07:32 PDT (build 30977) by p4build
   ...
   ```

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

Upgrading from your USB using the LCD

CAUTION

If you are upgrading from ArubaOS 7.0.2.0 to ArubaOS 7.1.0.0 or greater, you cannot upgrade from an external USB device using the LCD screen. Use either the WebUI or the CLI to complete your upgrade.

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

NOTE

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

3. Insert your USB device into the rear USB port (next to the console port) of your mobility access switch.
4. Slowly press the **Menu** button until you reach the **Maintenance** function.
5. Press the **Enter** button to enter the maintenance function.

6. Press the **Enter** button at **Upgrade Image** function.
7. 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.

NOTE

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

8. 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
   ```

9. 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
   ```

NOTE

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.

10. From the command line, execute **show image version member all** to view the partitions:

```
((host)#show image version member all
Member-id: 0
-----------------------------------
Partition               : 0:0 (/dev/ud1) **Default boot**
Software Version        : ArubaOS 7.1.0.0 (Digitally Signed - Production Build)
Build number            : 30977
Label                   : 30977
Built on                : Fri Nov 4 16:07:32 PDT 2011
----------------------------------
Partition               : 0:1 (/dev/ud2)
Software Version        : ArubaOS 7.0.0.0 (Digitally Signed - Production Build)
Build number            : 28198
Label                   : 28198
Built on                : Wed May 4 15:49:52 PDT 2011

Member-id: 1
----------------------------------
Partition               : 0:0 (/dev/ud1) **Default boot**
Software Version        : ArubaOS 7.1.0.0 (Digitally Signed - Production Build)
Build number            : 30977
Label                   : 30977
Built on                : Fri Nov 4 16:07:32 PDT 2011
----------------------------------
Partition               : 0:1 (/dev/ud2)
Software Version        : ArubaOS 7.0.0.0 (Digitally Signed - Production Build)
Build number            : 28198
Label                   : 28198
```

```
Built on                : Wed May 4 15:49:52 PDT 2011
```

11. Reload the entire stack:

```
(host) # reload
```

12. Execute the **show version member all** command to verify the reload and upgrade is complete.

```
(host)#show version member all
Member-id: 0
------------
Aruba Operating System Software.
ArubaOS (MODEL: ArubaS3500-24P-US), Version 7.1.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-11-04 at 16:07:32 PDT (build 30977) by p4build
...
Member-id: 1
------------
Aruba Operating System Software.
ArubaOS (MODEL: ArubaS3500-24P-US), Version 7.1.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-11-04 at 16:07:32 PDT (build 30977) by p4build
...
```

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

After completing the upgrade, your system will create a configuration file call **default.cfg.<timestamp>**. This file is your configuration at the time of upgrade. Another file is created called **default.cfg**, which is your configuration post-upgrade.

Downgrading after an Upgrade

If necessary, you can return to your previous version.

NOTE

Save your configuration file before and after completing your downgrade.

NOTE

MSTP will be disabled upon downgrading.

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. By default, ArubaOS creates a file called **original.cfg** upon upgrade. This file can be used instead of a previously-saved configuration file in case you did not save your configuration before upgrade.

   Use the **dir** command to confirm your saved configuration files or original.cfg.

```
(host)#dir
-rw-r--r--    1 root     root         3710 Nov  7 14:35 default.cfg
-rw-r--r--    2 root     root         3658 Nov  7 14:35 default.cfg.2011-11-07_1
-rw-r--r--    2 root     root         3658 Nov  7 14:35 original.cfg
```

Use the **boot config-file <filename>** command to select the configuration file you will boot from after downgrading.

```
(host)#boot config-file original.cfg
```

Confirm that you have selected the correct file using the **show boot** command.

```
(host)#show boot
Config File: original.cfg
Boot Partition: PARTITION 0
```

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.