ArubaOS 7.2.2

ARUBA® networks

Release Note

Copyright

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.

ARUBA®
networks

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1

Release Overview

ArubaOS 7.2.2 is a software maintenance release for the Mobility Access Switch (MAS) product line that introduces fixes to previously outstanding issues. For details on all the features supported on Mobility Access Switch, see the Related Documents section

This release note contains the following chapters:

- Chapter 2, "What's New in This Release" on page 9—describes the new content introduced in this release including new features, fixed issues, and newly identified issues
- Chapter 4, "Issues Fixed in a Previous Release" on page 29—a listing of fixed issues introduced in a previous 7.2.x release
- Chapter 5, "Known Issues Found In a Previous Release" on page 35—a listing of known issues organized by functionality in a previous 7.2.x release
- Chapter 6, "Upgrade Procedures" on page 45— instructions on how to upgrade your software

Supported Browsers

The WebUI supports the following browsers:

- 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 7.2 User Guide*
- *ArubaOS 7.2 Command Line Reference Guide*
- *ArubaOS 7.2 Quick Start Guide*
- *ArubaOS S1500 Series Mobility Access Switch Installation Guide*
- *ArubaOS S3500 Series Mobility Access Switch Installation Guide*
- *ArubaOS S2500 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

Chapter 2

What's New in This Release

This chapter provides a list of all the bugs fixed and new known issues identified in this release, as well as a brief summary of the new features included in this version of ArubaOS.

Support for S1500 Mobility Access Switch

This release of ArubaOS provides support for S1500-24P and S1500-48P Mobility Access Switch products:

S1500-24P—The S1500-24P Mobility Access Switch is a 24 port 10/100/1000BASE-T plus four fixed 1000BASE-x SFP ports. The S1500-24P supports IEEE 802.3af/IEEE802.3at PoE/PoE+ on each port, with total PoE budget of up to 400W

S1500-48P—The S1500-48P Mobility Access Switch is a 48 port 10/100/1000BASE-T plus four fixed 1000BASE-x SFP ports. The S1500-48P supports IEEE 802.3af/IEEE802.3at PoE/PoE+ on each port, with total PoE budget of up to 400W.

The S1500 Mobility Access Switch requires a minimum of ArubaOS 7.2.2 to operate. It supports a similar software feature set to that of S2500 and S3500 Mobility Access Switch. *See* Table 1 for a comparison of S1500 with the other Mobility Access Switch platforms.

Table 1 *Features Supported on Mobility Access Switch platforms*

Features Supported	S1500	S2500	S3500
10/100/1000BASE-T ports	24 or 48	24 or 48	24 or 48
Uplink Ports	4x SFP	4x SFP/SFP+	4x SFP/SFP+
PoE/PoE+ on 10/100/1000 ports	Yes	Yes	Yes
PoE Budget	400W	400W	Up to 1440W
Non-PoE models	No	Yes	Yes
Performance (24 port model) Performance (48 port model)	56 Gbps/ 41.5 Mpps 104 Gbps/ 77 Mpps	128 Gbps/ 95 Mpps 176 Gbps/131 Mpps	128 Gbps/ 95 Mpps 176 Gbps/131 Mpps
Stacking	Roadmap, Beta support in 7.2.2 **NOTE:** For more information, *see ArubaOS S1500 Series Mobility Access Switch Installation Guide*.	Yes, up to 8 members	Yes, up to 8 members
Layer 2 Features	All ArubaOS 7.x features	All ArubaOS 7.x features	All ArubaOS 7.x features
MAC Scaling	8K	12K	12K
VLANs	4094	4094	4094
QoS HW queues	4	8	8

Table 1 *Features Supported on Mobility Access Switch platforms*

Features Supported	S1500	S2500	S3500
Layer 3 Features	All ArubaOS 7.x features	All ArubaOS 7.x features	All ArubaOS 7.x features
Security Features	All ArubaOS 7.x features	All ArubaOS 7.x features	All ArubaOS 7.x features
WebUI	All ArubaOS 7.x features	All ArubaOS 7.x features	All ArubaOS 7.x features
LCD System Status Panel	No (Status via LEDs)	Yes	Yes
Console Port	Yes	Yes	Yes
Ethernet Management Port	No	Yes	Yes
USB	Yes	Yes	Yes
Redundant Power	No	No	Yes
Field replaceable fan tray	No	No	Yes
Dimensions (HxWxD) in	1.75x17.5x12.5	1.75x17.5x12.5	1.75x17.5x17.5
Minimum ArubaOS Version Supported	ArubaOS 7.2.2	ArubaOS 7.1.2	ArubaOS 7.0.0

WebUI Enhancements

This release of ArubaOS includes the following enhancements to the WebUI:

- The Monitoring tab is renamed to Dashboard.
- A new Diagnostics tab is introduced to include the diagnostics functionality.

Fixed Issues

The following bugs have been fixed in this version of ArubaOS 7.2.2. For a list of bugs fixed in previous releases of ArubaOS 7.2.x, see Chapter 4, “Issues Fixed in a Previous Release” on page 29.

Base OS Security

Table 2 *Fixed Base OS Security Issues*

Bug ID	Description
51952	**Symptom:** Loopguard, rootguard, and portfast could be enabled together on an MSTP/PVST profile even though they are mutually exclusive. The following error message is now displayed if you try to enable any of them together: ***Error: rootguard, loopguard & portfast are mutually exclusive*** **Scenario:** This issue is not specific to any Mobility Access Switch platform.
58177	**Symptom:** The root path cost information was not displayed by the `show spanning-tree` command when PVST was enabled. Executing the `show spanning-tree vlan` command now displays the root path cost information of the spanning tree. **Scenario:** This issue is not specific to any Mobility Access Switch platform.
79415	**Symptom:** When a client passed the 802.1x user authentication, any cached entry for the client in the local user database was refreshed. The cached entry for the client no longer gets refreshed with a successful 802.1x user authentication. **Scenario:** This issue was observed when machine authentication was enabled under 802.1x profile. This issue is not specific to any Mobility Access Switch platform.
80601	**Symptom:** When a duplicate entry of a client in unreachable-role aged-out in the user table, the corresponding MAC entry in the mac-in-unreachable-role table was removed. The MAC entry no longer gets removed from the mac-in-unreachable-role table as long as there is at least one entry for the client in the user table. **Scenario:** This issue was observed when a client in unreachable-role had a duplicate entry in the user table. This issue is not specific to any Mobility Access Switch platform.

Captive Portal

Table 3 *Fixed Captive Portal Issues and Limitations*

Bug ID	Description
74540	**Symptom:** The **Preview Current Settings** link in the WebUI under the **Configuration > Captive Portal** page did not display the new changes configured. **Scenario:** This issue was observed when Captive Portal Profile was configured with customized logo or background image or custom html page in the WebUI. This issue is not specific to any Mobility Access Switch platform.

Configuration

Table 4 *Fixed Configuration Issues*

Bug ID	Description
78868	**Symptom:** The `show neighbor-devices` command did not display the capability details of the neighboring LLDP and CDP devices. The command output now displays the capability information of the connected LLDP and CDP enabled peers. **Scenario:** This issue is not specific to any Mobility Access Switch platform.
82200	**Symptom:** To remove a subset of existing ports from the interface group, the `apply-to remove` command accepted only the entire set of ports and not a specific range of ports. You can now remove any range of ports from the interface group using the `apply-to remove` command. **Scenario:** This issue was observed when the apply-to remove command was used to remove a specific range of uplink ports. This issue is not specific to any Mobility Access Switch platform.

Layer 2 Forwarding

Table 5 *Fixed Layer 2 Forwarding Issues*

Bug ID	Description
80862	**Symptom:** The untagged traffic was dropped on the trunk port. The untagged membership has been added to the VLAN member to resolve this issue. **Scenario:** This issue was observed when the native VLAN was dynamically created using GVRP (GARP VLAN Registration Protocol). This issue is not specific to any Mobility Access Switch platform.
81402	**Symptom:** The layer 2 module crashed when MSTP tracing was enabled. MSTP tracing can now be enabled without a layer 2 module crash. **Scenario:** This issue was observed when the peer switches sent older versions of PDUs. This issue is not specific to any Mobility Access Switch platform.
81526	**Symptom:** LACP profile configuration was allowed on a hot standby link (HSL) backup interface. The following error message is now displayed when you try to configure an LACP profile on an HSL back-up interface: **Error: Backup interface is part of portchannel interface** **Scenario:** This issue is not specific to any Mobility Access Switch platform.

Logging

Table 6 *Fixed Logging Issues*

Bug ID	Description
60888	**Symptom:** The `show log all` command displayed incomplete log information when executed with a filter. This command now displays the complete logs. **Scenario:** This issue was observed when the command, `show log all` was executed with any of the filters, begin, include, or exclude. This issue is not specific to any Mobility Access Switch platform.
78622	**Symptom:** No logging was done to the Syslog when the user changed the Spanning Tree mode. A Syslog message with a logging level WARNING is now logged when the user changes the Spanning Tree mode. **Scenario:** This issue is not specific to any Mobility Access Switch platform.

OSPF

Table 7 *Fixed OSPF Issues*

Bug ID	Description
80395	**Symptom**: Layer 3 module restarted occasionally when OSPFwas disabled. Layer 3 module no longer gets restarted when OSPF is disabled. **Scenario**: This issue was observed when OSPF was disabled by executing the `no ip address` command followed by the `no router ospf` command. This issue is not specific to any Mobility Access Switch platform.

PoE

Table 8 *Fixed PoE Issues*

Bug ID	Description
83421	**Symptom:** Wrong value was indicated as the PoE budget when the `show poe controller` command was executed. The output of the command now shows the correct value which is 1465 W. **Scenario:** This issue was observed when this command was executed with two PSUs of 1050 W each was connected to the S3500—48PMobility Access Switch. **NOTE:** Although the PoE budget value is 1465 W, a maximum of 30 W per port is supported on all the 48 ports.

Switch-Platform

Table 9 *Fixed Switch-Platform Issues*

Bug ID	Description
80304	**Symptom:** The output of the `show poe interface gigabitethernet x/y/z` command displayed the power management as static for a brief period (approximately 5 seconds), even though it was configured as dynamic. **Scenario:** This issue was observed when this command was executed after disabling and enabling PoE under the poe-profile. This issue is not specific to any Mobility Access Switch platform.

Chapter 3

Features Added in a Previous Release

The following features were added in a previous version of ArubaOS 7.2.x:

RADIUS Fail-Open

When wired users try to access a network where AAA servers are unreachable, they will be unable to authenticate and will continue to stay in the configured initial role. As a result, a user may effectively be blocked off the network due to a restrictive initial-role. To overcome this problem, ArubaOS provides support for RADIUS Fail-open. This feature enables the IT administrators to provide an alternate user-role (*unreachable-role*) to the users for network connectivity during a AAA server outage. When AAA servers are unreachable, the RADIUS Fail-open feature assigns the *unreachable-role* to the users trying to authenticate. The users will stay in the *unreachable-role* until at least one of the AAA servers is back in service.

Enabling RADIUS Fail-Open

RADIUS Fail-open is an optional configuration. It is enabled only if:

- the *unreachable-role* is configured under the AAA profile, and
- the AAA server dead time expiry feature is enabled (i.e. the dead time value is set above 0)

Configuring Unreachable Role

Use the following command to configure the *unreachable-role*:

```
(host) (config) #aaa profile profile1
(host) (AAA Profile "profile1") # unreachable-role <user-role>
```

The following is a sample configuration:

```
(host) (config) #aaa profile profile1
(host) (AAA Profile "profile1") # unreachable-role new-role
```

Verifying Unreachable Role Configuration

You can use the following commands to verify the *unreachable-role* configuration:

```
(host) #show aaa profile profile1

AAA Profile "profile1"
-------------------
Parameter                              Value
---------                              -----
Initial role                           logon
MAC Authentication Profile             N/A
MAC Authentication Default Role        guest
MAC Authentication Server Group        N/A
802.1X Authentication Profile          dot1x-auth-profile
802.1X Authentication Default Role     default-role
802.1X Authentication Server Group     server-group
Download Role from ClearPass           Enabled
L2 Authentication Fail Through         Disabled
RADIUS Accounting Server Group         N/A
RADIUS Interim Accounting                   Disabled
XML API server                              N/A
AAA unreachable role                        new-role
RFC 3576 server                             N/A
User derivation rules                       N/A
SIP authentication role                     N/A
Enforce DHCP                                Disabled
Authentication Failure Blacklist Time       3600 sec
(host)# show running-config
...
...
...
aaa profile "profile1"
authentication-dot1x "dot1x-auth-profile"
dot1x-default-role "default-role"
dot1x-server-group "server-group"
unreachable-role "new-role"
...
...
...
```

Key Points to Remember

- A client remains in the initial role until all the AAA servers in the server group are processed. The *unreachable-role* is assigned to a user only when:
  - no intermediate role (such as UDR, MAC auth, and 802.1x machine-auth-machine-role) has been derived i.e. the user is still in initial role, and
  - the last AAA server in the AAA server group has been processed, and
  - if one or more AAA servers have timed out and the rest have failed the authentication, or if all the servers have timed out.

NOTE

A role derived after authenticating UDR or MAC auth will have more privileges than the initial or *unreachable-role*.

- A client will transition from the switch profile VLAN to AAA *unreachable-role*-based-VLAN only if:
  - AAA *unreachable-role* is assigned to that MAC, and
  - no intermediate VLAN has been derived.

NOTE

AAA *unreachable-role*-based-VLAN (high priority) takes precedence over the switching profile's VLAN (low priority).

- Clients that attempted AAA authentication and got timed out are added to the mac-in-unreachable-list table. This list also includes the clients that have derived an intermediate role (such as UDR and MAC auth) but failed AAA authentication due to time-out.

You can use the following command to view the list of clients in the *unreachable-role*:

```
(host) #show aaa mac-in-unreachable-list
Station Entry
-------------
       MAC          AAA profile Name  AAA server Group           Port
-----------------  ----------------  ----------------  --------------------
00:60:6e:00:f1:7d  dot1x             mac               gigabitethernet0/0/7

Entries: 1
```

- When the dead timer has expired (default 10 minutes), the Mobility Access Switch sends a dummy authentication request to the AAA server (username: DummyArubaUser). When the AAA server comes back in service, all the clients corresponding to that server group are cleared from the mac-in-unreachable-list table. The clients then re-attempt authentication.
- When a client is removed from the mac-in-unreachable-list table, the port to which it is connected is administratively disabled (shutdown) and then re-enabled (in 5 seconds). This is to ensure that the client initiates the DHCP process again when it re-attempts authentication. The port is administratively disabled and then re-enabled in the following scenarios:
  - When all the clients on the same port are removed from the mac-in-unreachable-list table, if there are more than one client on the same port.
  - When `aaa user delete` command is executed to delete a client entry that is in the mac-in-unreachable-list table.

> NOTE
>
> The port does not get shut when the client entry that is in the *unreachable-role* ages out due to AAA timer expiry.

- If the AAA server dead time expiry is set to 0, the clients that are in the *unreachable-role* are rolled back to initial role and are removed from the mac-in-unreachable-list table. No clients will be assigned the *unreachable-role* as RADIUS Fail-open gets disabled.
- If a system switch over happens (the secondary switch becomes the new primary and the primary switch becomes the new secondary) in the network while RADIUS Fail-Open is active, the following process takes place:
  - The servers that were marked out of service in the old primary are marked as in-service in the new primary.
  - The user table entries for the clients that were in mac-in-unreachable-list table are deleted and their respective interfaces are administratively disabled and then re-enabled. These clients re-attempt authentication and derive a role based on the authentication outcome.
  - If the servers are still out of service during the authentication re-attempt, they will be marked as out of service.
- When more than one server is configured under a server group and when server-group fail-through option is disabled, then the *unreachable-role* is assigned to the user only if:
  - all the servers are out of service, or
  - when all the servers except the last one in the server group are out of service and the last one fails authentication.

Limitations

- RADIUS Fail-Open is not supported when re-authentication timer is enabled.
- RADIUS Fail-Open is not supported when EAP-Termination is enabled under 802.1x authentication profile.
- Radius Fail Open is not supported for Captive Portal Authentication.

Auto Configuration Enhancement

Auto Configuration is a mechanism which is used to download a configuration file from the TFTP server through DHCP server options (option-67). In a large deployment, when the configuration file name is specified in the DHCP server option, all the Mobility Access Switch in the network will download the same configuration file.

This release of ArubaOS provides a mechanism for Auto Configuration to download a unique configuration file for each Mobility Access Switch in a large deployment. When the configuration file name (option-67) is not configured in the DHCP server option, the Mobility Access Switch automatically downloads a configuration file with its serial number as the name (Example: AU0000234.cfg).

Key Points to Remember

You must ensure that:

- the IP address of the TFTP server (option-150) is configured in the DHCP server options, and
- all the required configuration files are present in the specified TFTP server with the correct naming convention, <SERIAL-NUMBER>.cfg.

NOTE

The configuration file name is case-sensitive.

ArubaStack Enhancements

This release of ArubaOS introduces the following enhancements to ArubaStack:

- Enables the base ports to be configured as ArubaStack ports for specific topologies. You can use the following command to configure the base ports as ArubaStack:

  ```
  add stacking interface stack <module/port>
  ```

  To delete a stacking port, execute the following command locally as it cannot be completed from the primary:

  ```
  delete stacking interface stack <module/port>
  ```

NOTE

Use module=0 for base ports. For more information on adding a stacking interface, see *ArubaOS 7.2 Command Line Interface Guide*.

- Provides support for increased number of ArubaStack topologies.
- Provides support for the following use cases:
  - ArubaStack using base port links
    - Creating an ArubaStack with 10/100/1000 base ports
    - Creating an ArubaStack with S3500-24F base ports

    - Creating an ArubaStack across multiple wiring closets
- ArubaStack distributed wiring closet with redundancy
    - Creating an ArubaStack across two wiring closets with two layer redundancy

All the use cases are supported only with the exact interconnections as illustrated in the figures 1 to 4 provided in this document.

ArubaStack using Base Port Links

The following use-cases are supported under ArubaStack using base port links:

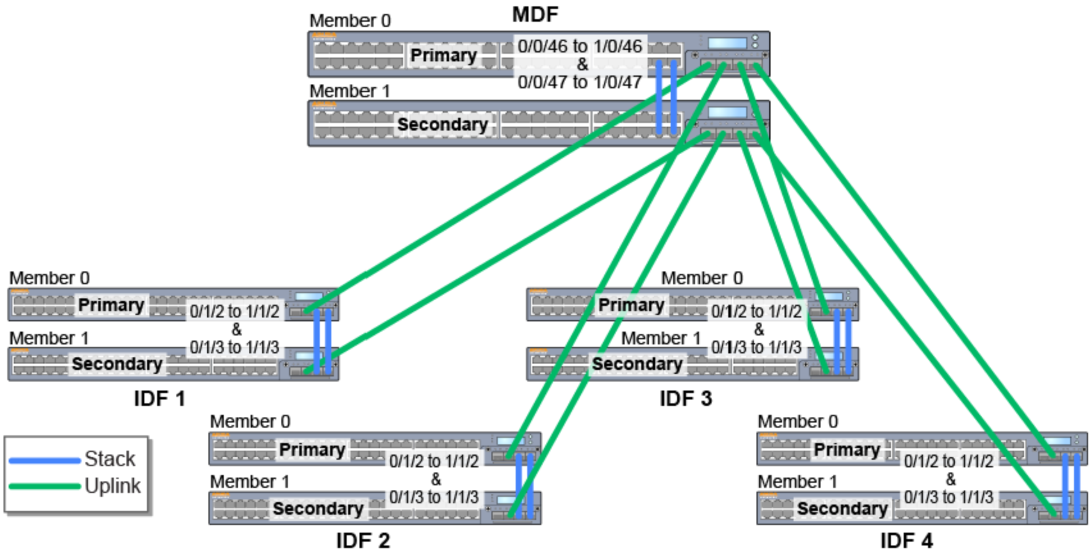
- Creating an ArubaStack with 10/100/1000 base ports
- Creating an ArubaStack with S3500-24F base ports
- Creating an ArubaStack across multiple wiring closets

All the ArubaStack using base port links support reduced ArubaStack bandwidth in MDF.

Creating ArubaStack with 10/100/1000 Base Ports

Figure 1 illustrates how to create an ArubaStack with 10/100/1000 base ports. This is useful when all the uplink ports are used for interconnecting with devices in the other locations.

Figure 1 *ArubaStack with 10/100/1000 Base Ports*



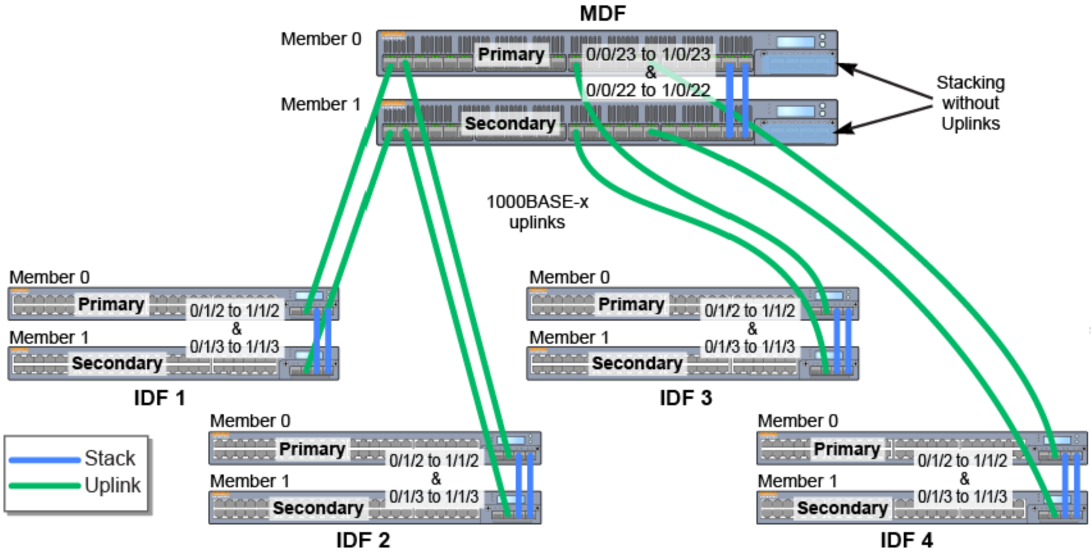
The characteristics of this topology are described below:

- Full redundancy is provided between every ArubaStack.
- Provides 1000BASE-T PoE on every ArubaStack.
- 1000Base-X (fiber) uplinks to MDF connect to the uplink ports.
- MDF stack is completed by 1000BASE-T base port links.
- x/0/x ports are stacked only with other x/0/x ports at MDF.

Creating ArubaStack with S3500-24F Base Ports

Figure 2 illustrates how to create an ArubaStack with S3500-24F base ports. This physical configuration is used to create a redundant S3500-24F aggregation layer without an uplink module.

Figure 2 *ArubaStack with S3500-24F Base Ports*



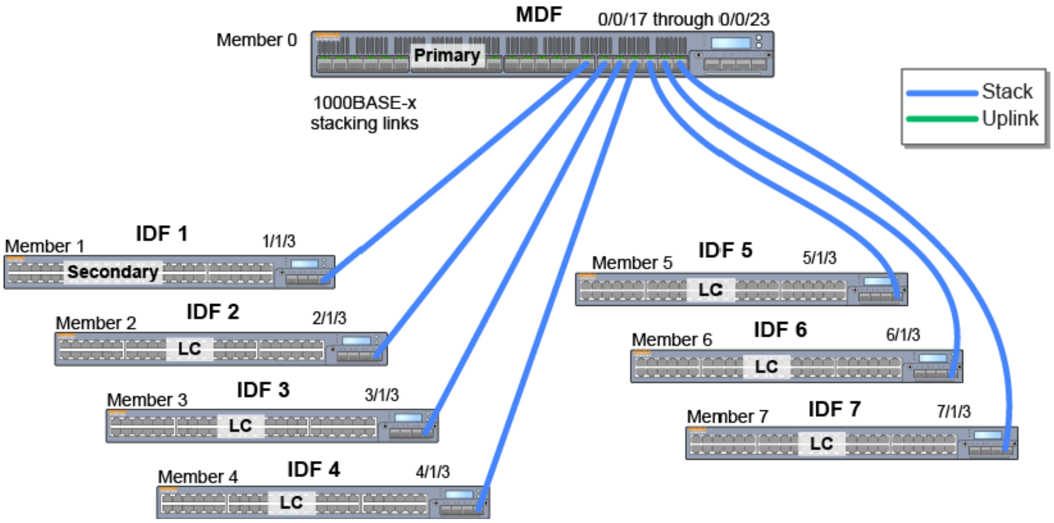
The characteristics of this topology are described below:

- Full redundancy is provided between every ArubaStack.
- No uplink module is required at MDF.
- 1000Base-X (fiber) uplinks to MDF connect to 1000Base-X base ports.
- MDF stack is completed by 1000BASE-X base port links.
- x/0/x ports are stacked only with other x/0/x ports at MDF.

Creating ArubaStack across Multiple Wiring Closets

Figure 3 illustrates how to create an ArubaStack across multiple wiring closets. This is an alternative star topology used for multiple remote wiring closets instead of the traditional ring topology.

Figure 3 *ArubaStack across Multiple Wiring Closets*



The characteristics of this topology are described below:

- MDF and IDFs are integrated as one ArubaStack for simplified management.
- 1000Base-X Fiber extends ArubaStack to a longer distance.
- No uplink module is required at MDF.
- 1000Base-X (fiber) uplinks to MDF connect to 1000Base-X base ports.
- A maximum of 7 ArubaStack ports are allowed at MDF (S3500-24F shown).

NOTE

This topology does not provide ArubaStack redundancy for stack members.

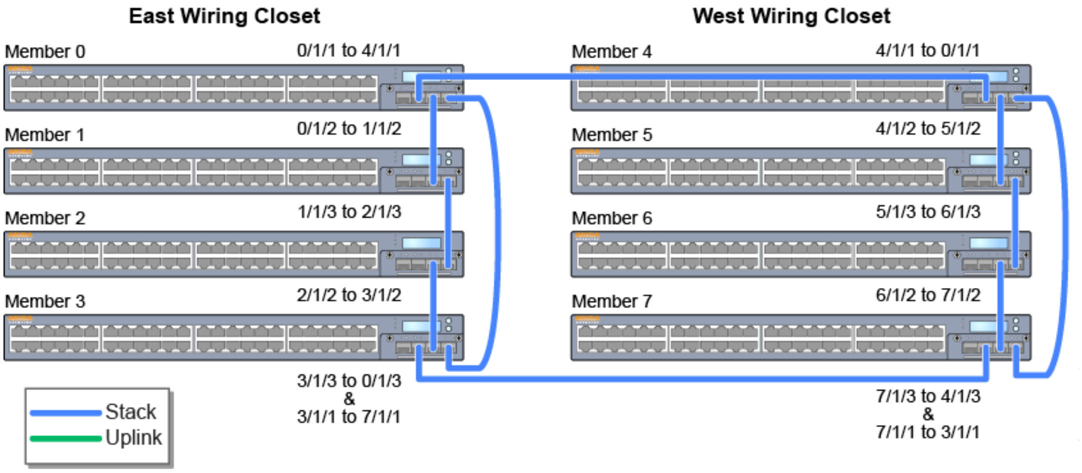
ArubaStack Distributed Wiring Closet with Redundancy

You can create an ArubaStack across two wiring closets with two layer redundancy. This use case provides redundancy through the traditional ring topology between the members within the wiring closet. It also provides a redundant ring between the members across the distributed wiring closets.

Creating ArubaStack across Two Wiring Closets with Two Layer Redundancy

Figure 4 illustrates how to create an ArubaStack across two wiring closets with two layer redundancy.

Figure 4 *ArubaStack across Two Wiring Closets with Two Layer Redundancy*



The characteristics of this topology are described below:

- Primary member is in one closet and the secondary is in the other.
- DAC is provided between the members within the closet and 10GE is provided between the closets.
- Full redundancy is provided in each wiring closet
- Full redundancy is provided between closets
- Provides simplified management.
- Redundant uplink interfaces are available to core.

PoE Compatibility with CISCO Legacy Devices

CISCO's legacy IP phone models such as 7940 and 7960 use a pre-standard Power Over Ethernet (PoE) detection mechanism and may not get powered up when connected to the Mobility Access Switch (MAS) PoE models. This release of ArubaOS introduces the functionality to provide PoE compatibility with CISCO legacy IP phones. By default, this function is disabled. If you enable this function, the Mobility Access Switch changes the detection mechanism to give power to the CISCO legacy IP phones.

Execute the following commands to enable this functionality under the PoE management profile:

```
(host) (config) #poe-management-profile slot <slot number 0-7>
(host) (poe-management profile "<slot number 0-7>") #cisco-compatibility
```

Execute the following command to disable this functionality:

```
(host) (poe-management profile "<slot number 0-7>") #no cisco-compatibility
```

Limitations

- The `cisco-compatibility` option is per stack member (slot) and not per port, i.e. if you configure this option it applies to the entire slot.
- When `cisco-compatibility` is disabled, the Mobility Access Switch continues to provide power to the CISCO legacy devices until that device is unplugged or the Mobility Access Switch is reloaded.
- When cisco-compatibility is enabled, Mobility Access Switch may provide PoE to any detected CISCO legacy switch with pre-standard PoE. It is recommended not to connect a CISCO legacy phone and legacy switch on the same slot.

Layer-2 and Layer-3 Enhancements

Multinetting

ArubaOS supports multiple IP addresses per VLAN and loopback interface. You can specify any number of of secondary IP addresses. Secondary IP address can be used in a variety of situations, such as the following:

- If an insufficient number of host addresses are available on a particular network segment. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet
- If the an older network is built using Layer 2 bridges and has no subnetting. Secondary addresses can aid in the transition to a subnetter, router-based network.
- Two subnets of a single network might be otherwise seperated by another network. You can create a single network from sunets that physically seperated by another network using a secondary address.

Important Points to Remember

- OSPF advertises the secondary IP address in the router LSA but it does not form adjancency on the secondary IP address.
- PIM will not send hello packets on the secondary IP address.
- DHCP servers identify the subnets associated with secondary IP addresses used for allocation.

IP Prefix List

The ip prefix-list command is used to configure IP prefix filtering. Prefix lists are used to either permit or deny the configured prefix based on the matching condition. The prefix list consists of an IP address and a bit mask. The IP address can be classful network, a subnet, or a single host route. IP Directed Broadcast

IP Directed Broadcast

This release of ArubaOS Mobility Access Switch introduces IP Directed Broadcast. An IP directed broadcast is typically used by network management systems (NMS) for features like Wake On LAN to broadcast packets on a local subnet even though the source of that broadcast is located on a remote subnet.

When the source device initiates this broadcast packet, it is routed through the network as a unicast packet until it reaches the target subnet. Other than the router directly attached to the target subnet, all routers across the network view it as a unicast packet. The router directly attached to the target subnet identifies the packet as a directed broadcast, converts it to a link-layer broadcast packet and propagates it across the target subnet.

Route Metrics

The Mobility Access Switch provides support for Route Metrics. For a given route destination, there can be multiple nexthops. A route metric enables the Mobility Access Switch to prefer one route over another or load balance when the metric is the same.

A route destination with a lower metric is added to the route manager. The higher metric routes are added only when the lower metric routes are removed.

Equal Cost Multipath Support

Equal Cost Multipath (ECMP) enables Mobility Access Switch to forward the data packets to any of the multiple nexthops of a routing destination. The route manager identifies the best routing destination based on the priority of the protocol. After the route manager identifies the best route, all the nexthops of that route are used for datapath forwarding.

ECMP provides flow-based load balancing for the chosen routing destination. For a given flow same nexthop is used to forward all the packets. For multiple flows, load balancing happens across multiple nexthops. ECMP uses the source IP and destination IP to define a flow. For TCP/UDP packets, it also uses the source and destination ports to define the flow.

Apart from multiple nexthops, ECMP also enables addition of metric for a route. ECMP nexthops are per metric basis. For a given metric, there can be multiple nexthops (up to 4). A route with a lower metric is added to the route manager. The higher metric routes are added only when the lower metric routes are deleted.

OSPF Area Types

This release of ArubaOS Mobility Access Switch supports all Open Shortest Path First (OSPF) area types including Totally Stubby Area (TSA) and Not-So-Stubby-Area (NSSA).

NAT Support on VLAN Interfaces

Aruba Mobility Access Switches support source Network Address Translation (NAT) with Port Address Translation (PAT) on VLAN interfaces. When source NAT is enabled on a VLAN interface, the IP address of the egress VLAN interface as determined by the routing table will be used as the source IP. For example, if "ip nat inside" is enabled on interface VLAN X and traffic will be routed out interface vlan Y, the IP address of interface VLAN Y will be used as the source IP for traffic from VLAN X.

Bridge Protocol Data Unit (BPDU) Guard

This release of ArubaOS Mobility Access Switch supports BPDU guard functionality, which prevents malicious attacks on edge ports. When the malicious attacker sends a BPDU on the edge port, it triggers unnecessary STP calculation. To avoid this attack, use the BPDU guard on that edge port. BPDU guard enabled port shuts down as soon as a BPDU is received.

Support for GARP VLAN Registration Protocol (GVRP)

In this release of ArubaOS, support for GARP VLAN Registration Protocol (GVRP) is added. Configuring GVRP in Mobility Access Switch enables the switch to register/de-register the dynamic VLAN information received from a GVRP applicant such as an IAP in the network. GVRP support also enables the switch to propagate the registered VLAN information to the neighboring bridges in the network.

L2-GRE Tunnel

This release of ArubaOS Mobility Access Switch supports L2 connectivity through Generic Routing Encapsulation (GRE) tunnel. L2-GRE tunnel extends VLANs across Mobility Access Switches and Aruba controllers. GRE encapsulates Layer-2 frames with a GRE header and transmit through an IP tunnel over the could.

Security Features

Captive Portal

Captive portal is one of the methods of authentication supported by the Mobility Access Switch. A captive portal presents a web page, which requires user action, before network access is granted. The required action can be simply viewing and agreeing to an acceptable user policy, entering Email ID, or entering a user ID and password, which must be validated against a database of authorized users.

NOTE

Captive Portal authentication is not supported for users behind a router.

RADIUS Change of Authorization

The following command configures a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576, "Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS)".

VoIP Auto-discovery on Untrusted Ports

This release of Mobility Access Switch automatically discovers the Cisco Discovery Protocol (CDP) phones on an untrusted interface and assigns a VoIP VLAN to the phone. For more details on configuring CDP auto-discovery on an un-trusted port, see *ArubaOS 7.2 User Guide*.

Branch Office Features

Site-to-Site VPN

This release of ArubaOS Mobility Access Switch supports Site-to-Site Virtual Private Network (VPN), which allows sites at different physical locations to securely communicate with each other over a Layer 3 network.

The following IKE SA authentication methods are supported for site-to-site VPNs:

- Certificate authentication
- Preshared Key authentication
- Digital certificates: You can configure a RSA server certificate and a CA certificate for each site-to-site VPN IPsec map configuration. If you are using certificate-based authentication, the peer must be identified by its certificate subject-name distinguished name (for deployments using IKEv2) or by the peer's IP address (for IKEv1).

NOTE

Certificate-based authentication is only supported for site-to-site VPN between two Aruba devices with static IP addresses. Additionally, Certificate-based authentication is also supported with dynamic IP addresses when IKEv2 is used.

Aruba Solutions

Aruba AirGroup Integration

Aruba AirGroup is a unique enterprise-class capability that leverages zero configuration networking to allow mobile devices to use services like the Apple AirPrint wireless printer service and the Apple AirPlay streaming service. These services use multicast DNS (mDNS) packets to locate devices and the services that those devices offer.

To ensure Wired and Wireless AirPrint/AirPlay devices can communicate with one another previously required all devices to be on the same Layer-2 network which may not be desirable. This release of ArubaOS Mobility Access Switch and ArubaOS 6.1.3.4-AirGroup for the Mobility Controller avoids that need by enabling the ability to just redirect mDNS traffic to a Mobility Controller regardless of VLAN. A simple rule on the MAS is used to redirect all incoming mDNS packets on a port to an L2-GRE tunnel which is then terminated on a Mobility Controller. This allows the Mobility Controller to handle the rest of the AirGroup functionality.

ClearPass Policy Manager Integration

This release of ArubaOS Mobility Access Switch and ClearPass Policy Manager (CPPM) 6.0 includes support for centralized policy definition and distribution. With this new release, ArubaOS Mobility Access Switch introduces downloadable roles. By using this feature, when CPPM successfully authenticates a user and the role is not defined in the Mobility Access Switch (MAS), the MAS can now automatically download the role attribute details from CPPM and assign the role to the client.

Current Limitations

CPPM does not perform any error checking to confirm accuracy in the configuration. Therefore, it is recommended that you review your CPPM policy before it is downloaded. It is recommended that the downloadable role description be copied from an existing configuration that has been tested to ensure the tree structure and the syntax in the enforcement profile are correct.

- Only attributes that are part of the commands listed below are accepted by MAS.
  - `netdestination`
  - `netservice`
  - `ip access-list stateless`
  - `user-role access-list stateless`
  - `user-role vlan`
- Any attributes that are referred to by a CPPM policy must be configured on the MAS before the policy is downloaded.
- An instance name (name of a whitelist role attribute like ‘netservice’, case-sensitive) should not match any CLI option nested under a command from the whitelist; and should not be a number or a combination of numbers and '.'. Example below are considered as invalid configuration and will cause CPPM download to MAS failed:

  ```
  netservice 'tcp' tcp 443
  netdestination 'alias'
  netdestination '10.1.5'
  ip access-list stateless '100'
  ```

  It is recommended that some naming convention similar to say the Hungarian Notation (mixture of upper and lower case letters in a single word) be used to avoid collisions with the CLI options in the role description.

Instant AP (IAP) Integration

The ArubaOS Mobility Access Switch can be provisioned to support IAP integration by plugging the Instant AP directly to the Mobility Access Switch (MAS) port.

NOTE

Aruba Instant AP Integration with the MAS is currently only supported on trusted ports.

The major IAP integration features are as follows:

PoE Prioritization - When an Instant AP is plugged directly into the MAS port, the MAS increases the PoE priority of the port. This is done only if the PoE priority is set by default in the MAS.

Rogue AP Containment - When a rogue AP is detected by Instant, it sends the MAC Address of the rogue AP to the MAS. The MAS blacklists the MAC address of the rogue AP and turns off the PoE on the port or the MAS installs a bridge entry with the source MAC command as `DROP` to discard the packets originating from or carried to the Rouge AP.

GVRP Integration - Configuring GVRP in the Mobility Access Switch enables the switch to register/de-register the dynamic VLAN information received from a GVRP applicant such as an IAP in the network. GVRP support also enables the switch to propagate the registered VLAN information to the neighboring bridges in the network.

SNMP Updates

This release of ArubaOS Mobility Access Switch provides support for new standard MIBs and Traps.

MIB Enhancements

Table 1 provides the list of new standard MIBs, tables supported in each MIB, and the scalars that are not supported in each of these MIBs:

Table 1 *Standard MIBs Supported*

MIB Name	Supported Tables	Scalars Not Supported
RMON2-MIB (RFC 4502)	● probeConfig	—

Table 1 *Standard MIBs Supported*

MIB Name	Supported Tables	Scalars Not Supported
HC-RMON-MIB (RFC 3273)	etherStatsHighCapacityGroup etherHistoryHighCapacityGroup	etherStatsHighCapacityOverflowPkts64Octets etherStatsHighCapacityPkts64Octets etherStatsHighCapacityOverflowPkts65to127Octets etherStatsHighCapacityPkts65to127Octets etherStatsHighCapacityOverflowPkts128to255Octets etherStatsHighCapacityPkts128to255Octets etherStatsHighCapacityOverflowPkts256to511Octets etherStatsHighCapacityPkts256to511Octets etherStatsHighCapacityOverflowPkts512to1023Octets etherStatsHighCapacityPkts512to1023Octets etherStatsHighCapacityOverflowPkts1024to1518Octets etherStatsHighCapacityPkts1024to1518Octets
OSPF-MIB	ospfGeneralGroup ospfAreaTable ospfStubAreaTable ospfIfTable ospfNbrTable ospfLsdbTable ospfExtLsdbTable	ospfDemandExtensions ospfIfDemand ospfNbmaNbrPermanence ospfNbrHelloSuppressed ospfStubMetric ospfImportAsExtern ospfNbmaNbrPermanence ospfNbrHelloSuppressed ospfIfAuthKey ospfExtLsdbAdvertisement ospfLsdbAdvertisement
ENTITY-MIB	entityGeneral entPhysicalTable entLogicalTable entAliasMappingTable entPhysicalContainsTable	entPhysicalMfgName entPhysicalAssetID entPhysicalUris entPhysicalHardwareRev entPhysicalAlias entPhysicalMfgDate entLPMappingTable

Trap Enhancements

Table 2 provides the list of new standard traps for OSPF-MIBand ENTITY-MIB:

Table 2 *Supported Standard Traps*

Supported Traps
ospfIfStateChange ospfNbrStateChange entConfigChange

Table 3 provides the list of new supported enterprise traps for WLSX-TRAP-MIB.

Table 3 *Supported Enterprise Traps*

Supported Traps
● wlsxIfStateChangeTrap (Enhanced for BPDU guard feature)

Issues Fixed in a Previous Release

The following issues have been fixed since the last release of ArubaOS 7.2.x.

Base OS Security

Table 1 *Fixed Base OS Security Issues*

Bug ID	Description
49140	A “permit any any” in an IP based ACL applied to a physical port used to allow non-IP traffic and a “deny any” in an IP-based ACL applied to a physical port used to deny non-IP traffic. Now with the fix for bug 82706, non-IP traffic is not impacted by the IP based ACLs applied to a physical port. When a Port ACL (PACL) was used to restrict IP connectivity, non-IP traffic was also impacted. To allow non-IP traffic, a “permit any any” ACE was needed after all the IP based ACEs. This issue is not specific to any Mobility Access Switch platform.
79128	An issue has been resolved when certain VLAN (ranging between 129-255 and every alternate 128 VLAN) were returned as Vendor Specific Attribute (VSA) from RADIUS, incorrect VLAN were derived for the clients.This issue was observed on Mobility Access Switch running ArubaOS 7.2.0 and is not specific to a Mobility Access Switch platform.
82706	IP based ACLs applied to a physical port blocked non-IP traffic as well. IP based ACLs are now applicable only to the IP based traffic on the physical ports. When a Port ACL (PACL) was used to restrict IP connectivity, non-IP traffic was also impacted. To allow non-IP traffic, a “permit any any” ACE was needed at the end of the IP based ACL after all the IP based ACEs. This issue is not specific to any Mobility Access Switch platform.

CPPM

Table 2 *Fixed CPPM Issues*

Bug ID	Description
74854	Roles downloaded from CPPM no longer fail if the whitelist includes 500+ ACE entries or 500+ host in netdestination, which exceeds 16k buffer size.
74892	Access-lists are no longer displayed multiple times repeatedly when more than 60 access-list entries are downloaded from CPPM.

Generic Routing Encapsulation

Table 3 *Fixed Generic Routing Encapsulation Issues*

Bug ID	Description
77222	An issue has been resolved where the traffic did not pass through an L2 GRE tunnel as the tunnel was created in untrusted mode. This occurred when a GRE tunnel was created, deleted, and then recreated.

Instant AP

Table 4 *Fixed Instant AP Issues*

Bug ID	Description
72910	An IAP no longer reboots when connected to a linecard of a stack, which becomes the secondary by changing election priority followed by a system switchover.

IPSec

Table 5 *Fixed IPSec Issues*

Bug ID	Description
79576	An issue has been resolved where the tunnel node traffic was getting dropped. This occurred when the trunk port was configured as the tunnel node port. This issue is not specific to a Mobility Access Switch platform.

Layer 2 Forwarding

Table 6 *Fixed Layer 2 Forwarding Issues*

Bug ID	Description
74338	When both L2GRE and tunneled-node is configured to the same controller, the L2GRE tunnel will come up, even if none of the tunneled-node sessions are UP (i.e. `show tunneled-node state` is not **complete** for all the ports).
74836	Multicast packet are correctly forwarded when the L2GRE tunnel VLAN has a IP address.

Layer 3 Routing

Table 7 *Fixed Layer 3 Routing Issues*

Bug ID	Description
74363	The number of entries under prefix-list is no longer limited to 300 or less.
74508	The default route injected into NSSA via default-route-originate with translate-always option now has the correct, configured metric-type.
74759	Any IP route change that should result in picking up a new egress route-path and new NAT'ed IP is correctly executed.
74847	The commands `show ip route static` or `show ip route ospf` no longer display VPN routes.
74888	The last entry of the previous page is no longer displayed again on the beginning of next page with different age when there is more than one page in the output of `show ip ospf database`.
75167	When NSSA is configured with `translate-always` option, the `translate-always` keyword can be saved to running-config and is no longer lost after reload.

Table 7 *Fixed Layer 3 Routing Issues (Continued)*

Bug ID	Description
78464	An issue has been resolved where executing the **`show arp`** command was causing file descriptor leaks. This occurred when the **`show arp`** command was executed. This issue is not specific to a Mobility Access Switch platform.

Link Layer Discovery Protocol

Table 8 *Fixed Link Layer Discovery Protocol Issues*

Bug ID	Description
76997	Executing the **`show neighbor-devices`** command no longer displays wrong information when the neighbor devices are Cisco devices. This occurred when the hostname of the Cisco device was more than 20 characters. This issue was observed on Mobility Access Switch running ArubaOS 7.2.0 and is not specific to a Mobility Access Switch platform.
78178	An issue has been resolved where the DSCP and dot1P values configured in the VoIP profile were not transmitted to the voice devices through LLDP. This occurred when the voice devices were connected to an untrusted interface. This issue was observed on Mobility Access Switch running ArubaOS 7.2.0 and is not specific to a Mobility Access Switch platform.

Logging

Table 9 *Fixed Logging Issues*

Bug ID	Description
76640	An issue has been resolved where the cm_trace.log file was getting filled very fast. This issue was observed on Mobility Access Switch running ArubaOS 7.2.0 and is not specific to a Mobility Access Switch platform.

Management Authentication and User Rights

Table 10 *Fixed Management Authentication and User Rights Issues*

Bug ID	Description
77291	An issue has been resolved where the incorrect NAS port type (Ethernet instead of Virtual) was sent to the RADIUS server when MSCHAPv2 was enabled under the management authentication profile. This issue was observed on Mobility Access Switch running ArubaOS 7.2.0 and is not specific to a Mobility Access Switch platform.

Power over Ethernet

Table 11 *Fixed PoE Issues*

Bug ID	Description
77474	An issue has been resolved where the Power over Ethernet (PoE) was down on an interface when **`QoS trust (auto|dscp|dot1p)`** was enabled on the interface. This issue was observed on Mobility Access Switch running ArubaOS 7.2.0 and is not specific to a Mobility Access Switch platform.

SNMP

Table 12 *Fixed SNMP Issues*

Bug ID	Description
75350	The SNMP engine time value of the authoritative messages no longer gets reset incorrectly. This issue was observed on Mobility Access Switch running ArubaOS 7.1.3 when the SNMP polling was done on a stack. This is not specific to a Mobility Access Switch platform.

Stacking

Table 13 *Fixed Stacking Issues*

Bug ID	Description
75224	A system switchover can successfully be executed immediately after a `write memory`.
78259	An issue has been resolved where a stack failure occurred due to multiple multicast routes in the system. This issue was observed on Mobility Access Switch running ArubaOS 7.1.3 or 7.2.0 and is not specific to a Mobility Access Switch platform.

Switch-Platform

Table 14 *Fixed Switch-Platform Issues*

Bug ID	Description
76338	An issue has been resolved where certain Cisco switches connected to S3500 and S2500 were powering down when Mobility Access Switch was rebooting. This issue was observed on Cisco switches (from 3750G) when the Mobility Access Switch was rebooting.
78828	The reload of devices no longer occurs due to lack of memory. This occurred when there were more than 50 OSPF neighbors in the system. This issue was observed on Mobility Access Switch running ArubaOS 7.2.0 and is not specific to a Mobility Access Switch platform.
81818	While rebooting, forming, or joining a device to an ArubaStack, the PoE devices such as APs and IP phones connected to some of the members went down as the PoE was disabled. The PoE no longer gets disabled during a stacking process. This is not specific to any Mobility Access Switch platform.

WebUI

Table 15 *Fixed WebUI Issues*

Bug ID	Description
76924	Setting the time zone to GMT in the WebUI, no longer displays the incorrect value (GMT - 12:00). This issue occurred when the time zone was set to GMT from the **Configuration > Basic Info** page in the WebUI. This issue was observed on Mobility Access Switch running ArubaOS 7.2.0 and is not specific to a Mobility Access Switch platform.

Chapter 5

Known Issues Found In a Previous Release

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

Uplink Module

NOTE

This issue only applies to the S3500 with an 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

Stacking

The members running a version older than ArubaOS 7.1.3 cannot become the members of ArubaStack.

Tunneled Node Controller-IP

ArubaOS 6.1.x does not currently support routing on a controller's loopback interface. With current controller function, if configuring a tunneled node controller-IP pointing to the controller's loopback interface, then a static route entry needs to be configured on the Mobility Access Switch. Or you can configure the tunneled node controller-IP pointing to a routable VLAN interface (RVI) on the controller.

Base OS Security

Table 1 *Known Base OS Security Issues*

Bug ID	Description
80192	When the primary switch is moved out of the stack and brought back in, authentication is not triggered for the clients connected to it. This issue is observed on Mobility Access Switch running ArubaOS 7.2.0 and is not specific to any Mobility Access Switch platform. **Workaround**: Once the stack is stabilized after the member is re-added, remove the untrusted port and AAA configuration from the interface of the member and add them back. If the configuration is inherited from the interface-group, remove the interfaces from the interface-group and add them back.

DHCP

Table 2 *Known DHCP Issues and Limitations*

Bug ID	Description
60298	DHCP discovery packets drop when the MAS is under heavy loads of traffic. **Workaround:** Reduce the traffic rate; this is not seen in regular normal operation.

IPv6

Table 3 *Known IPv6 Issues and Limitations*

Bug ID	Description
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.
60573	Duplicate IPv6 address detection is not supported. Connectivity issues may occur when duplicate IPv6 addresses are configured. **Workaround:** Take care not to configure duplicate IPv6 addresses.

Layer 2 Forwarding

Table 4 *Known Layer 2 Forwarding Issues and Limitations*

Bug ID	Description
57519	With Spanning Tree **loopguard** enabled, an interface will enter **LOOP_Inc** state if that interface is not receiving any more BPDU. When the situation happens, restart L2M daemon (such as doing stacking primary failover) may mistakenly bring the interface back to DES/FWD state. **Workaround:** Check your network when an interface enters **LOOP_Inc** state. Resolve your network problem before doing stacking primary failover or L2M restart. **NOTE:** A typical problem that causes an interface not to receive BPDU happens on the fiber connection in which TX is successful but RX fails.
58248	ICMP Redirect messages are not generated on VLAN interfaces. **Workaround:** None.
59597	Spanning Tree is automatically disabled after downgrading from ArubaOS 7.1.x to 7.0. **Workaround:** Manually enable MSTP after downgrading.
73285	The MAS does not register a GVRP VLAN on STP blocked ports. When there is a change in STP topology and the blocked port becomes forward,the port first register the vlan and then the data traffic flow can continue. Therefore, it will take a longer time to resume the traffic under these conditions. **Workaround:** None.

Table 4 *Known Layer 2 Forwarding Issues and Limitations (Continued)*

Bug ID	Description
75086	Forwarding multicast data packets into tunnels is rate-limited to 50pps if the forwarding happens solely based on igmp-snooping mrouter port detection. For example, no igmp-report based receiver detected on the tunnel. **Workaround:** Ensure there is at-least one IGMP-report based igmp-snooping membership for the multicast group.
75501	OSPF neighbors are not formed across L2 GRE tunnels. **Workaround:** None.
76422	The **clone** command under **interface tunnel** (L2 GRE) will not work if the source-ip and destination-ip of the source tunnel are configured. **Workaround:** Remove either source-ip or the destination-ip of the source tunnel.
76870	If you created a Tunnel Node on trunk port and a user VLAN was created on the MAS before enabling spanning tree, the tunnel traffic will be dropped. **Workaround :** Remove the user VLAN from the MAS and add it back if needed.

Layer 3 Routing

Table 5 *Known Layer 3 Routing Issues and Limitations*

Bug ID	Description
57090	OSPF link cost is not associated with the actual link bandwidth or interface type. **Workaround:** Configure interface cost under `interface-profile ospf-profile`.
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.
59085	Should not reform OSPF adjacency while changing OSPF priority. **Workaround:** None.
59572	Traceroute to and from a routing VLAN interface (RVI) fails if connecting to a non-primary member interface. **Workaround:** None.
59609, 59738	The maximum routes supported with this image is 1500 entries (routes). **Workaround:** None.
60033	Router-ID needs to be a valid unicast IP address. **Workaround:** Do not configure Router-ID to be multicast UP (224.0.0.0 ~ 239.255.255.255), or 128.x.x.x, or 240.0.0.0 ~ 255.255.255.255

Table 5 *Known Layer 3 Routing Issues and Limitations (Continued)*

Bug ID	Description
60804	The command `show ip ospf database detail` might display twice when executed. **Workaround:** None.
62038	When entering a router-id before executing clear ip ospf process and then entering the same router-id again, the clear ip ospf process warning will not be displayed even though clear ip ospf process is required for the new router-id to take effect. **Workaround:** None.
74123	With Source NAT enabled, no matter what MTU value is assigned to the RVI, packets up to 1784 bytes will be source NAT'ed. Packets larger than this are dropped on the ingress RVI because fragmentation not supported. Additionally, no matter what MTU is configured, packets leaving the egress RVI are not fragmented. **Workaround:** None.

Multicast

Table 6 *Known Multicast Issues and Limitations*

Bug ID	Description
58360	When the host is in IGMPv3 mode, the MAS will not forward packets to the host. **Workaround:** Configure the switch to be in igmp-snooping proxy mode.
58618	When multiple MAS connect over an extended VLAN, if the PIM-SM DR switch is different to IGMP Snoop Querier switch, then the traffic may flood on VLAN. **Workaround:** None.
61456	The MAS does not create (S,G) for multicast group address range for SSM (232.0.0.0 - 232.255.255.255). Traffic will not be up for these groups. **Workaround:** None.
63951	MLD reports on un-trust ports are ignored. Therefore, mld-snooping membership table will not be formed. IPv6 on untrust port is not supported in this release. **Workaround:** None.
65314	The S3500 does not send query on xSTP topology change. This delays the formation of the MLD-snooping membership table. **Workaround:** None.

OSPF

Table 7 *Known OSPF Issues*

Bug ID	Description
80395	**Symptom**: L3M restarts occasionally when OSPF is disabled by executing `no ip address` command followed by `no router ospf` command. **Scenario**: This issue is observed on Mobility Access Switch running ArubaOS 7.2.0 and is not specific to any Mobility Access Switch platform. **Workaround**: First disable OSPF by executing `no router ospf` and ensure that all the OSPF routes are removed before executing `no ip address` command.

QoS

Table 8 *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.

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 reauthentication under 802.1X authentication profile to make machine auth and user auth to work.
48692	The `MAC-Limit` parameter under the command `show interface-config gigabitethernet` does not support untrusted interfaces. **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 an L2 ACL that specifically blocks all L2 traffic.
49262	If the same IP address is used by two clients on different VLANs, the MAS 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.

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

Bug ID	Description
51168, 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 MAS is rebooted. **Workaround:** Use server certificate that has certificate request generated from Certificate WebUI only.
56900	In some cases, the command `show trace-buf` might not track all `rad acct start` information. **Workaround:** None.
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 also use `aaa user delete` to remove the original VLAN entry before timeout.
65520	When a user connects to a port with more than one role configured (initial role and a "final" role) and there is heavy traffic on that port, the user may be placed in the wrong role even if it meets the requirements based on the UDR. This is caused by improper packet processing due to the heavy traffic. **Workaround:** None.
66160	Windows XP clients may get an IP address from the initial VLAN (instead of the final authenticated VLAN) if 802.1X authentication takes a long time to complete(~10 sec) **Workaround:** Since Windows XP clients does not initiate DHCP process once again after passing 802.1x authentication, they might retain the IP from initial VLAN. In such cases, the user must manually release and renew the IP.
66749	Multiple Matching DHCP-Options in UDR causes Role and corresponding VLAN under the role causes role and VLAN flap. **Workaround:** As of now Multiple Matching DHCP-Options in UDR are not supported.
70396, 74257	It is possible that a user can get a DHCP IP from a VLAN in a previous role (such as the VLAN in initial role) even after moving to a new VLAN as a result of authentication. **Workaround:** 1) The user need to release and renew his IP in such cases. 2) In the AAA profile, make sure DHCP is denied in the initial role.
73189	If you have the same profile name configured on two CPPM servers, there is possibility that a role may be downloaded from both CPPM servers, causing an overlap. **Workaround:** Do not use same profile name in enforcement in CPPM.

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

Bug ID	Description
74062	With CPPM downloadable-role enabled, you are prompted to save configuration when rebooting or executing a sytem switchover on the MAS from the CLI even when not configuration changes were made. **Workaround:** Save your configuration before rebooting or completing the system switchover. When you are prompted to save your configuration when initiating the reboot or system switchover, choose the "no" option. Also see bug 75224 under the Stacking section of this document for related information
74264	A combination of CPPM and Windows Radius server for fail-through is not supported. **Workaround:** Use either CPPM servers as Primary and Backup or Windows Radius as Primary and Backup. Do not mix them.

Stacking

Table 10 *Known Stacking Issues and Limitations*

Bug ID	Description
58832	When a stack splits and merges back after activating an inactive stack, it may soft-reset winner stack members and configuration lost on winner-stack. **Workaround:** After stack-split, clear the `away` stack-members by using command `clear stacking member-id <id>` and then merging so that issue will not be seen.
65804	When the applied election-priority of primary and secondary of stack is removed so all the members have priority, it is observed that the roles of primary and secondary swap. **Workaround:** None.
66444	If one or more members in a stack are running version older than 7.1.3.0, they will not form adjacency and will not be shown as Dormant members with version mismatch. **Workaround:** Upgrade those MAS devices separately and then make it part of the stack running 7.1.3.0 or later.
66800	When changing the preset slot-number configuration using WEBUI with more than two primary-capable members, sometimes the secondary role might change. **Workaround:** There will not be any impact to traffic and functionality. Only secondary role changes.

Switch-Datapath

Table 11 *Known Switch-Datapath Issues*

Bug ID	Description
79631	After the Mobility Access Switch is reloaded, the policer-profile and qos-profile configured under the user-role are not applied to the user-role. This occurs whenever the switch is reloaded or rebooted. This issue is observed on Mobility Access Switch running ArubaOS 7.2.0 and is not specific to any Mobility Access Switch platform. **Workaround**: Reconfigure the policer-profile and qos-profile under user-role from the startup-config which has the relevant configuration (show startup-config).

Switch-Platform

Table 12 *Known Switch-Platform Issues and Limitations*

Bug ID	Description
58584	When an AP is connected to a MAS through a mid-span PoE injector, auto negotiation 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.
65807	IPv6 is not supported on untrusted ports in this release. **Workaround:** None.
65324	The memory usage on MAS will increase along with increasing number of history samples and/or etherstat entries. **Workaround:** Make sure that the configured samples/entries do not end up consuming all the available free memory.
68091	An interface which is operationally down as a result of Ethernet OAM failure may still transmit data and other control packets. **Workaround:** Enable STP on the interface or configure the link as a port-channel member.
68465	If you exceed the recommended value of 16 users per port on multiple switch ports, some of those user-entries may not get installed correctly. Traffic forwarding from those users will be impacted. This error will trigger a syslog similar to the example below: `<dpa 343000> <CRIT> |dpa| Unable to allocate resources for new user 00:04:1e:01:11:b1 on interface gigabitethernet0/0/22` Best practice is to not have more than 16 users connected on the untrusted interfaces. **Workaround:** None.

Tunneled Node

Table 13 *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.

Table 13 *Known Tunneled Node Issues and Limitations (Continued)*

Bug ID	Description
57690	A local VLAN is not required for Tunneled-Node operation. However, to apply a switch-profile to a Tunneled-Node configuration, a local VLAN is required to activate the switch-profile. **Workaround:** None. Ignore the warning message that appears.

VPN

Table 14 *Known VPN Issues and Limitations*

Bug ID	Description
73261	Site-to-site IPSec VPN with transport-mode is not supported in this release. **Workaround:** None.
76803	The sha-1-96 algorithm is not currently supported with IKEv1. **Workaround:** It is recommended that you use sha-160 instead.

WebUI, MIB, SNMP

Table 15 *Known WebUI, MIB, SNMP Issues and Limitations*

Bug ID	Description
60244	If you reboot the stack using the WebUI access and then stay on the same web page, after login on same page, it shows standalone mobility access rather than a stack. **Workaround:** Once you click on any options under Monitoring, Configuration, or Maintenance tabs, the proper stack information is displayed. This does not affect normal functionality of WebUI, only the display for nodes is affected.
63893	On the Monitoring page, stack ports are not shown when they are not connected to other stack ports in the stack. **Workaround:** None.

Chapter 6

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

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 7.2.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 7.2.2

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 46
- "Upgrading from the Command Line" on page 47
- "Upgrading from your USB using the LCD" on page 49

CAUTION

If you are upgrading from 7.0.x to 7.2.x and are going to create a stack, each Mobility Access Switch in the stack must be upgrade to ArubaOS 7.2.x 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:

```
(ArubaS2500-48P) #show image version member all

Member-id: 0
------------
----------------------------------
Partition               : 0:0 (/dev/ud1)
Software Version        : ArubaOS 7.2.1.0 (Digitally Signed - Production Build)
Build number            : 37429
Label                   : 37429
Built on                : Fri Mar 1 10:07:39 PST 2013
----------------------------------
Partition               : 0:1 (/dev/ud2) **Default boot**
Software Version        : ArubaOS 7.2.2.0 (Digitally Signed - Production Build)
Build number            : 38128
Label                   : 38128
Built on                : Fri Apr 19 19:50:19 PDT 2013

Member-id: 1
------------
----------------------------------
Partition               : 0:0 (/dev/ud1)
Software Version        : ArubaOS 7.2.1.0 (Digitally Signed - Production Build)
Build number            : 37429
```

```
Label                    : 37429
Built on                 : Fri Mar 1 10:07:39 PST 2013
----------------------------------
Partition                : 0:1 (/dev/ud2) **Default boot**
Software Version         : ArubaOS 7.2.2.0 (Digitally Signed - Production Build)
Build number             : 38128
Label                    : 38128
Built on                 : Fri Apr 19 19:50:19 PDT 2013

Member-id: 2
------------
----------------------------------
Partition                : 0:0 (/dev/ud1)
Software Version         : ArubaOS 7.2.1.0 (Digitally Signed - Production Build)
Build number             : 37429
Label                    : 37429
Built on                 : Fri Mar 1 10:07:39 PST 2013
----------------------------------
Partition                : 0:1 (/dev/ud2) **Default boot**
Software Version         : ArubaOS 7.2.2.0 (Digitally Signed - Production Build)
Build number             : 38128
Label                    : 38128
Built on                 : Fri Apr 19 19:50:19 PDT 2013
```

6. Reload the entire stack:

   ```
   (host) # reload
   ```

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

   ```
   show version member all

   Member-id: 0
   ------------
   Aruba Operating System Software.
   ArubaOS (MODEL: ArubaS3500-48P), Version 7.2.2.0
   Website: http://www.arubanetworks.com
   Copyright (c) 2002-2013, Aruba Networks, Inc.
   Compiled on 2013-04-19 at 19:50:19 PDT (build 38128) by p4build
   ROM: System Bootstrap, Version CPBoot 1.0.37.1 (build 37850)
   Built: 2013-04-01 00:09:52
   Built by: p4build@re_client_37850
   Switch uptime is 3 hours 10 minutes 7 seconds
   Reboot Cause: User reboot.
   Processor XLS 208 (revision A1) with 1023M bytes of memory.
   955M bytes of System flash

   Member-id: 1
   ------------
   Aruba Operating System Software.
   ArubaOS (MODEL: ArubaS3500-24P), Version 7.2.2.0
   ```

```
Website: http://www.arubanetworks.com
Copyright (c) 2002-2013, Aruba Networks, Inc.
Compiled on 2013-04-19 at 19:50:19 PDT (build 38128) by p4build
ROM: System Bootstrap, Version CPBoot 1.0.37.1 (build 37850)
Built: 2013-04-01 00:09:52
Built by: p4build@re_client_37850
Switch uptime is 3 hours 10 minutes 20 seconds
Reboot Cause: User reboot.
Processor XLS 208 (revision A1) with 1023M bytes of memory.
955M bytes of System flash

Member-id: 2
------------
Aruba Operating System Software.
ArubaOS (MODEL: ArubaS3500-24P), Version 7.2.2.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2013, Aruba Networks, Inc.
Compiled on 2013-04-19 at 19:50:19 PDT (build 38128) by p4build
ROM: System Bootstrap, Version CPBoot 1.0.37.1 (build 37850)
Built: 2013-04-01 00:09:52
Built by: p4build@re_client_37850
Switch uptime is 3 hours 10 minutes 17 seconds
Reboot Cause: User reboot.
Processor XLS 208 (revision A1) with 1023M bytes of memory.
955M bytes of System flash
```

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 MAS 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:

```
 (ArubaS2500-48P) #show image version member all
Member-id: 0
------------
----------------------------------
Partition                : 0:0 (/dev/ud1)
Software Version         : ArubaOS 7.2.1.0 (Digitally Signed - Production Build)
Build number             : 37429
Label                    : 37429
Built on                 : Fri Mar 1 10:07:39 PST 2013
----------------------------------
Partition                : 0:1 (/dev/ud2) **Default boot**
Software Version         : ArubaOS 7.2.2.0 (Digitally Signed - Production Build)
Build number             : 38128
Label                    : 38128
Built on                 : Fri Apr 19 19:50:19 PDT 2013

Member-id: 1
------------
----------------------------------
Partition                : 0:0 (/dev/ud1)
Software Version         : ArubaOS 7.2.1.0 (Digitally Signed - Production Build)
Build number             : 37429
Label                    : 37429
Built on                 : Fri Mar 1 10:07:39 PST 2013
----------------------------------
Partition                : 0:1 (/dev/ud2) **Default boot**
```

```
Software Version        : ArubaOS 7.2.2.0 (Digitally Signed - Production Build)
Build number            : 38128
Label                   : 38128
Built on                : Fri Apr 19 19:50:19 PDT 2013

Member-id: 2
------------
----------------------------------
Partition               : 0:0 (/dev/ud1)
Software Version        : ArubaOS 7.2.1.0 (Digitally Signed - Production Build)
Build number            : 37429
Label                   : 37429
Built on                : Fri Mar 1 10:07:39 PST 2013
----------------------------------
Partition               : 0:1 (/dev/ud2) **Default boot**
Software Version        : ArubaOS 7.2.2.0 (Digitally Signed - Production Build)
Build number            : 38128
Label                   : 38128
Built on                : Fri Apr 19 19:50:19 PDT 2013
```

11. Reload the entire stack:

    (host) # **reload**

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

```
show version member all

Member-id: 0
------------
Aruba Operating System Software.
ArubaOS (MODEL: ArubaS3500-48P), Version 7.2.2.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2013, Aruba Networks, Inc.
Compiled on 2013-04-19 at 19:50:19 PDT (build 38128) by p4build
ROM: System Bootstrap, Version CPBoot 1.0.37.1 (build 37850)
Built: 2013-04-01 00:09:52
Built by: p4build@re_client_37850
Switch uptime is 3 hours 10 minutes 7 seconds
Reboot Cause: User reboot.
Processor XLS 208 (revision A1) with 1023M bytes of memory.
955M bytes of System flash

Member-id: 1
------------
Aruba Operating System Software.
ArubaOS (MODEL: ArubaS3500-24P), Version 7.2.2.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2013, Aruba Networks, Inc.
Compiled on 2013-04-19 at 19:50:19 PDT (build 38128) by p4build
ROM: System Bootstrap, Version CPBoot 1.0.37.1 (build 37850)
Built: 2013-04-01 00:09:52
Built by: p4build@re_client_37850
```

```
Switch uptime is 3 hours 10 minutes 20 seconds
Reboot Cause: User reboot.
Processor XLS 208 (revision A1) with 1023M bytes of memory.
955M bytes of System flash

Member-id: 2
------------
Aruba Operating System Software.
ArubaOS (MODEL: ArubaS3500-24P), Version 7.2.2.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2013, Aruba Networks, Inc.
Compiled on 2013-04-19 at 19:50:19 PDT (build 38128) by p4build
ROM: System Bootstrap, Version CPBoot 1.0.37.1 (build 37850)
Built: 2013-04-01 00:09:52
Built by: p4build@re_client_37850
Switch uptime is 3 hours 10 minutes 17 seconds
Reboot Cause: User reboot.
Processor XLS 208 (revision A1) with 1023M bytes of memory.
955M bytes of System flash
```

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.