ArubaOS 7.1.3

Release Note

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
Tunneled-Node Fragmentation & Reassembly 7
Stack Pre-Provisioning 7
Maximum Port Channel 7
Port Security 7
RA Guard 8
Loop Protect 8
MAC Limit 8
DHCP Trust 8
VoIP Auto-Discovery 9
OSPF MD5 Authentication 9
Remote Monitoring (RMON) 9
MLD Snooping 9
LCD Functionality 10

Chapter 3 **Fixed Issues** 11
DHCP 11
Interface 11
Layer 2 Forwarding 11
Layer 3 Routing 12
Multicast 12
Security 12
Stacking 13
Switch-Platform 13
Tunneled Node 13
WebUI, MIB, SNMP 14

Chapter 4 **Known Issues** 15
Uplink Module 15
Stacking 15
Tunneled Node Controller-IP 15
Auto-Configuration Download 15
DHCP 16
IPv6 16
Layer 2 Forwarding 16
Layer 3 Routing 17
Multicast 18

QoS 19
Security 19
Stacking 21
Switch-Platform 23
Tunneled Node 23
WebUI, MIB, SNMP 24

Chapter 5 Upgrade Procedures 25
Important Points to Remember 25
Before you Upgrade 25
Save your Configuration 26
Saving the Configuration in the WebUI 26
Saving the Configuration in the CLI 26
Upgrading to 7.1.x 26
Upgrading from the WebUI 26
Upgrading from the Command Line 27
Upgrading from your USB using the LCD 28
Downgrading after an Upgrade 31
Before You Call Your Support Provider 32

Chapter 1

Release Overview

ArubaOS 7.1.3 is a software maintenance release for the Mobility Access Switch (MAS) product line 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.

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

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 15—a listing of known issues organized by functionality
- Chapter 5, "Upgrade Procedures" on page 25— 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 7.1.3 User Guide*
- *ArubaOS 7.1.3 Command Line Reference Guide*
- *ArubaOS 7.1.3 Quick Start Guide*
- *Aruba S3500 Series Mobility Access Switch Installation Guide*
- *Aruba 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 document provides a brief summary of the new features for the Mobility Access Switch (MAS) in this release.

If you are upgrading from Beta version 7.1.1.0, you must first execute the **write erase** command before you upgrade to this release.

Tunneled-Node Fragmentation & Reassembly

With tunneled-node, the supported MTU size had to be greater than 1564 bytes at intermediate routes between Tunneled-Node Clients (MAS) and Tunneled-Node Servers (Controller) because MAS did not support fragmentation and reassembly function. With the ArubaOS 7.1.1.1 and later, this limitation has been resolved.

Stack Pre-Provisioning

The stack pre-provisioning feature allows you to configure the role and member-id of the members before the stack is created. In preset config the members are configured using their serial numbers, which can be found on the purchase order or can be located on the back of the Mobility Access Switch. Additionally, the CLI commands `show inventory` or `show stacking members` displays the serial number.

Maximum Port Channel

The maximum number of port channels allowed on a Mobility Access Switch has been increased from 8 to 64. The setting range was 0-7 but it has changed from 0-63.

```
(host) (config) #interface-profile lacp-profile LACP_TEST

(host) (LACP "LACP_TEST") #group-id ?
<group-id>              Link aggregation group identifier, range 0-63

(host) (config) #interface port-channel ?
<id>                    Port-channel interface number, range 0-63
(host) (config) #interface port-channel
```

Port Security

This release of ArubaOS Mobility Access Switch supports Port Security functionality which provides network security at Layer 2. You can now filter the unauthorized devices to send the control packets, restrict the number of MACs allowed on the interface, and detect the unwanted loops in the network.

You can enable or disable this functionality at an interface level.You can recover the port automatically by enabling the `auto-recovery` option.You can also manually recover the port using the `clear` command.

RA Guard

The RA Guard feature analyzes the RAs and filters out RA packets sent by unauthorized devices. The RA guard feature is disabled by default. By enabling, the RA packets received on the interface are dropped and the port can be shutdown based on the interface configuration. The port can be re-activated after the configured time by configuring the auto-recovery timeout.

Loop Protect

The Loop Protect detects the unwanted physical loops in your network. You can enable or disable this functionality at an interface level. A proprietary protocol data unit (PDU) is used to detect the physical loops in the network. When the system detects a loop, it disables the port that sends the PDU.

MAC Limit

The MAC limit restricts the maximum number of MACs that can be learnt on the interface. When the MAC limit is enabled, it provides support to log the excess MACs or drop the new MAC learning requests or shutdown the port itself.

MAC-limit configuration has been moved to “port-security-profile”. Any existing mac-limit configurations are automatically upgraded to the new profile.

To convert mac limit setting which was applied to a port channel:

- If mac-limit is configured for port-channel 0, the profile will be `__mac_limit_pc_0_ sec_profile__`

To convert mac limit setting which was applied to an interface-group:

- If mac-limit is configured for interface-group abc, the profile will be `__mac_limit_abc_ sec_profile__`

To convert mac limit setting which was applied to an interface:

- If mac-limit is configured for interface 0/1/2, the profile will be `__mac_limit_0_1_2_ sec_profile__`

DHCP Trust

The DHCP trust functionality provides support to filter the IPv4 DHCP packets from the unauthorized devices. The following IPv4 DHCP messages are filtered on enabling the DHCP Trust:

- DHCP offer messages
- DHCP ACK messages

You can enable the DHCP trust on any interface. By default the DHCP packets are trusted on the interface. When DHCP Trust is disabled, the DHCP offer and ACK packets that are received on the interface are dropped.

VoIP Auto-Discovery

ArubaOS provides support for VoIP Auto-discovery (also referred as CDP Finger Printing) to discover the VoIP phones using neighbor discovery protocols (such as LLDP-MED and CDP) and assign Voice VLAN to the traffic originating from the phone.

You can configure VoIP either in static mode or auto-discover mode. By default, VoIP is configured in static mode. When VoIP operates in static mode, the phone is expected to know the Voice VLAN to be used and send the Voice traffic with the Voice VLAN tag. This is achieved, only if the Voice VLAN is configured statically on the phone or propagated to the phone using LLDP-MED.

In auto-discover mode, when LLDP-MED or CDP discovers a phone, the switch creates a rule to associate all the traffic originating from the phone to the Voice VLAN. Hence, the Voice VLAN need not be configured statically on the phone. The Voice VLAN can be tagged or untagged depending on the LLDP-MED configuration.

VoIP configured in auto-discover mode applies the Voice VLAN only to the first neighbor discovered in an interface. If both LLDP-MED and CDP neighbors are discovered, the preference is always given to the first LLDP-MED neighbor even if a CDP neighbor is already associated.

OSPF MD5 Authentication

MD5 is a message-digest algorithm that is specified in RFC 1321 and considered to be the most secure OSPF authentication mode. In this release, OSPF MD5 authentication is supported on a per-interface basis. and supports one key only.

Remote Monitoring (RMON)

This release of ArubaOS Mobility Access Switch supports RMON that provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area networks (LANs). Monitoring devices (commonly called "probes") contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients. While both agent configuration and data collection use SNMP, RMON is designed to operate differently than other SNMP-based systems:

- Probes have more responsibility for data collection and processing, which reduces SNMP traffic and the processing load of the clients.
- Information is only transmitted to the management application when required, instead of continuous polling.

MLD Snooping

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link. When multicast is supported at the IPv6 level, it often broadcasts at lower levels. So, for example, an Ethernet switch broadcasts multicast traffic on all ports, even if only one host wants to receive it. To prevent entire Ethernet segments from being flooded, MLD snooping can be implemented on Ethernet switches. The MLD snooping solution is similar to the IGMP snooping solution for IPv4. When MLD snooping is implemented on a switch, it detects all MLD version 1 messages that are exchanged on the link. It also maintains a table that indicates which IPv6 multicast groups should be forwarded for each of the interfaces.

LCD Functionality

Table 1 *LCD Maintenance Functions Over Stacking*

Mode	Any Stack Member (affects only local member)	Primary Only (affects all stack members)
Maintenance		
Upgrade Image		Yes
Upload Configuration		Yes
Erase Config		Yes
Media Eject		Yes
Factory Default	Yes	
System Reboot	Yes	Yes
System Halt	Yes	Yes

The options **Erase Config** has been added to the Mobility Access Switch LCD menu. **Erase Config** performs the same function as the CLI command `write erase all`.

Factory Default is an existing command but its functionality has changed. This option now performs the same function as the command `restore factory-default stacking`, which erases the current configuration and removes the stacking database.

The following issues were fixed in this release.

DHCP

Table 2 *Fixed DHCP Issues*

Bug ID	Description
58516	User can configure both static default gateway and “default gateway import DHCP.” Static and OSPF routes have a better preference than DHCP and DHCP has better preference than OSPF ASE.
62776	“Default-router” obtained from a DHCP server via “option routers” are correctly installed in the routing table.

Interface

Table 3 *Fixed Interface Issues*

Bug ID	Description
62335	Port-channel interfaces no longer go down when pc_default profile is edited with non-default values and `interface port-channel x` stanza not present in running config (on one side)
62498	When configuring a loopback interface IP, netmask is no longer requested. Instead, it will be automatically given a 32-bit mask.
62644	An uplink will no longer go down when a cable is removed and reattached to a neighboring uplink port.

Layer 2 Forwarding

Table 4 *Fixed L2 Forwarding Issues*

Bug ID	Description
56517	Configuring non-default values for parameters **fwd-delay** and **max-age** now take effect immediately.
59879	An HSL blocked interface is no longer observed sending forwarding traffic under any conditions.
62466	Quickly adding and deleting a PVST profile no longer causes L2 Manager to crash.
63180	An interface is no longer removed from the switch VLAN port list when the interface is changed from trusted to untrusted,
64209	PVST maxAge and forwardDelay are now taken from pvst-profiles configuration.
65122	SP entries are now removed when a port is changed from trusted to untrusted.

Table 4 *Fixed L2 Forwarding Issues (Continued)*

Bug ID	Description
65128	An L2M crash that occurred when renumbering stack member IDs with a Voice VLAN configured has been fixed.

Layer 3 Routing

Table 5 *Fixed Layer 3 Routing Issues*

Bug ID	Description
54091	Area 0.0.0.0 is now displayed in `show running-config`.
61903	The `clear ip ospf` process is mandatory after initial router ID configuration (without any RVI/ loopback IPs).
62269	If the user very quickly adds and removes the same vlan-interface with ospf and/or pim enabled multiple times, the VLAN interface no longer enters a state where it is not reachable.
62634	The MAS no longer crashes when using `mtrace` command on a Cisco router to trace multicast routes to the MAS.
62663	OSPF Type-4 LSA are cleaned up once the MAS is reconfigured from OSPF normal area to stub area.
62714	Changing an OSPF area from normal to stub no longer causes the adjacency between an MAS and a Cisco router to be dropped.
63100, 62759	OSPF adjacency is successfully formed after VLAN interfaces are removed and re-added before OSPF profile is created and attached to the interface.

Multicast

Table 6 *Fixed PIM-SM Issues*

Bug ID	Description
61727	When a MAS is involved in PIM assert mechanism with other 3rd party PIM routers, MAS will no longer incorrectly win and become the PIM forwarder.
63131	Duplicate multicast traffic no longer occurs when the RP interface is disabled and enabled with a topology in which RPT and SPT are partially overlaid.

Security

Table 7 *Fixed Security Issues*

Bug ID	Description
62258	ACL Mirror and send-deny-response action are unsupported commands and have been remove from stateless ACL.
64005	Setting ethernet ACL filter based on ethertype 0x86DD (IPv6) now works correctly.

Table 7 *Fixed Security Issues (Continued)*

Bug ID	Description
65020	When a role is configured with both voice vlan and voip-profile, the phone will now be assigned a correct untagged voice vlan-membership.
65149	A client that receives a role based on MAC match in a UDR rule is no longer incorrectly deleted and then recreated 20 seconds later.
65449, 65568	DHCP relay derivates to the proper VLAN when the option matches the UDR rules.

Stacking

Table 8 *Fixed Stacking Issues*

Bug ID	Description
58817	The CLI configuration command `syslocation` and the MIB object wlsxStackMemberSysLocation specify local system location of the entire Stack; Per member System location is now available.
60715	The command `clear loginsession` can now clear all valid sessions.
62496	An uplink will no longer flap when the command `reload local` is executed.
62757	When a stack is split, the stack MAC address is correctly refreshed to the new MAC address after the mac-persistent timer expires.

Switch-Platform

Table 9 *Fixed Switch-Platform Issues*

Bug ID	Description
63574	Entering a non-existent loopback ID when executing `show interface loopback <loopback-ID>` no longer causes the Interface Manager to crash.
63637	Users are created correctly when an interface is changed from trusted to untrusted with ingress ACL.
65317	User sessions on untrusted interfaces are now properly reinstalled to the hardware forwarding table, which no longer causes software forwarding and significant amounts traffic to be dropped.

Tunneled Node

Table 10 *Fixed Tunneled Node Issues*

Bug ID	Description
63458	Tunneled-Node clients with 2Kbits certificate are successfully authenticated at Tunneled-Node Server.

WebUI, MIB, SNMP

Table 11 *Fixed WebUI, MIB, SNMP Issues*

Bug ID	Description
61224	When deleting a large number of VLANs, the WebUI no longer incorrectly updates before VLAN removed completely.
62210	The dhcp-option condition is no longer available under User Derivation Rule.
62341	The SNMP traps linkUp and linkDown are now generated correctly.
62897, 63090	PAPI error messages no longer continuously appear and fill up the syslog. The member-id for a stack primary now show up in the syslog server.
66738	An issue in which a bogus IP address was shown in the MIB IP-to-MAC interface table has been fixed.

Chapter 4

Known Issues

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.

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

If you have an Mobility Access Switches running a version older than 7.1.3, you must upgrade those devices to 7.1.3 if you want to merge them with a stack currently running 7.1.3.

Tunneled Node Controller-IP

ArubaOS 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.

Auto-Configuration Download

In the release, your Mobility Access Switch and FTP download server must be on the same subnet to complete auto-configuration download. This occurs because the default-gateway option offered by the DHCP server is not applied. For more information, see "66783" on page 17.

DHCP

Table 12 *Known DHCP Issues and Limitations*

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.
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 13 *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 14 *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.

Table 14 *Known Layer 2 Forwarding Issues and Limitations (Continued)*

Bug ID	Description
66783	In factory-default config, when a VLAN interface gets a DHCP IP, the default-gateway option (if any) offered by the DHCP server will not be applied. Therefore, Auto-Configuration using a TFTP server outside of its local subnet will not work. **Workaround:** To enable importing the default-gateway, configure `default-gateway import dhcp` under `ip-profile`.

Layer 3 Routing

Table 15 *Known Layer 3 Routing Issues and Limitations*

Bug ID	Description
56986	VLAN interfaces do not generate network unreachable and host unreachable ICMP response packets. **Workaround:** None.
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 beta 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
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.

Table 15 *Known Layer 3 Routing Issues and Limitations (Continued)*

Bug ID	Description
62240	No matter what netmask is configured for loopback interface IP address, it is always displayed as netmask 32 in routing table. **Workaround:** None.

Multicast

Table 16 *Known Multicast Issues and Limitations*

Bug ID	Description
56195	When LRH has no routes toward a multicast source; and traffic will come from *,G tree, the maximum traffic will be limited to 100pps. **Workaround:** For better performance, please ensure the LRH have unicast route to the multicast source router.
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.
65152	When IPv6 multicast receivers, which have the same last 4 bytes of their IP addresses, request the same multicast traffic, only one of them will receive the traffic. For example, if two IPv6 receivers with addresses ending in ff10::1 - ff1e::1 request the same multicast traffic, only one will receive it. **Workaround:** Use different last 4 bytes for the ipv6 multicast address.
65314	The S3500 does not send query on xSTP topology change. This delays the formation of the MLD-snooping membership table. **Workaround:** None.

QoS

Table 17 *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.
64144	The command `show datapath policer management-counter` only displays counters of the primary stack member. **Workaround:** None.

Security

Table 18 *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	The `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 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.
51168, 51213, 51332	MAC authentication does not work with jumbo frames larger than 1700 bytes. **Workaround:** None.

Table 18 *Known Security Issues and Limitations (Continued)*

Bug ID	Description
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.
61179	The MAS only supports 1024-bit authentication certificates. It does not support 2048-bit or 4086-bit certificate even though they can be generated through MAS WebUI. • 1024-bit certificate: server cert is downloaded; authentication succeeds • 2048-bit or 4086-bit certificate: no server certificate is downloaded; authentication fails **Workaround:** None.
61644	In case of scaled acl (around 500 ACE entries in single ACL) configuration, the Profile Manager will be busy for about 10 minutes after boot up. **Workaround:** Wait for about 10 mins until the system completely processes this config. (`show cpuload` command will show the system CPU state)
64356	RA messages are not dropped on untrusted interfaces. **Workaround:** None.
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.
66401	DHCP Relay may not relay DHCP NAK packets from DHCP server back to the client. **Workaround:** None.

Table 18 *Known Security Issues and Limitations (Continued)*

Bug ID	Description
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.
66814	Upon reboot, the CLI sometimes allows the user to remove a user-derivation-rule which is still being referenced by one or more AAA profiles. Use the command `show profile-errors` verify if you are experiencing this issue. **Workaround:** Adding the user-derivation-rule back will restore the reference.
66818	Only the first 127 rules under a single UDR are processed, any additional rules are ignored. **Workaround:** None. Do not add more than 127 rules to a single UDR.

Stacking

Table 19 *Known Stacking Issues and Limitations*

Bug ID	Description
53033	The command `clear counters <cr>` clears only gigabitethernet interface counters and not Port-channel interface counters. **Workaround:** Use the command `clear counters port-channel <id/all>`. This clears given or all port-channel interface counters.
56634	When changing System-time using the **clock set** command, the Primary-clock changes immediately as expected. However, when using NTP external server, the Primary-clock change may take a few minutes based on standard NTP convergence. In both cases, after the Primary-clock is updated, stacking-members (Secondary, Linecards) may take 30 minutes or longer to sync their clock with the Primary-clock. **Workaround:** None.
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.
59703	ArubaOS does not accept a partial word for the option `all` under the `show XXXX member all` commands. **Workaround:** Use option `all` to execute the command on all members of the stack.
59976	If the primary member is rebooted, the tunneled-node traffic might not recover. **Workaround:** Use the command `process restart l2m` to restart L2M process. Only use this command in concert with your support provider.

Table 19 *Known Stacking Issues and Limitations (Continued)*

Bug ID	Description
62204	While using custom switch certificate for WebUI access, it may rollback to the default or previously configured certificate upon system switchover. **Workaround:** Remove the switch-cert reference under web-server by using the `no switch-cert` command and reference the same certificate again under web-server `switch-cert <cert_name>` and issue write memory.
62256	When renumbering a stacking primary to a new member identification which has been configured with the highest priority, then the old primary will become the new primary after renumbering. However, the default gateway won't work after this change. **Workaround:** Use the **reload local** command to restart the Primary; or raise another member priority to become a new Primary.
62422, 64425	When reconfiguring an RVI IP address, if adding a new IP without first removing the existing IP, the OSPF and PIM neighbors may failed to form. **Workaround:** None.
63429	MAS stacking function is limited to support 8 stack members. If connecting more than 8 members, it may cause an issue and the stack will be unable to renumber stack members later. **Workaround:** N/A. Do not connect more than 8 stack members.
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.
66195, 65703	When creating a pre-provisioned stack, if you mistype a serial number, the stack will form but some members will become Dormant. **Workaround:** If no primary has been elected, you should remove the stacking cable and reconfigure each member individually or use the factory default function on the LCD to remove the stacking database and return the device to factory default settings.
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-Platform

Table 20 *Known Switch-Platform Issues and Limitations*

Bug ID	Description
57089	When a powered device (PD) is not receiving power, different status may be displayed. • If PD hardware issue or no connection, the MAS may display as `PD detection is in progress` • If power is out of budget under static mode, the MAS may display as `Off: PoE power management` • If power is out of budget under class mode, the MAS may display as `(code=3c) Off` **Workaround:** None.
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.
61447	When changing time-range-profile mode, the command `show time-range-profile <profile>` displays the new mode but command `show poe interface gigabitethernet x/y/z` still displays the old mode. **Workaround:** Use CLI command `show time-range-profile <profile>` to display.
64551	Very rarely, executing `show version` could result in MAS stop responding with 'cpu_2 received a bus/ cache error'. **Workaround:** None.
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.

Tunneled Node

Table 21 *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.

Table 21 *Known Tunneled Node Issues and Limitations (Continued)*

Bug ID	Description
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 configuration, a local VLAN is required to activate the switch-profile. **Workaround:** None. Ignore the warning message that appears.

WebUI, MIB, SNMP

Table 22 *Known WebUI, MIB, SNMP Issues and Limitations*

Bug ID	Description
50562	Interfaces on the MAS Uplink Module are not supported by the MIB ifExtPortIfIndex. **Workaround:** None.
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.
62341	When a link status changes (either Up or Down), an SNMP trap is **not** sent as expected. **Workaround:** Use the **show log network all** command to monitor the link status.
62608	PoE power budget information may not reliable on WebUI after a local is reloaded or the stack priority changes. **Workaround:** Not applicable the on WebUI. Use the CLI to display power budget.
63893	On the Monitoring page, stack ports are not shown when they are not connected to other stack ports in the stack. **Workaround:** None.
64071	WebUI Initial Setup is supposed to only work with factory default configuration. However, after using LCD reset device back to factory default without reload the device, LCD allows users to bring up WebUI Initial Setup. **Workaround:** Reload the device after doing factory default.
66790	The command `show port-security interface` does not do anything and when executed, returns `Interface is invalid`. **Workaround:** None.

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.

If you are upgrading from Beta version 7.1.1.0, you must first execute the **write erase** command before you upgrade to this release.

Topics in this chapter include:

- "Important Points to Remember" on page 25
- "Before you Upgrade" on page 25
- "Save your Configuration" on page 26
- "Upgrading to 7.1.x" on page 26
- "Downgrading after an Upgrade" on page 31
- "Before You Call Your Support Provider" on page 32

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.x

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 26
- "Upgrading from the Command Line" on page 27
- "Upgrading from your USB using the LCD" on page 28

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

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
   ```

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 7.1.3.0 (Digitally Signed - Production Build)
   Build number            : 31703
   Label                   : 31703
   Built on                : Thu Dec 29 02:13:37 PST 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 7.1.3.0 (Digitally Signed - Production Build)
   Build number            : 31703
   Label                   : 31703
   Built on                : Thu Dec 29 02:13:37 PST 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 7.1.3.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-12-29 at 02:13:37 PST (build 31703) by p4build
ROM: System Bootstrap, Version CPBoot 1.0.32.0 (build 29889)
Built: 2011-08-22 16:07:09
Built by: p4build@re_client_29889
Switch uptime is 11 minutes 29 seconds
Reboot Cause: User reboot.
Processor XLS 208 (revision A1) with 960M bytes of memory.
955M bytes of System flash

Member-id: 1
------------
Aruba Operating System Software.
ArubaOS (MODEL: ArubaS3500-24P-US), Version 7.1.3.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-12-29 at 02:13:37 PST (build 31703) by p4build
ROM: System Bootstrap, Version CPBoot 1.0.32.0 (build 29889)
Built: 2011-08-22 16:07:09
Built by: p4build@re_client_29889
Switch uptime is 11 minutes 44 seconds
Reboot Cause: User reboot.
Processor XLS 208 (revision A1) with 960M 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

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**

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.

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
   ```

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 7.1.3.0 (Digitally Signed - Production Build)
Build number            : 31703
Label                   : 31703
Built on                : Thu Dec 29 02:13:37 PST 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 7.1.3.0 (Digitally Signed - Production Build)
Build number            : 31703
Label                   : 31703
Built on                : Thu Dec 29 02:13:37 PST 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 7.1.3.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-12-29 at 02:13:37 PST (build 31703) by p4build
ROM: System Bootstrap, Version CPBoot 1.0.32.0 (build 29889)
Built: 2011-08-22 16:07:09
Built by: p4build@re_client_29889
Switch uptime is 11 minutes 29 seconds
Reboot Cause: User reboot.
Processor XLS 208 (revision A1) with 960M bytes of memory.
955M bytes of System flash

Member-id: 1
------------
Aruba Operating System Software.
ArubaOS (MODEL: ArubaS3500-24P-US), Version 7.1.3.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-12-29 at 02:13:37 PST (build 31703) by p4build
ROM: System Bootstrap, Version CPBoot 1.0.32.0 (build 29889)
Built: 2011-08-22 16:07:09
```

```
Built by: p4build@re_client_29889
Switch uptime is 11 minutes 44 seconds
Reboot Cause: User reboot.
Processor XLS 208 (revision A1) with 960M 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.