ArubaOS 7.0

Release Note

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.

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1

Release Overview

ArubaOS 7.0 is a major software release that introduces new features and fixes to many previously outstanding issues. For details on all of the features described in the following sections, see the *ArubaOS 7.0 User Guide and ArubaOS 7.0 CLI Reference Guide*

Chapter Overview

- Chapter 2, “What’s New in this Release” on page 7 describes the new features introduced in this release.
- Chapter 3, “Known Issues” on page 15 provides descriptions and workarounds for outstanding issues in ArubaOS 7.0.

Supported Browsers

Beginning with ArubaOS 7.0, the following browsers are officially supported for use with the ArubaOS WebUI:

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

Contacting Support

Table 1 *Web Sites and Emails*

Web Site	
• Main Site	http://www.arubanetworks.com
• Support Site	https://support.arubanetworks.com
• Software Licensing Site	https://licensing.arubanetworks.com/login.php
• Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
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

Table 2 *Contact Phone Numbers*

Telephone Numbers	
• Aruba Corporate	+1 (408) 227-4500
• FAX	+1 (408) 227-4550
Support	
United States	800-WI-FI-LAN (800-943-4526)
Universal Free Phone Service Number (UIFN): Australia, Canada, China, France, Germany, Hong Kong, Ireland, Israel, Japan, Korea, Singapore, South Africa, Taiwan, and the UK	+800-4WIFI-LAN (+800-49434-526)
All other countries	+1 (408) 754-1200

Chapter 2

What's New in this Release

This chapter provides a brief summary of the new features included in this release of ArubaOS. For more information about each feature, refer to the *ArubaOS 7.0 User Guide* or *Command Line Reference*.

CAUTION

ArubaOS 7.0 can only run on the Aruba S3500 Mobility Access Switch. It will not run on any other

Profiles-Based Configuration

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

- enet-link-profile—allows you to configure an Ethernet Link
- lacp-profile—allows you to configure an LACP
- lldp-profile—allows you to configure an LLDP Profile
- mirroring-profile—allows you to configure a Mirroring profile
- mstp-profile—allows you to configure an Interface MSTP
- poe-profile—allows you to configure a Power over Ethernet profile
- switching-profile—allows you to configure a switching profile
- tunneled-node-profile—allows you to configure a Tunneled Node Server profile
- voip-profile—allows you to configure a VOIP profile

Interface Groups

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

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

Ethernet Link Profile

You can use the ethernet link profile to configure the gigabit ethernet switching and uplink ports. The ethernet interfaces support auto negotiation from 10BaseT to 1000BaseT as per IEEE 802.3u/z standards.

When you enable auto negotiation, the device that is connected to the port is automatically configured to the highest speed supported by the device in the following order (highest to lowest):

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

Auto negotiation also supports the pause capabilities, automatic Media Detection Interface (MDI), and Media Detection Interface Crossover (MDIX) cable detection. The devices exchange information using the Fast link Pulse (FLP) bursts. The auto negotiation on the link is performed when you perform any of the following activities:

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

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

Gigabit Ethernet Network Interfaces

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

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

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

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

10 Gigabit Ethernet Uplink Interfaces

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

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

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

Ethernet Flow Control

Ethernet flow control prevents loss of frames by providing a back pressure. When an ethernet port receives frames faster than it can handle, it sends a PAUSE frame to stop the transmission from the sender for a specific period of time. The PAUSE frame has a destination group address of 01-80-c2-00-00-01.

When flow control frames are received, only pausing the transmit is supported. Sending flow control frames are not supported. This means that the system can only respond to PAUSE frames and cannot generate them. The flow-control can be enabled or disabled to respond to incoming PAUSE frames.

Power Over Ethernet

Power over Ethernet (PoE) as per IEEE 802.3at is a technology for wired Ethernet LANs to carry the electric-power required for the device in the data cables. You can use this technology to power IP telephones, wireless LAN access points, cameras with pan tilt and zoom (PTZ), remote Ethernet switches, embedded computers, thin clients, and LCDs.

The IEEE standard defined in IEEE 802.3af allows network equipment (power sourcing equipment) to provide up to 15.4 Watts of power at the output for powered devices (PDs). In addition, the IEEE 802.3at (PoE+) standard provides more power to PDs where up to 30.0 Watts of power on output is delivered on the standard copper cable. The Mobility Access Switch supports both PoE standards.

The Mobility Access Switch supports three PoE power management modes:

- Static Mode.
- Dynamic Mode.
- Class-based Mode.

Static Port-Channels

A port-channel is a bundle of multiple physical interfaces that form a single logical interface. You can use port-channels to provide additional bandwidth or link redundancy between two switches. You can configure port-channels using the static Link Aggregation Group (LAG) and the dynamic Link Aggregation Control Protocol (LACP) methods. You can create port channels using the Link Aggregation Group (LAG) static method. In the static method, you must first create the port-channel interface, and then add the physical interfaces to the port-channel.

Link Aggregation Control Protocol (LACP)

The Mobility Access Switch supports Link Aggregation Control Protocol (LACP) based on the IEEE 802.3ad standard. LACP provides a standardized means for exchanging information with partner systems, to form a dynamic link aggregation group. LACP avoids port channel misconfiguration.

Two ports (actor and partner) exchange LACP data units (DUs) in the process of forming a port-channel. If one or more ports in the system have the same actor system ID, actor key, partner system ID, and partner key, they are grouped in the same port-channel.

The maximum number of supported port-channels is eight. With the introduction of LACP, this number remains the same. Using the Link Aggregation Control Protocol (LACP), you can set the port-channel dynamically. You can define the LACP parameters in a `lacp-profile`, where the port-channel group ID is configured to reference the ports utilizing the `lacp-profile`.

Two LACP configured ports exchange LACP Data Units (LACPDU) to form a port-channel. A port is configurable as an active or passive participant. In the active mode, the port initiates DUs irrespective of the partner state. The passive mode ports respond only to the incoming DUs sent by the partner port. Hence, to form a port-channel group between two ports, one port must be an active participant.

LACPDUs exchange their corresponding system identifier or priority along with their port's key or priority. This information determines the port-channel of a given port. The port-channel for a port is selected based on its keys; the port is placed in that port-channel only when it's system ID or key and partner's system ID or key matches the other ports in the port-channel (if the group has ports).

VLANs

The Mobility Access Switch supports tag-based, MAC-based, and port-based VLANs adhering to IEEE 802.1Q standard. The Mobility Access Switch operates also as a layer-2 switch that uses a VLAN as a broadcast domain. You can configure on e or more physical ports and port-channels on the Mobility Access Switch to be members of a VLAN. Additionally, each client association constitutes a connection to a physical port on the Mobility Access Switch, with membership in a specified VLAN. You can place all authenticated users into a single VLAN or into different VLANs. The VLANs can exist only inside the Mobility Access Switch or they can extend outside the Mobility Access Switch through the IEEE 802.1q VLAN tagging.

You can optionally configure an IP address and netmask for a VLAN on the Mobility Access Switch. The IP address is up when at least one physical port in the VLAN is up. You can use only one VLAN IP address as a gateway to external devices.

The Mobility Access Switch supports the following types of VLANs:

- Port-based VLANs
- MAC-based VLANs.
- Tag-based VLANs.

VLAN Interface for Layer 3 Connectivity

For Layer 3 connectivity, you can assign an IP address to the logical interface on a VLAN. Only one VLAN interface can be configured in this release. You should first remove the IP address on the existing interface VLAN, and then remove the existing interface VLAN itself (VLAN 1, created by default) before configuring the new VLAN interface. This restriction does not apply to the VLANs in Layer 2, but only for the VLAN interface for Layer 3.

VOIP VLANs

The VOIP VLAN feature enables access ports to accept both untagged (data) and tagged (voice) traffic from IP phones connected directly to the Mobility Access Switch and separate these traffic into different VLANs (namely data VLAN and Voice VLAN). You can configure a voice VLAN using the `interface voip-profile`.

LLDP and LLDP MED

You can use the IEEE 802.1ab Link Layer Discovery Protocol (LLDP) for switches, routers, and wireless LAN access points to advertise information about themselves such as identity, capabilities, and neighbors to other nodes on the network and store the discovered information. LLDP can run on all IEEE 802.1 media and data-link layer allowing two systems running different network layer protocols to learn about each other.

Link Layer Discovery Protocol (LLDP), defined in IEEE 802.1AB standard, is a Layer 2 protocol that allows network devices to advertise their identity and capabilities on the LAN. The switch supports simple one-way neighbor discovery protocol with periodic transmissions of LLDP PDU.

- LLDP frames are constrained to a local link.
- LLDP frames are TLV (Type-Length-Value) form.
- LLDP Multicast address is 01-80-C2-00-00-0E.

LLDP-MED (media endpoint devices) is an extension to LLDP developed by TIA (ANSI/TIA-1057) to support interoperability between VoIP endpoint devices and other networking end-devices. LLDP-MED is focused mainly on discovery running between network devices and end-points such as IP phones.

LLDP-MED network policy discovery lets end-points and network devices advertise their VLAN IDs (e.g. voice VLAN), IEEE 802.1p, and DSCP. The Mobility Access Switch switch can instruct end-devices to modify their settings to match VoIP requirements.

The inventory management discovery allows information such as vendor, model, firmware and serial number of end-point devices to be stored on network devices and accessible to network management systems for inventory reporting.

MSTP

Multiple Spanning Tree Protocol (MSTP) is based on the IEEE Standard 802.1D-2004 and 802.1Q-2005. In addition, MSTP supports the loopguard, rootguard, and portfast features.

Hot-Standby Link (HSL)

The Hot-Standby Link (HSL) enables a Layer 2 interface (or port-channel) to back-up another Layer 2 interface (or port-channel) so that these interfaces become mutual backups. HSL consists of a pair of redundant links. One is the primary for traversing traffic, and the other is the backup. When the primary fails, a rapid traffic failover occurs to the awaiting backup.

Multicast Support with IGMP Snooping

You can enable multicast support on the Mobility Access Switch with IGMP snooping. You can enable the Mobility Access Switch to listen in on the IGMP conversation between hosts and network devices, and create a mapping table of which links need which IP multicast streams and which multicasts can be filtered from the links which do not need them.

The Mobility Access Switch switch supports IGMP snooping, which prevents multicast flooding on Layer 2 network treating multicast traffic as broadcast traffic. All streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would be receiving all the streams only to be discarded without snooping.

Mrouter

VLANs in a Layer 2 switch need to know the path to the PIM router that connects Layer 2 domain to the Layer 3 Network. When the multicast source is present on the Layer 2 switch, the traffic that originates from the Layer 2 switches need to know a port through which multicast traffic can reach the Layer 3 PIM router. For this reason, the VLAN in the Layer 2 switch on which IGMP snooping is enabled will designate a port as Mrouter port. The mrouter port can be detected dynamically or statically. The dynamic detection is based on IGMP query message or PIM hello messages. You can also configure static mrouter ports.

When multicast receivers are present on the VLAN in a Layer 2 switch, the IGMP report message from the host is forwarded out of the mrouter port towards the PIM router to let the PIM router know that there are

receivers interested in receiving multicast traffic, so that, PIM routers can add the VLAN interface to the outgoing list in the multicast route on a multicast router.

Tunneled Nodes

Tunneled node (previously known as Mux) provides the ability to tunnel the ingress packets (via GRE) from an interface on the Mobility Access Switch (tunneled node port) to an Aruba controller (tunneled node server). You can use the tunneled nodes to allow the controller to provide centralized security policy, authentication, and access-control.

Quality of Service

ArubaOS 7.0 supports the following Quality of Service (QoS) features:

- A QoS profile that can be applied to an interface, user role, and traffic flow.
- Eight queues per interface in hardware.
- Eight traffic classes (TC), which map to the corresponding queue (0 – 7).
- Drop-precedence for controlling tail-drop.

Access Control List

Access control lists (ACLs) are a common way of restricting certain types of traffic on a physical port. The Mobility Access Switch supports multiple types of access control lists to provide flexibility to control the traffic and it supports the following types of ACLs:

- Ethertype ACL
- MAC ACL
- Standard ACL
- Extended ACL
- Stateless ACL

Roles and Policies

Every client in an ArubaOS [Release Version] is associated with a *user role*, which determines the client's network privileges, how often it must re-authenticate, and which bandwidth contracts are applicable. A *policy* is a set of rules that applies to traffic that passes through the ArubaOS Mobility Access Switch. You specify one or more policies for a user role. Finally, you can assign a user role to clients before or after they authenticate to the system.

Authentication

ArubaOS 7.0 supports the many types and methods of authentication.

Authentication Types

ArubaOS 7.0 supports the following authentication types:

- MAC Based Authentication
- 802.1X Authentication
- Client Certificate authentication

- Public Key authentication
- Machine authentication
- Management authentication

AAA Authentication Profiles

ArubaOS 7.0 supports the following AAA authentication features:

- Role-based access on wired ingress through the application of an AAA profile.
- The interface is a wired port
- Packets from these sources are enforced by the configuration in the AAA profile.

External Authentication Servers

ArubaOS 7.0 supports the following external authentication servers:

- RADIUS (Remote Authentication Dial-In User Service)
- LDAP (Lightweight Directory Access Protocol)
- TACACS+ (Terminal Access S3500 Access Control System)
- S3500 Internal Database

Storm Control

Some protocols or features can degrade the network by creating and propagating traffic storms. Storm Control prevents interfaces from disruptions by providing protection against excessive ingress rates of unknown-unicast, multicast, and broadcast traffic.

Port Mirroring

You can use port mirroring to send copies of all or sampled packets seen on specific port(s) or port-channel to a destination. You can use this method for appliances such as sniffers that monitor network traffic for further analysis.

MIB and SNMP Support

ArubaOS Mobility Access Switch supports versions 1, 2c, and 3 of Simple Network Management Protocol (SNMP) for monitoring the connected devices and uses standard MIBs (Management Information base) for obtaining the data from the devices. For more information on configuring the SNMP parameters and view the list of supported MIBs, *See ArubaOS 7.0 User Guide*.

The following are known issues currently affecting this release of ArubaOS. Applicable bug IDs and workarounds are included.

Uplink Module

The uplink module allows you can bring up 4 additional ports of 1GE or 10GE interfaces or combination; depending on the inserted transceivers automatically detected by SW driver. Current image can support SFP-SX, SFP-TX, SFP-LX, SFP+ SR, and SFP+ LR. The following issues are known on current hardware:

- No support on module hot swap – after inserting an uplink module, you must reload your Mobility Access Switch

Stacking Port Settings

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

The following command shows the ports reserved for stacking.

```
(S3500) #show stacking interfaces
Stacking ports:
---------------
stk1/3   Hardware info(module:1, port:3)
stk1/2   Hardware info(module:1, port:2)
```

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

```
(S3500) #stacking interface delete stk 1/2
   Reboot the system to apply the changes.
(S3500) #stacking interface delete stk 1/3
   Reboot the system to apply the changes.
```

Tunneled-Node MTU Size and MTU Discovery

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

```
(ArubaS3500) (Tunneled Node Server profile "TEST") #mtu ?
<mtu>                   MTU on path to controller [1024-1500]. Default: 1400
```

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

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

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

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

Security

Table 4 *Known Issues and Limitations*

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

Layer 2 Forwarding

Table 5 *Known Issues and Limitations*

Bug ID	Description
48692	Tthe `MAC-Limit` parameter under the command `show interface-config gigabitethernet` does not support untrusted interfaces. **Workaround:** None.

Table 5 *Known Issues and Limitations*

Bug ID	Description
52699	If you have a 1 GB transciever installed and replace it with a 10 GB transciever while traffic is flowing, traffic will no longer be passed. **Workaround:** Before inserting the new transciever, shut down the interface using the `interface gigabitethernet x/y/z shutdown` command. Then use the `interface gigabitethernet x/y/z no shutdown` command to bring the interface up after inserting the new transciever.

QoS

Table 6 *Known 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.
52702	If a QoS profile, attached to an ACL, and both the ACL and QoS profile are both removed, DPA will still have the QoS profile. Additionally, creating the QoS profile again will cause the OID suppression of the new object. **Workaround:** None.

Tunneled Node

Table 7 *Known 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.

WebUI, MIB, SNMP

Table 8 *Known Issues and Limitations*

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