Note

Voice over IP (VoIP) Deployment with Aruba Mobility Access Switch

Version 1.0

ARUBA networks

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

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WEATHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY AND QUET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACUTALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURSHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Warning and Disclaimer

This guide is designed to provide information about wireless networking, which includes Aruba Network products. Though Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, this guide and the information in it is provided on an "as is" basis. Aruba assumes no liability or responsibility for any errors or omissions.

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY, AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice.

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Table of Contents

Chapter 1: Introduction

The Aruba Mobile Virtual Enterprise (MOVE) architecture enables unified access with an emphasis on mobility. MOVE also delivers unique technology to support the increasing numbers of multimedia applications and population of client endpoints. Multimedia and Voice over IP (VoIP) continue to be a growing part of this client ecosystem. VoIP is an integral part of current enterprise networks. Many networks have transitioned from having a separate private branch exchange system and a data network to a single integrated data network that also supports VoIP. The fundamental reason for this change is the reduction of operational cost where network technology has advanced and can support voice functionality on top of the data network.

The Aruba Mobility Access Switch family of products provides various features including voice VLAN, Link Layer Discovery Protocol – Media Endpoint Discovery (LLDP-MED), and Quality of Service (QoS) to enable successful deployment of VoIP in enterprise networks. As part of the MOVE architecture, the Aruba Mobility Access Switch also provides support for targeted endpoint device fingerprinting. This support eliminates the need for proprietary protocol support and vendor lock-in for VoIP phone development.

This application note addresses traditional techniques and introduces new device-aware support to deploy VoIP phones. This document is intended for all system engineers and network administrators who are deploying a VoIP solution in an enterprise network. This document describes various methods of deploying a VoIP solution at the access layer of the enterprise network. Physical connectivity, interface type, and discovery protocol (LLDP-MED) are described. Table 1 lists the current software versions for this guide.

Table 1 Aruba Software Versions

Product	Version
ArubaOS™ (mobility controllers)	6.1.3.3
ArubaOS™ (mobility access switch)	7.1.3.2

Chapter 2: Deployment Methods

The VoIP solution can be implemented in many different ways with different physical connectivity and switch configurations. The decision of which method to use depends on specific business and technological requirements, as well as the preference of network administrators. This section describes the physical configurations of the Aruba Mobility Access Switch for the two most common deployment methods and lists its key benefits. Two major cases are described: 1) the VoIP phone and an endpoint host, such as a laptop, that share a single switch interface, and 2) the VoIP phone and an endpoint host that use separate interfaces.

Deploying VoIP Phone with Endpoint Host Using a Single Switch Interface

Enterprise networks commonly use a single switch interface to connect the switch interface to a VoIP phone and to connect an endpoint host to the VoIP phone. In this daisy-chain method, the physical connection of the switch interface, VoIP phone, and endpoint host forms a chain. One of the greatest advantages of this method is that fewer interfaces or switch ports are required for deployment. Two devices share a single interface, so only half of the numbers of end-user-facing interfaces are needed. Fewer interfaces reduces the initial cost for required number of access switches, number of physical cable drops at individual locations, as well operational cost to implement and maintain the deployed network. Figure 1 shows a typical setup, with a laptop sharing a connection through a VoIP phone.

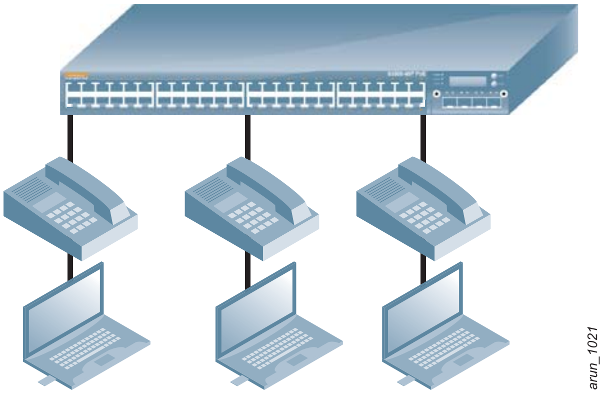


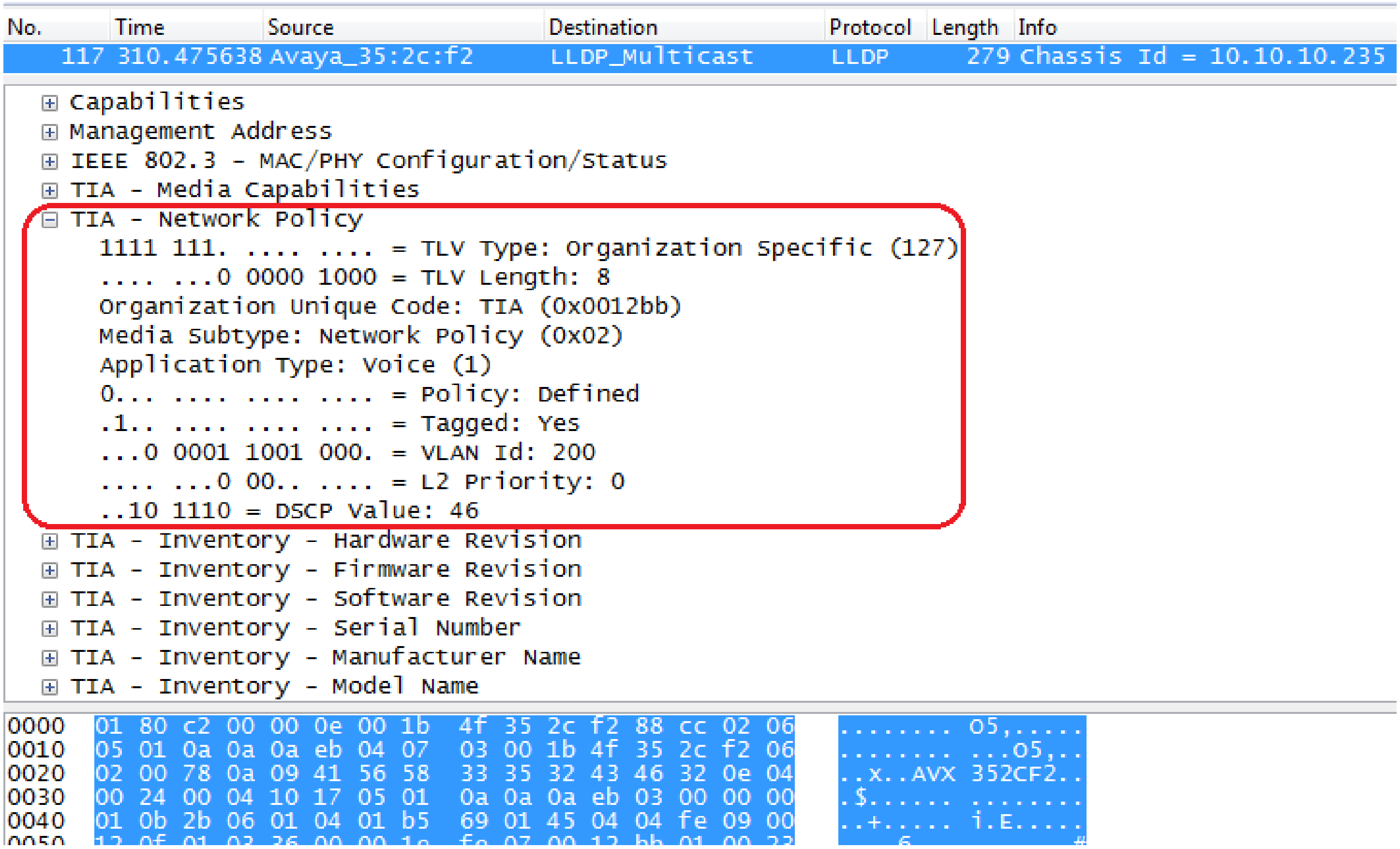
Figure 1 Aruba Mobility Access Switch – VoIP phone – laptop

Separation of Voice and Data Traffic in Daisy Chain

Several logical configurations are possible with this daisy-chain method. The VoIP phone and endpoint host can belong to separate VLANs for each device or they can belong to the same VLAN. Enterprise networks often separate voice and data traffic for a variety reasons, such as management and QoS. The Aruba Mobility Access Switch supports a voice VLAN feature to accommodate this method. The voice VLAN feature enables an access interface, which normally does not accept any tagged traffic, to allow traffic with VLAN tag (voice) in addition to the untagged traffic (data). This voice VLAN feature is especially useful when the VoIP phone that is attached to the switch interface supports LLDP-MED, simplifying the deployment of voice services.

Link-Layer Discovery Protocol – Media Endpoint Discovery (LLDP-MED)

LLDP-MED is an extension to the LLDP (defined in IEEE 802.1AB) published by Telecommunications Industry Association (TIA) as ANSI/TIA-1057. This extension primarily is designed to support and enhance the interoperability between VoIP end devices, such as VoIP phones and VoIP-related networking devices. One primary benefit of LLDP-MED is the ability for network devices to advertise network policy such as VLAN ID (voice VLAN) and QoS marking information (802.1p or DSCP value). Figure 2 highlights the LLDP-MED header as seen in a packet capture.



```
No.  Time        Source          Destination     Protocol Length Info
 117 310.475638 Avaya_35:2c:f2  LLDP_Multicast  LLDP        279 Chassis Id = 10.10.10.235

 ⊞ Capabilities
 ⊞ Management Address
 ⊞ IEEE 802.3 - MAC/PHY Configuration/Status
 ⊞ TIA - Media Capabilities
 ⊟ TIA - Network Policy
     1111 111. .... .... = TLV Type: Organization Specific (127)
     .... ...0 0000 1000 = TLV Length: 8
     Organization Unique Code: TIA (0x0012bb)
     Media Subtype: Network Policy (0x02)
     Application Type: Voice (1)
     0... .... .... .... = Policy: Defined
     .1.. .... .... .... = Tagged: Yes
     ...0 0001 1001 000. = VLAN Id: 200
     .... ...0 00.. .... = L2 Priority: 0
     ..10 1110 = DSCP Value: 46
 ⊞ TIA - Inventory - Hardware Revision
 ⊞ TIA - Inventory - Firmware Revision
 ⊞ TIA - Inventory - Software Revision
 ⊞ TIA - Inventory - Serial Number
 ⊞ TIA - Inventory - Manufacturer Name
 ⊞ TIA - Inventory - Model Name

0000  01 80 c2 00 00 0e 00 1b  4f 35 2c f2 88 cc 02 06   ........ O5,.....
0010  05 01 0a 0a 0a eb 04 07  03 00 1b 4f 35 2c f2 06   ........ ...O5,..
0020  02 00 78 0a 09 41 56 58  33 35 32 43 46 32 0e 04   ..x..AVX 352CF2..
0030  00 24 00 04 10 17 05 01  0a 0a 0a eb 03 00 00 00   .$...... ........
0040  01 0b 2b 06 01 04 01 b5  69 01 45 04 04 fe 09 00   ..+..... i.E.....
0050  12 0f 01 03 36 00 00 1e  fe 07 00 12 bb 01 00 23   ....6... .......#
```

Figure 2 Wireshark capture of LLDP-MED from Aruba Mobility Access Switch

Like other vendor-specific discovery protocols, LLDP-MED uses a specific, well-known, multicast MAC address (01-80-c2-00-00-0e) to send and receive data units (LLDPDUs). These data units are contained within a LAN segment and are not forwarded to other LAN segments.

Supported Phone Models

Several vendors manufacture VoIP phones that support LLDP-MED. Table 2 lists some commonly deployed VoIP phone models and vendors. This list is intended as a quick reference of the vendors and models, therefore it is not an exhaustive list of every vendor and model. This information has been gathered from various public sources. Before VoIP deployment is planned, consult the product documentation for the relevant vendors.

Table 2 VoIP Phones that Support LLDP-MED

Vendor	Model
Avaya	4600 series with firmware release 2.6 9600 series with firmware release 1.2.1 or 2.0 (depending on voice protocol type)
Cisco	6921 6941 6961 with firmware version 9.0(2) or later 7906G with firmware version 8.3(3) or later 7911G with firmware version 8.3(3) or later 7931G with firmware version 8.3(3) or later 7941G/GE 7942G 7945G with firmware version 8.3(3) or later 7961G/GE 7962G 7965G with firmware version 8.3(3) or later 7970G 7971G-GE 7975G with firmware version 8.3(3) or later 8961 9951 9971 with firmware version 9.1(1) or later
Polycom	SoundPoint IP 320 / 321 / 330 / 331 with firmware 3.2.0 SoundPoint IP 430 / 450 / 550 / 560 / 650 / 670 with firmware 3.2.0 SoundStation IP 6000 / 7000 with firmware 3.2.0 VVX 1500 with firmware 3.2.0

Voice VLAN with VoIP Phones that Support LLDP-MED

When you enable the voice VLAN feature on an Aruba Mobility Access Switch with VoIP phones that support LLDP-MED, the VoIP phones do not require any manual configuration for connectivity and registration.

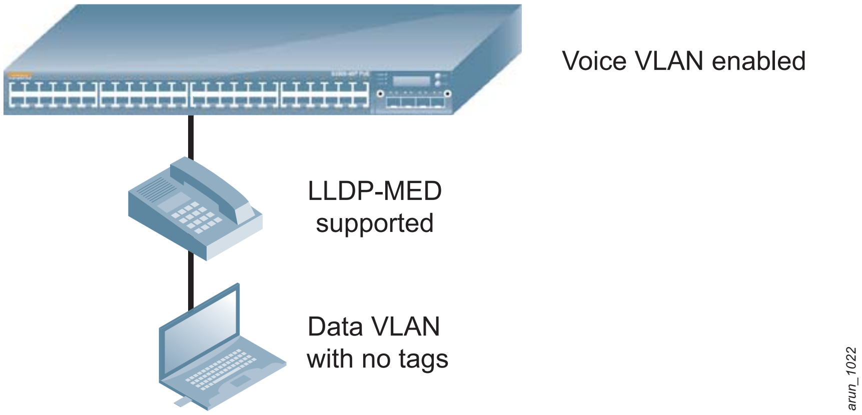


Figure 3 Aruba Mobility Access Switch – phone – laptop with voice VLAN and LLDP-MED

A configuration example of an Aruba Mobility Access Switch with the voice VLAN feature with settings for VoIP phones that support LLDP-MED in a typical implementation is shown below.

In this example, two VLANs are created:

- VLAN 100 is for data where end-hosts will be placed.
- VLAN 200 is for VoIP where VoIP phones will be placed.

```
vlan "100"
   description "DATA-ONLY"
!
vlan "200"
   description "VOIP-ONLY"
!
```

A switching interface profile is created for the data VLAN (100).

```
interface-profile switching-profile "DATA-ONLY"
   access-vlan 100
!
```

A VoIP interface profile is created with two parameters:

- VLAN 200 for voice traffic.
- DSCP value of 46 for voice packets.

```
interface-profile voip-profile "PHONES"
   voip-vlan 200
   voip-dscp 46
!
```

The switching and VoIP interface profiles are then applied to the interface. In addition, the interface is configured with QoS trust mode. VoIP packets from the phone that are marked with DSCP value (46) will be given preferred treatment compared to data traffic (DSCP value of 0). However, the qos-profile can be configured to provide more granular control if desired. For more details on qos-profile configuration, refer to *Aruba Mobility Access Switch User Guide*.

```
interface gigabitethernet "x/x/x"
   switching-profile "DATA-ONLY"
   voip-profile "PHONES"
   qos trust auto
!
```

(Optional) If multiple interfaces need to be configured with the same profiles, interface-group can be used. Also, some of the factory-default profiles, such as PoE and LLDP, would need to be applied to the newly created interface-group. QoS trust mode can also be configured for the interface-group. For more details on interface-group configuration, refer to *Aruba Mobility Access Switch User Guide*.

```
interface-group gigabitethernet "FIRST-FLOOR"
   apply-to x/x/x-y/y/y
   voip-profile "PHONES"
   lldp-profile "lldp-factory-initial"
   poe-profile "poe-factory-initial"
   switching-profile "DATA-ONLY"
   qos trust auto
!
```

(Optional) Another switching profile is created for VoIP server (VLAN 200). Then, it is applied to the interface where VoIP server/gateway is connected.

```
interface-profile switching-profile "VOIP-ONLY"
   access-vlan 200
!

interface gigabitethernet "y/y/y"
   switching-profile "VOIP-ONLY"
!
```

For more detail about individual CLI configuration syntax, refer to the *Aruba Mobility Access Switch User Guide*.

When the configuration has been completed, LLDP and LLDP-MED operation can be verified by issuing these commands:

```
(ArubaS3500-48P) #show interface-profile lldp-profile lldp-factory-initial

LLDP Profile "lldp-factory-initial"
-----------------------------------
Parameter                              Value
---------                              -----
LLDP pdu transmit                      Enabled
LLDP protocol receive processing       Enabled
LLDP transmit interval (Secs)          30
LLDP transmit hold multiplier          4
LLDP-MED protocol                      Enabled
Control proprietary neighbor discovery Disabled

(ArubaS3500-48P) #show lldp interface gigabitethernet 0/0/0

Interface: gigabitethernet0/0/0
LLDP Tx: Enabled, LLDP Rx: Enabled
LLDP-MED: Enabled
Transmit interval: 30, Hold timer: 120
```

To display detailed information about the connected VoIP phone and LLDP-MED neighbor, specifically the network policy information including VLAN ID and DSCP/802.1p values, issue the following command (only relevant information is shown) and verify the information shown under LLDP-MED network policy section:

```
(ArubaS3500-48P) #show lldp neighbor interface gigabitethernet 0/0/0 detail

Interface: gigabitethernet0/0/0, Number of neighbors: 1
------------------------------------------------------
Chassis id: 10.10.10.54, Management address: 10.10.10.54
...
System capabilities: Bridge,Phone
Enabled capabilities: Bridge
System name: AVB352CF2
System description:
   Not received
Auto negotiation: Supported, Enabled
Autoneg capability:
   10Base-T, HD: yes, FD: yes
   100Base-T, HD: yes, FD: yes
   1000Base-T, HD: no, FD: yes
Media attached unit type: 1000BaseTFD - Four-pair Category 5 UTP, full duplex mode (30)
LLDP-MED:
Device Type:  Communication Device Endpoint (Class III)
Capability:   LLDP-MED capabilities, Network policy, Inventory
LLDP-MED Network Policy for: AppType: 1, Defined: yes
   Descr:        Voice
   VLAN:         200
   Layer 2 Priority: 0
   DSCP Value:       46
Inventory:
   Hardware Revision: 9640GD01A
   Software Revision: ha96xxua3_00.bin
   Firmware Revision: hb96xxua3_00.bin
   Serial Number: xxxxxxxxxxxx
   Manufacturer: Avaya
   Model:        9640G
```

Voice VLAN Without LLDP-MED Supported VoIP Phones

The advantages of LLDP-MED-supported VoIP phones are clear, but some older phones do not support LLDP-MED or have only the proprietary protocol of the manufacturer. The voice VLAN feature on the Aruba Mobility Access Switch still can be used in such cases, but the VoIP phones must be configured manually by the network administrator. Configuration includes VLAN IDs (voice VLAN) to be used for the voice traffic, as well as any information that is related to QoS such as 802.1p or DSCP marking, which is typically completed by the administrator on the VoIP phone if available. Figure 4 shows that though the physical connection is unchanged, the operating model has shifted.

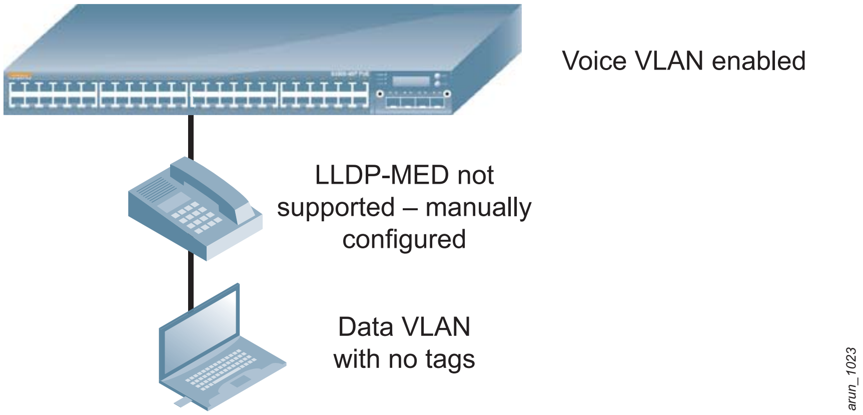


Figure 4 Aruba Mobility Access Switch – phone – laptop without LLDP-MED

Cisco VoIP Device Fingerprinting

One of the key technologies in the Aruba MOVE architecture is the ability to “fingerprint” selected devices or protocols. The device fingerprinting capability on the Aruba Mobility Access Switch is available to fingerprint the Cisco Discovery Protocol. This fingerprinting enables customers to deploy Cisco phones that do not support standards-based LLDP-MED seamlessly with Aruba Mobility Access Switches. In particular, this capability can be implemented to support non-LLDP-MED VoIP phones. The device fingerprinting capability identifies the connected devices (VoIP phones) and treats the incoming packets from the device as if they were already modified by the phones themselves through LLDP-MED. This is especially useful in cases where a large number of VoIP phones exist that do not support LLDP-MED and cannot be configured manually.

In this example, a Cisco VoIP phone that does not support LLDP-MED is connected to the interface. The Aruba Mobility Access Switch identifies the incoming traffic from the phone and places the traffic on the appropriate VLAN with QoS marking. The phone requires no network policy configuration on itself because the Mobility Access Switch can identify the device and achieve the desired implementation.

The Cisco Discovery Protocol VoIP device finger printing is configured in the VoIP interface profile with additional parameters:

- VLAN 200 for voice traffic.
- DSCP value of 46 for voice packets.
- The “auto-discover” mode has been enabled for Cisco Discovery Protocol-only phones.

```
interface-profile voip-profile "CDP-PHONES"
   voip-vlan 200
   voip-dscp 46
   voip-mode auto-discover
!
```

Then, LLDP interface profile is created and LLDP and LLDP-MED functionality is turned on with Cisco Discovery Protocol receive processing.

```
interface-profile lldp-profile "CDP-PROCESSING"
   lldp transmit
   lldp receive
   med enable
   proprietary-neighbor-discovery
!
```

The LLDP and VoIP interface profiles are applied to the interface. The interface-group configuration can also be used to apply the profiles to multiple interfaces at once. Refer to Voice VLAN with VoIP Phones that Support LLDP-MED on page 7 for a configuration example.

```
interface gigabitethernet "x/x/x"
   voip-profile "CDP-PHONES"
   lldp-profile "CDP-PROCESSING"
!
```

Cisco Discovery Protocol fingerprinting can be verified by using the following CLI command. The VoIP mode being set to auto-discover indicates the Cisco Discovery Protocol fingerprinting is enabled:

```
(ArubaS3500-48P) #show interface-profile voip-profile CDP-PHONES

VOIP profile "CDP-PHONES"
-------------------------
Parameter  Value
---------  -----
VOIP VLAN  200
DSCP       46
802.1 UP   0
VOIP Mode  auto-discover
```

To view information about the connected Cisco Discovery Protocol-only VoIP phone and any Cisco Discovery Protocol neighbors including the remote interface identification information, issue these commands:

```
(ArubaS3500-48P) #show neighbor-devices

Neighbor Devices Information
----------------------------
Interface  Neighbor ID           Protocol  Remote intf         Expiry-Time (Secs)
---------  -----------           --------  -----------         ------------------
GE0/0/0    SEPxxxxxxxxxxxx       CDPv2     Port 1              163
GE0/0/47   CUCMExxxxxxxxxx       CDPv2     GigabitEthernet0/0  137

Number of neighbors: 2


(ArubaS3500-48P) #show neighbor-devices phones

Neighbor Phones
---------------
Interface  Protocol  Phone MAC           Voice VLAN
---------  --------  ---------           ----------
GE0/0/0    CDPv2     xx:xx:xx:xx:xx:xx   200

Number of phones: 1
```

VoIP Phones and Endpoint Host in Same VLAN

When you place the VoIP phone and the endpoint host in a single VLAN, the configuration is simplified. The connected switch interface is an access interface where voice and data traffic will not need to be separated. This is not a commonly deployed configuration; however, it can be used if the simplest configuration is desired.

A switching interface profile is created for a data-and-voice VLAN. The interface-group configuration can also be used to apply the profiles to multiple interfaces at once. Refer to Voice VLAN with VoIP Phones that Support LLDP-MED on page 7.

```
interface-profile switching-profile "DATA-AND-VOICE"
   access-vlan 200
!
interface gigabitethernet "x/x/x"
   switching-profile "DATA-AND-VOICE"
!
```

VoIP Phone and Endpoint Host Deployed on Separate Switch Interfaces

Another method of deploying VoIP is to have each device, whether VoIP phone or endpoint host (such as a laptop), occupy its own interface on the switch. This method often is chosen when each end-user device must occupy its own interface for business or management reasons. The network administrator must assign specific interface(s) to either data VLAN or voice VLAN, depending on where the endpoint device or VoIP phone would be connected. For the VoIP phone, LLDP-MED is not needed to advertise which voice VLAN should be used because the interface is already in the voice traffic VLAN.

Using Separate Switch Interfaces with Voice VLAN

Even though only a single device connects to each switch interface, it can still be useful to configure the interface with access interface with voice VLAN feature if the phones support LLDP-MED. This allows switch interfaces that face end users to be configured in consistent manner without requiring any prior knowledge of which interface would be connected to the endpoint device or VoIP phone. The configuration of this method is identical to the voice VLAN with LLDP-MED supported VoIP phones. Figure 5 shows the separated physical connections.

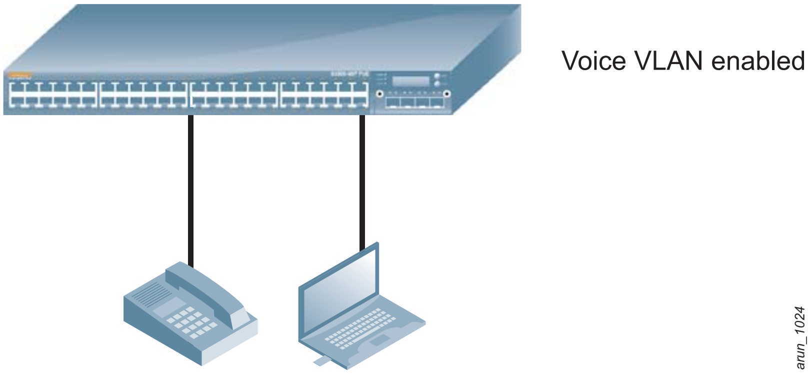


Figure 5 Separate physical connections for phones and other devices

Chapter 3: Authentication on VoIP Phones

When a VoIP solution is deployed in an enterprise network, network administrators may set up authentication of connected devices so that only the allowed devices gain access to the network. Several methods are available, depending on the supportability of connected devices. Two typical methods are IEEE 802.1X and MAC address-based authentication. This document does not describe all possible combinations of authentication methods on VoIP phones and endpoint hosts, but some of the common scenarios are described. For more details on authentication such as authentication and AAA profile configuration, refer to the *Aruba Mobility Access Switch User Guide*.

Using MAC Address Based Authentication to Authenticate VoIP phone and 802.1X to Authenticate Endpoint Host

One of the most common methods of authentication is to use MAC-address based authentication for the VoIP phone while 802.1X for the endpoint host, because each device must be authenticated separately. This configuration requires that the network administrator obtain the MAC address of the VoIP phone and populate the authentication server with appropriate credentials. Currently most endpoint hosts such as laptops and desktops support 802.1X. However some VoIP vendors and models still do not support 802.1X. The Aruba Mobility Access Switch supports different authentication methods on a given interface which allows each device or supplicant to be authenticated individually. The configuration below shows how MAC-address based authentication as well as 802.1X is implemented for a VoIP phone and endpoint host.

Starting with two VLANs to be created:

- VLAN 100 for data VLAN where endpoint hosts will be placed.
- VLAN 200 where VoIP phones will be placed.

```
vlan "100"
   description "DATA-ONLY"
!
vlan "200"
   description "VOIP-ONLY"
!
```

A VoIP profile is created with VLAN 200 for VoIP phones and DSCP value 46 for voice traffic. Cisco Discovery Protocol fingerprinting can also be added for Cisco Discovery Protocol-only phones if necessary. Refer to Cisco VoIP Device Fingerprinting on page 11 for configuration details.

```
interface-profile voip-profile "PHONES"
   voip-vlan 200
   voip-dscp 46
!
```

Two roles are defined for endpoint hosts (PC-ROLE and PHONE-ROLE). The PHONE-ROLE is also assigning the PHONES voip-profile for the role.

```
user-role PHONE-ROLE
   voip-profile "PHONES"
   access-list stateless allowall-stateless
!

user-role PC-ROLE
   vlan 100
   access-list stateless allowall-stateless
!
```

An Authentication server and group are defined, where the authentication server with IP address of a.b.c.d should contain the list of 802.1X supplicants and MAC addresses and be reachable from the Aruba Mobility Access Switch.

```
aaa authentication-server radius "RADIUS1"
   host "a.b.c.d"
   key <shared secret>
!

aaa server-group "AUTH-SERVER-GROUP1"
   auth-server RADIUS1
!
```

AAA authentication profiles are defined for 802.1X (for endpoint hosts) and MAC authentication (for VoIP phones).

```
aaa authentication dot1x "DOT1X-ACCESS"
!

aaa authentication mac "MAC-ACCESS"
!
```

An AAA profile is created with default of PHONE-ROLE for successful MAC-address based authentication and PC-ROLE for successful 802.1X supplicant authentication.

```
aaa profile "MAC-DOT1X-AAA"
   authentication-mac "MAC-ACCESS"
   mac-default-role "PHONE-ROLE"
   mac-server-group "AUTH-SERVER-GROUP1"
   authentication-dot1x "DOT1X-ACCESS"
   dot1x-default-role "PC-ROLE"
   dot1x-server-group "AUTH-SERVER-GROUP1"
!
```

The AAA profile is applied to the interface, configured as untrusted with QoS trust mode. The interface-group configuration can also be used to apply the profiles to multiple interfaces at once. Refer to Voice VLAN with VoIP Phones that Support LLDP-MED on page 7.

```
interface gigabitethernet "x/x/x"
   aaa-profile "MAC-DOT1X-AAA"
   no trusted port
   qos trust auto
!
```

(Optional) Another switching profile is created for VoIP server (VLAN 200). Then it is applied to the interface where VoIP server/gateway is connected.

```
interface-profile switching-profile "VOIP-ONLY"
   access-vlan 200
!
interface gigabitethernet "y/y/y"
   switching-profile "VOIP-ONLY"
!
```

(Optional) An IP address is assigned to management (MGMT) interface with default gateway configured for connectivity with authentication server.

```
interface mgmt
   ip address <IP address> <netmask>
!
ip-profile
   default-gateway <IP address>
!
```

NOTE

The VoIP interface profile is applied to the user role in the example because the interface is untrusted for authentication. Currently, VoIP interface profile can only be applied to trusted interfaces or user roles as shown in the Voice VLAN with VoIP Phones that Support LLDP-MED scenario.

MAC address based and 802.1X authentication profile configuration as well as authentication status of users and/or supplicants can be viewed by the following CLI commands:

```
(ArubaS3500-48P) #show aaa profile MAC-DOT1X-AAA

AAA Profile "MAC-DOT1X-AAA"
---------------------------
Parameter                              Value
---------                              -----
Initial role                           logon
MAC Authentication Profile             MAC-ACCESS
MAC Authentication Default Role        PHONE-ROLE
MAC Authentication Server Group        AUTH-SERVER-GROUP1
802.1X Authentication Profile          DOT1X-ACCESS
802.1X Authentication Default Role     PC-ROLE
802.1X Authentication Server Group     AUTH-SERVER-GROUP1
...

(ArubaS3500-48P) #show user-table

Users
-----
    IP                MAC                 Name    Role        Age(d:h:m)   Auth         AP
name Roaming    Essid/Bssid/Phy       Profile
----------        ------------       ------       ----        ----------    ----          -------
192.168.10.200  xx:xx:xx:xx:xx:xx  pcuser         PC-ROLE     00:00:00     802.1x-Wired   0/0/0
Wired                     MAC-DOT1X-AAA
10.10.10.174    yy:yy:yy:yy:yy:yy  yyyyyyyyyyyy    PHONE-ROLE   00:00:00     MAC            0/0/0
Wired                     MAC-DOT1X-AAA

User Entries: 2/2
```

The MAC address table can be used to verify the authentication status and its associated VLAN ID on per-MAC address basis. The following CLI command can be used:

```
(ArubaS3500-48P) #show mac-address-table

Total MAC address: 3
Learnt: 1, Static: 0, Auth: 2, Phone: 0

MAC Address Table
-----------------
Destination Address  Address Type   VLAN  Destination Port
-------------------  ------------   ----  ----------------
xx:xx:xx:xx:xx:xx    Auth           0100  GE0/0/0
yy:yy:yy:yy:yy:yy    Auth           0200  GE0/0/0
zz:zz:zz:zz:zz:zz    Learnt         0200  GE0/0/47
```

NOTE

EAP-MD5 is not currently supported on the Aruba Mobility Access Switch, so the 802.1X method cannot be used for VoIP phone authentication.

Authenticating the VoIP Phone Using MAC Address-Based Authentication While Using 802.1X for Endpoint Host Centrally on the Aruba Mobility Controller through Tunneled Node

As mentioned earlier, some VoIP phones do not support 802.1X. In such cases, the MAC address of the VoIP phone can be used to provide some level of security while 802.1X is used for the endpoint host. In addition, the Aruba Mobility Access Switch supports the tunneled node feature where authentication can take place centrally. This example uses the Aruba 3400 mobility controller to authenticate the devices. For more information on tunneled node feature, refer to the *Aruba Mobility Access Switch User Guide*.

Tunneled Node Configuration on the Aruba Mobility Access Switch

Layer 3 reachability is required for the tunneled-node feature. This configuration can be used as a reference, where <VLAN-ID> is a VLAN number that is used for connectivity between the Aruba Mobility Access Switch and the Aruba Mobility Controller.

```
vlan <VLAN-ID>
!
interface vlan <VLAN-ID>
   ip address <IP address> <netmask>
!

ip-profile
   default-gateway <IP address of controller or default gateway>
!

interface-profile switching-profile "VLAN-<VLAN-ID>"
   access-vlan <VLAN-ID>
!
interface gigabitethernet x/x/x
   switching-profile VLAN-<VLAN-ID>
!
```

Tunneled-node and switching profiles are defined on the Mobility Access Switch.

```
interface-profile tunneled-node-profile "TUNNELED-NODE"
   controller-ip <IP address>
!
interface-profile switching-profile "CONTROLLER-VLAN-100"
   access-vlan 100
```

Configured profiles are applied to the interface where end-host/VoIP phone will be connected. The interface-group configuration can also be used to apply the profiles to multiple interfaces at the same time. Refer to the Voice VLAN with VoIP Phones that Support LLDP-MED on page 7.

```
interface gigabitethernet "x/x/x"
   tunneled-node-profile "TUNNELED-NODE"
   switching-profile "CONTROLLER-VLAN-100"
!
```

VoIP and Authentication Configuration on a Mobility Controller

Layer 3 reachability is required for tunneled-node feature. This configuration can be used as a reference, where <VLAN-ID> is a VLAN number that is used for connectivity between the Mobility Access Switch and the Aruba Mobility Controller as well as authentication server.

```
vlan <VLAN-ID>
interface vlan <VLAN-ID>
   ip address <IP address> <netmask>
!
ip default-gateway <IP address>
!
interface gigabitethernet "z/z"
   access-vlan <VLAN-ID>
!
```

Two VLANs are created (100 for endpoint hosts and 200 for VoIP phones).

```
vlan 100 "DATA-ONLY"
vlan 200 "VOIP-ONLY"
```

Two roles are defined for endpoint hosts (TN-PC-ROLE and TN-PHONE-ROLE). The TN-PHONE-ROLE is also assigning VLAN 200 for the role.

```
user-role TN-PC-ROLE
   access-list session allowall
!
user-role TN-PHONE-ROLE
   vlan 200
   access-list session allowall
!
```

An authentication server and group are defined, where the authentication server with IP address of a.b.c.d should contain the list of 802.1X supplicants and MAC addresses and be reachable from the Aruba Mobility Access Switch.

```
aaa authentication-server radius "RADIUS1"
   host "a.b.c.d"
   key <shared secret>
!
aaa server-group "TN-AUTH-SERVER-GROUP1"
   auth-server RADIUS1
!
```

AAA authentication profiles are defined for 802.1X (for endpoint hosts) and MAC authentication (for VoIP phones).

```
aaa authentication mac "MAC-ACCESS"
!
aaa authentication dot1x "DOT1X-ACCESS"
!
```

Defined authentication profiles (802.1X and MAC authentication) are applied to the AAA profile.

- 802.1X has the default role of TN-PC-ROLE for endpoint hosts.
- MAC authentication has the default role of TN-PHONE-ROLE for VoIP phones.

```
aaa profile "TN-AAA"
   authentication-mac "MAC-ACCESS"
   mac-default-role "TN-PHONE-ROLE"
   mac-server-group "TN-AUTH-SERVER-GROUP1"
   authentication-dot1x "DOT1X-ACCESS"
   dot1x-default-role "TN-PC-ROLE"
   dot1x-server-group "TN-AUTH-SERVER-GROUP1"
!
```

The AAA profile is applied to VLAN 100.

```
vlan 100 wired aaa-profile "TN-AAA"
```

Tunneled node client status and the controller IP address can be viewed by the following CLI command on the Aruba Mobility Access Switch:

```
(ArubaS3500-48P) #show tunneled-node config

Tunneled Node Client: Enabled
Tunneled Node Server: 172.16.0.254
Tunneled Node Loop Prevention: Disabled
```

Operational status of tunneled node feature that includes the tunneled node interface, state of the tunnel, its associated VLAN ID and controller MAC address can be viewed by the following CLI commands on the Aruba Mobility Access Switch:

```
(ArubaS3500-48P) #show tunneled-node state

Tunneled Node State
-------------------
IP            MAC                Port     state     vlan  tunnel  inactive-time
--            ---                ----     -----     ----  ------  -------------
172.16.0.254  aa:aa:aa:aa:aa:aa  GE0/0/0  complete  0100  4094    0000


(ArubaS3500-48P) #show mac-address-table

Total MAC address: 1
Learnt: 1, Static: 0, Auth: 0, Phone: 0

MAC Address Table
-----------------
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  ----------------
bb:bb:bb:bb:bb:bb    Learnt        0001  GE0/0/45
```

Similar to the commands above, operational status of tunneled-node feature as well as MAC address based and 802.1X authentication status can be viewed by the following CLI commands on the mobility controller:

```
(Aruba3400) #show tunneled-node state

Tunneled Node State
-------------------
IP            MAC                s/p                   state     vlan  tunnel  inactive-time
--            ---                ---                   -----     ----  ------  -------------
172.16.0.100  aa:aa:aa:aa:aa:aa  gigabitethernet0/0/0  complete  100   9       1

(Aruba3400) #show tunneled-node config

Tunneled node Server:Enabled
Tunnel Loop Prevention:Disabled

(Aruba3400) #show user-table

Users
-----
    IP          MAC                 Name         Role           Age(d:h:m)  Auth        VPN
link  AP name    Roaming  Essid/Bssid/Phy                                       Profile
Forward mode  Type
----------      ------------       ------       ----           ----------  ----        ---
10.10.10.94     yy:yy:yy:yy:yy:yy  yyyyyyyyyyyy  TN-PHONE-ROLE  00:00:01    MAC
tunnel 9  Wired   172.16.0.100:gigabitethernet0/0/0/aa:aa:aa:aa:aa:aa  TN-AAA    tunnel
192.168.10.200  xx:xx:xx:xx:xx:xx  pcuser        TN-PC-ROLE     00:00:00    802.1x-Wired
tunnel 9  Wired   172.16.0.100:gigabitethernet0/0/0/aa:aa:aa:aa:aa:aa  TN-AAA    tunnel

User Entries: 2/2
```

Using 802.1X to Authenticate the Endpoint Host Only with User-Derived Role (UDR) for VoIP Phones

Another common scenario is to authenticate only the endpoint hosts using 802.1X while allowing the VoIP phones to connect using user-derived role (UDR). This scenario is less secure than the previous scenario where VoIP phones were authenticated using MAC address based authentication. This method is deployed when the network administrator does not need to authenticate the VoIP phones individually (which may or may not support 802.1X), but still needs to have the endpoint hosts to authenticate.

The switch interface must be configured as untrusted, so the first half (or three octets) of the MAC address of the VoIP phones, also known as Organizationally Unique Identifier (OUI), can be used to define a separate rule derivation.

Two VLANs are created:

- VLAN 100 for data VLAN where endpoint hosts will be placed.
- VLAN 200 VoIP VLAN where VoIP phones will be placed.

```
vlan "100"
   description "DATA-ONLY"
!
vlan "200"
   description "VOIP-ONLY"
!
```

A VoIP profile is created with VLAN 200 for VoIP phones and DSCP value 46 for voice traffic. Cisco Discovery Protocol fingerprinting can also be added for Cisco Discovery Protocol-only phones. Refer to Cisco VoIP Device Fingerprinting on page 11 for configuration details.

```
interface-profile voip-profile "PHONES"
   voip-vlan 200
   voip-dscp 46
!
```

Two roles are defined: one for VoIP phones and the other for endpoint hosts (PCs). The VoIP phone role has the VoIP profile applied to the role and PC-ROLE has the VLAN 100 tag.

```
user-role PHONE-ROLE
   voip-profile "PHONES"
   access-list stateless allowall-stateless
!

user-role PC-ROLE
   vlan 100
   access-list stateless allowall-stateless
!
```

An authentication server and group are defined, where authentication server a.b.c.d must be reachable from the Aruba Mobility Access Switch.

```
aaa authentication-server radius "RADIUS1"
   host "a.b.c.d"
   key <shared secret>
!

aaa server-group "AUTH-SERVER-GROUP1"
   auth-server RADIUS1
!
```

An 802.1X authentication profile is configured with default of PC-ROLE for successful supplicant authentication. In addition, a user derivation rule is defined for phones that will not be authenticated using 802.1X. Phones can be placed into PHONE-ROLE upon matching the first three octets (OUI).

NOTE

When entering the VoIP phone OUI, colon format must be used for CLI syntax (00:11:22).

```
aaa authentication dot1x "DOT1X-ACCESS"
!

aaa derivation-rules user PHONES-UDR
   set role condition macaddr starts-with "XX:XX:XX" set-value PHONE-ROLE
!

aaa profile "UDR-DOT1X-AAA"
   authentication-dot1x "DOT1X-ACCESS"
   dot1x-default-role "PC-ROLE"
   dot1x-server-group "AUTH-SERVER-GROUP1"
   user-derivation-rules "PHONES-UDR"
!
```

The AAA profile is applied to the interface, configured as untrusted with QoS trust mode. The interface-group configuration can also be used to apply the profiles to multiple interfaces at the same time. Refer to Voice VLAN with VoIP Phones that Support LLDP-MED on page 7.

```
interface gigabitethernet "x/x/x"
   aaa-profile "UDR-DOT1X-AAA"
   no trusted port
   qos trust auto
!
```

(Optional) Another switching profile is created for VoIP server (VLAN 200). Then it is applied to the interface where VoIP server/gateway is connected.

```
interface-profile switching-profile "VOIP-ONLY"
   access-vlan 200
!

interface gigabitethernet "y/y/y"
   switching-profile "VOIP-ONLY"
!
```

(Optional) Connectivity with authentication is necessary for authentication to take place. An IP address is assigned to the MGMT interface with the default gateway configured for connectivity with the authentication server.

```
interface mgmt
   ip address <IP address> <netmask>
!
ip-profile
   default-gateway <IP address>
!
```

User derivation rule and 802.1X authentication profile configuration and user/supplicant status can be viewed by the following CLI commands:

```
(ArubaS3500-48P) #show aaa profile UDR-DOT1X-AAA

AAA Profile "UDR-DOT1X-AAA"
---------------------------
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-ACCESS
802.1X Authentication Default Role     PC-ROLE
802.1X Authentication Server Group     AUTH-SERVER-GROUP1
RADIUS Accounting Server Group         N/A
RADIUS Interim Accounting              Disabled
XML API server                         N/A
User derivation rules                  PHONES-UDR
Enforce DHCP                           Disabled
Authentication Failure Blacklist Time  3600 sec

(ArubaS3500-48P) #show user-table

Users
-----
    IP               MAC          Name     Role       Age(d:h:m)  Auth         AP name
Roaming  Essid/Bssid/Phy   Profile
----------       --------         ----     ----       ---------   ----         -------
192.168.10.200  xx:xx:xx:xx:xx:xx pcuser  PC-ROLE     00:00:11   802.1x-Wired  0/0/0
Wired                     UDR-DOT1X-AAA
10.10.10.174    yy:yy:yy:yy:yy:yy         PHONE-ROLE  00:00:11                 0/0/0
Wired                     UDR-DOT1X-AAA

User Entries: 2/2
```

The MAC address table can be used to verify the authentication status and its associated VLAN ID on per-MAC address basis. The following CLI command can be used:

```
(ArubaS3500-48P) #show mac-address-table

Total MAC address: 3
Learnt: 1, Static: 0, Auth: 2, Phone: 0

MAC Address Table
-----------------
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  ----------------
xx:xx:xx:xx:xx:xx    Auth          0100  GE0/0/0
yy:yy:yy:yy:yy:yy    Auth          0200  GE0/0/0
zz:zz:zz:zz:zz:zz    Learnt        0200  GE0/0/47
```

Conclusion

The Aruba Mobility Access Switch supports various methods to deploy VoIP in enterprise networks. These methods include different ways to connect VoIP phones and endpoint host devices physically as well as various types of configuration that can be implemented on the Mobility Access Switch. Furthermore, the VoIP solution can also provide security by adding an authentication mechanism such as IEEE 802.1X or MAC address-based authentication. In addition to a clear understanding of the various available options discussed, careful planning prior to actual deployment is highly recommended for successful VoIP deployment in enterprise networks.

Appendix A: Contacting Aruba Networks

Contacting Aruba Networks

Web Site Support	
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

Validated Reference Design Contact and User Forum	
Validated Reference Designs	http://www.arubanetworks.com/vrd
VRD Contact Email	referencedesign@arubanetworks.com
AirHeads Online User Forum	http://community.arubanetworks.com

Telephone Support	
Aruba Corporate	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support	
● United States	+1-800-WI-FI-LAN (800-943-4526)
● Universal Free Phone Service Numbers (UIFN):	
■ Australia	Reach: 1300 4 ARUBA (27822)
■ United States	1 800 9434526 1 650 3856589
■ Canada	1 800 9434526 1 650 3856589
■ United Kingdom	BT: 0 825 494 34526 MCL: 0 825 494 34526

Telephone Support

- Universal Free Phone Service Numbers (UIFN):

Japan	IDC: 10 810 494 34526 * Select fixed phones IDC: 0061 010 812 494 34526 * Any fixed, mobile & payphone KDD: 10 813 494 34526 * Select fixed phones JT: 10 815 494 34526 * Select fixed phones JT: 0041 010 816 494 34526 * Any fixed, mobile & payphone
Korea	DACOM: 2 819 494 34526 KT: 1 820 494 34526 ONSE: 8 821 494 34526
Singapore	Singapore Telecom: 1 822 494 34526
Taiwan (U)	CHT-I: 0 824 494 34526
Belgium	Belgacom: 0 827 494 34526
Israel	Bezeq: 14 807 494 34526 Barack ITC: 13 808 494 34526
Ireland	EIRCOM: 0 806 494 34526
Hong Kong	HKTI: 1 805 494 34526
Germany	Deutsche Telkom: 0 804 494 34526
France	France Telecom: 0 803 494 34526
China (P)	China Telecom South: 0 801 494 34526 China Netcom Group: 0 802 494 34526
Saudi Arabia	800 8445708
UAE	800 04416077
Egypt	2510-0200 8885177267 * within Cairo 02-2510-0200 8885177267 * outside Cairo
India	91 044 66768150