

# **Dell Networking W-Series ArubaOS 6.x MIB**



Reference Guide

## Copyright

© 2014 Aruba Networks, Inc. Aruba Networks trademarks include  **airwave**, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System®. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. All other trademarks are the property of their respective owners.

## Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011

Infoblox, Inc. All rights reserved. [This product includes software developed by Lars Fenneberg, et al.](#) The Open Source code used can be found at this site:

[http://www.arubanetworks.com/open\\_source](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.

<b>Chapter 1</b>	<b>About this Guide .....</b>	<b>9</b>
	Contents .....	9
	Related Documents .....	9
	Text Conventions.....	9
	Frequently Used Acronyms .....	10
	Contacting Support .....	13
<b>Chapter 2</b>	<b>MIBs Overview .....</b>	<b>15</b>
	MIBs .....	15
	SNMP .....	16
	Traps.....	17
<b>Chapter 3</b>	<b>Using MIBs .....</b>	<b>19</b>
	Downloading MIB Files.....	19
	Reading MIB Files.....	20
	SNMP File.....	25
	HP OpenView .....	26
	MIB Limitations.....	26
<b>Chapter 4</b>	<b>MIB Modules and Traps .....</b>	<b>27</b>
	AP and AM Modules.....	27
	Authentication Module.....	27
	Controller Transport Service.....	28
	External Services Interface (ESI) Module.....	28
	IF External (IF EXT) .....	28
	Mesh Module .....	28
	Mobility Module .....	28
	Monitor Module .....	28
	Signal Noise Ratio (SNR) Module .....	28
	Switch Module.....	29
	System External Module.....	29
	Textual Conventions .....	29
	Traps Module.....	29
	Tunneled-Node Module.....	29
	User Module .....	29
	User6 module .....	30
	Voice Module.....	30
	Wireless Local Area Network Module.....	30



Table 1	Contents Overview .....	9
Table 2	Conventions.....	9
Table 3	Frequently Used Acronyms .....	10
Table 4	Contact Information.....	13
Table 5	MIB Node Identification - enterprise nodes.....	15
Table 6	MIB Keywords .....	17
Table 7	Limitations and Constraints.....	26



Figure 1	High Level MIB Hierarchy .....	16
Figure 2	CLI Interface .....	19
Figure 3	Graphical User Interface.....	20
Figure 4	CTS OIDs Relative to Dell.....	25





This manual is for network administrators and operators responsible for managing the controller.



MIB module tables and OIDs are no longer documented in this guide. To view current MIB module tables and OIDs, download the standard mibs tar.gz file from the support site and view each MIB using a free MIB browser. See section “MIB Browsers” on page 19 for viewing MIBs.

## Contents

This guide provides information about Dell Networking W-Series ArubaOS MIBs. Unless otherwise stated in the following table, each chapter provides information about the hierarchy, OIDs, and descriptions of the statistical information the MIBs provide.

**Table 1** Contents Overview

Chapter	Contents
MIBs Overview	Introductory information about ArubaOS MIBs—hierarchy, relationship with SNMP, and Traps.
Using MIBs	Information and tips about MIB files.
MIB Modules and Traps	Information about access points (AP) and air monitors (AM). <b>NOTE:</b> All MIB tables and MIB OIDs in this chapter were deprecated in ArubaOS 3.0 and are no longer supported

## Related Documents

Related documents include the following guides:

- *Dell Networking W-Series ArubaOS Quick Start Guide*
- *Dell Networking W-Series ArubaOS User Guide*
- *Dell Networking W-Series ArubaOS CLI Reference Guide*
- *Dell Networking W-Series ArubaOS Release Notes*

## Text Conventions

Table 2 presents the conventions used throughout this manual to emphasize important concepts:

**Table 2** Conventions

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.

**Table 2** *Conventions*

Type Style	Description
System items	This fixed-width font depicts the following: Sample screen output, System prompts, Filenames, software devices, and certain commands when mentioned in the text.
<b>Commands</b>	In the command examples, this bold font depicts text that the user must type exactly as shown.

## Frequently Used Acronyms

Table 3 defines frequently used acronyms.

**Table 3** *Frequently Used Acronyms*

Acronym	Definition
3DES	Triple DES
ACL	Access Control List
ADP	ArubaOS Discovery Protocol
AM	Air Monitor
AP	Access Point
ARM	Adaptive Radio Management
BSSID	Basic Service Set Identifier
CA	Certificate Authority
CAC	Call Admission Control
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSR	Certificate Signing Request
CW	Contention Window
DA	Destination Address
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DOS	Denial of Service

**Table 3** *Frequently Used Acronyms (Continued)*

Acronym	Definition
DPD	Dead Peer Detection
DSS	Direct Spread Spectrum
EAP	Extensible Authentication Protocol
EDCA	Enhanced Distributed Channel Access
EIRP	Effective Isotropic Radiated Power
ESI	External Services Interface
ESSID	Extended Service Set Identifier
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HAT	Home Agent Table
HT	High Throughput
IAS	Internet Authentication Service
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IV	Initialization Vectors
KB	Kilobyte
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LI	Listening Interval
MAC	Media Access Control
MB	Megabyte
MCHAP	Microsoft Challenge Handshake Authentication Protocol
MIB	Management Information Base
NAS	Network Address Server
NAT	Network Address Translation
NIC	Network Interface Card

**Table 3** *Frequently Used Acronyms (Continued)*

Acronym	Definition
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OUI	Organizational Unit Identifier
PAP	Password Authentication Protocol
PEAP	Protected EAP
PEF	Policy Enforcement Firewall
PIN	Personal Identification Number
PoE	Power over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-Shared Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAP	Remote Access Point
RF	Radio Frequency
RMON	Remote Monitor
RSA	Rivest-Shamir-Aldeman (encryption algorithm)
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
TIM	Traffic Indication Map
TLS	Transport Layer Security
ToS	Type of Service
TSPEC	Traffic Specification
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network

**Table 3** *Frequently Used Acronyms (Continued)*

Acronym	Definition
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor Specific Attributes
WEP	Wired Equivalent Protocol
WINS	Windows Internet Naming Service
WLAN	Wireless Local Area Network
WMM	Wireless MultiMedia / Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access

## Contacting Support

**Table 4** *Contact Information*

Web Site Support	
Main Website	dell.com
Support Website	dell.com/support
Documentation Website	dell.com/support/manuals



This chapter provides an overview of the ArubaOS Enterprise MIBs in the following sections:

- “MIBs” on page 15
- “SNMP” on page 16
- “Traps” on page 17

## MIBs

A Management Information Base (MIB) is a virtual database that contains information that is used for network management. Each managed device contains MIBs that define the properties of that device. A separate MIB is provided for each defined property, such as the group of physical ports that are assigned to a VLAN or the statistical data of packets that are transferred at a specific rate.

MIB objects, such as a MIB table or a specific element of data in a MIB table, are identified with Object Identifiers (OIDs). The OIDs are designated by text strings and integer sequences.

The hardware MIBs are assigned under the Dell organization code, while all others are under the Aruba organization code.

*Dell* is the parent of the proprietary MIBs that are supported on Dell Networking W-Series Mobility Controllers.

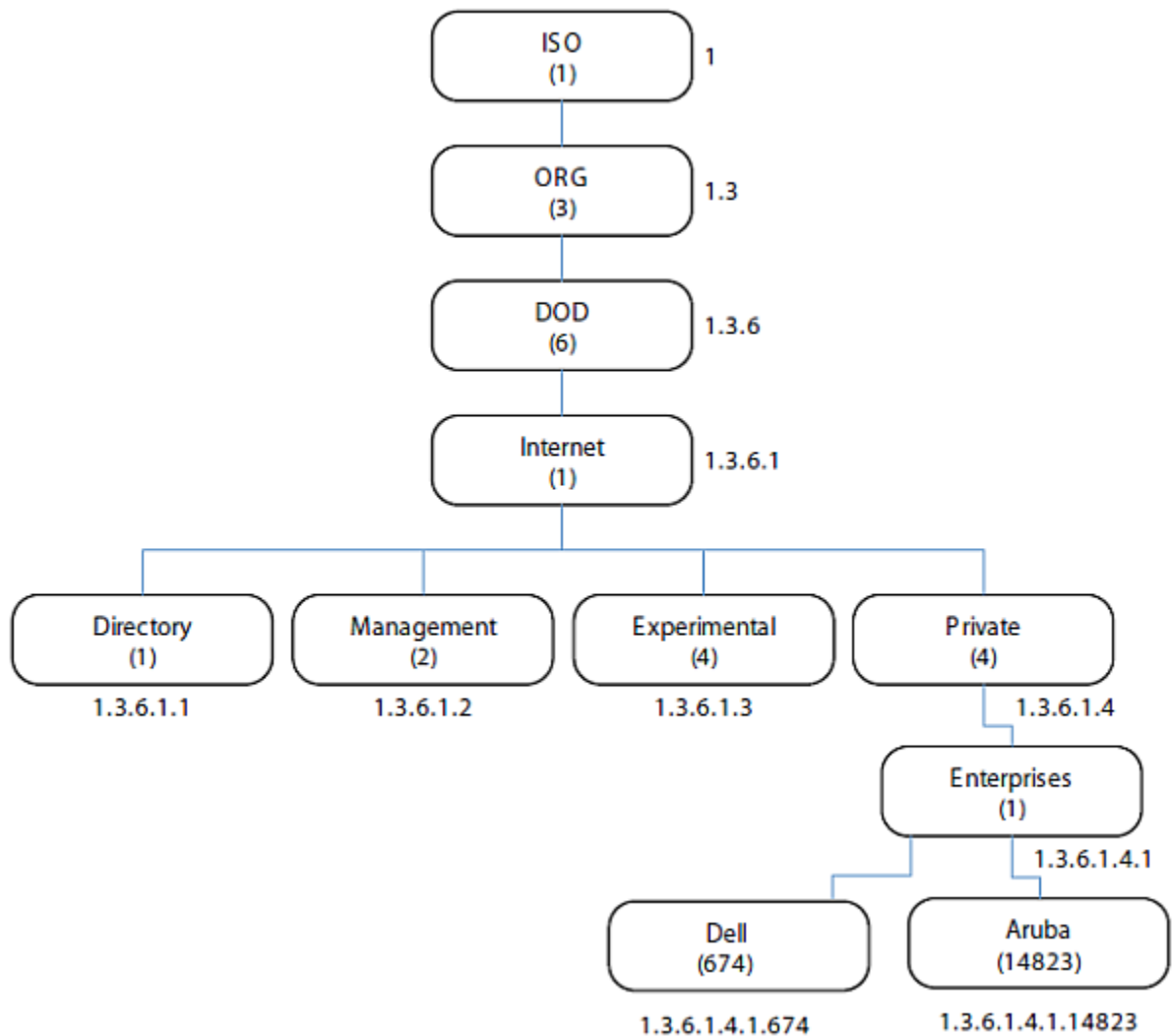
The numerical string lists the nodes of the enterprise MIB hierarchy, as shown in [Table 5](#).

**Table 5** MIB Node Identification - enterprise nodes

Integer	String	Name
1	1	OSI
3	1.3	ORG
6	1.3.6	DOD
1	1.3.6.1	Internet
4	1.3.6.1.4	Private
1	1.3.6.1.4.1	Enterprise
674	1.3.6.1.4.1.674	Dell

[Figure 1](#) illustrates the high-level hierarchy of the MIBs. This document only covers the enterprise MIBs, objects designed to specifically support Dell devices. Standard MIBs are not covered.

**Figure 1** High Level MIB Hierarchy



MIB is one of the elements of Simple Network Management Protocol (SNMP), which is used to manage network devices. To deliver information between devices, every object referred to in an SNMP message must be listed in the MIB. If a component of a device is not described in a MIB, that component cannot be recognized by SNMP—there is no information for SNMP managers and SNMP agents to exchange.

The information provided by a MIB is a file that describes network elements with numerical strings. This information is compiled into readable text by the SNMP manager. For information about reading MIB text files, see “[Reading MIB Files](#)” on page 20.

## SNMP

Three significant elements of SNMP are Managers, Agents, and MIBs.

- Managers (software application) are consoles that are used to communicate with and manage devices that support SNMP Agents. Managers collect information by polling Agents. Managers can also be used to send configuration updates or send controlling requests to actively manage a network device.
- Agents (software application) provide information from the network devices to the Managers. Network devices include workstations, routers, microwave radios, and other network components. Agents are



embedded in the controller firmware, unlike some devices such as servers that require the agent to be installed separately.

- MIBs are used for communication between the Managers and the Agents. The OIDs of the MIBs enable the Managers and Agents to communicate specific data requests and data returns.
- To ensure functionality with SNMP, MIB objects must be defined with the proper *keywords*, as shown in Table 6.

ArubaOS Enterprise MIBs support SNMPv1, SNMPv2, and SNMPv3.

**Table 6** MIB Keywords

Keyword	Description
<b>Sequence</b>	The sequence of objects of the MIB. This keyword is used mostly with entry MIB objects to list the MIB objects that exchange information.
<b>Syntax</b>	Textual conventions, such as <i>Integer32</i> .
<b>Max-Access</b>	Defines the object accessibility: <i>read-only</i> : can be retrieved but not modified <i>read-write</i> : can be retrieved and modified <i>not-accessible</i> : cannot be retrieved; it is for internal (device) use only <i>accessible-for-notify</i> : can be retrieved when a trap message (notification) is sent
<b>Status</b>	Defines the status of the object: <i>current</i> : up to date <i>deprecated</i> , <i>obsolete</i> , and <i>to be phased out in the future</i>
<b>Description</b>	A text string that describes the object.



History may be included in some MIB tables—it lists in which ArubaOS release the MIB was updated or otherwise changed.

## Traps

An event is a change on a network device, such as a change in value that crosses threshold. Some events are categorized as alarms, other events only provide information. When an event occurs on a network device, SNMP notifications are sent out as traps or information requests.

- Traps are unconfirmed notifications—the receiver does not acknowledge to the sender that the information was received.
- Inform requests are confirmed notifications—the receiver acknowledges to the sender that the information was received.

Following are descriptions of trap types.

- Discrete Alarm Inputs

These traps, also known as digital inputs or contact closures, are used for monitoring equipment failures, intrusion alarms, beacons, and flood and fire detectors.

- Analog Alarm Inputs

Analog alarms measure characteristics that can affect equipment performance—variable levels of voltage or current, temperature, humidity, and pressure.

- Ping Alarms

Ping alarms are used to ping network devices at regular intervals. If a device fails to respond, an alarm (SNMP trap) will be sent.

- **Control Relays**

Relay outputs enable operating remote site equipment.

- **Terminal Server Function**

The terminal server function enables connection to remote-site serial devices. For example, device connection to serial ports enables telnet access via LAN.

This chapter provides information on and examples of using MIBs.

- “Downloading MIB Files” on page 19
- “Reading MIB Files” on page 20
- “SNMP File” on page 25
- “HP OpenView” on page 26
- “MIB Limitations” on page 26

## Downloading MIB Files

The most recent Dell MIB files are available for registered customers at: [dell.com/support](http://dell.com/support)

## Retrieving Information from a MIB

To retrieve information from a MIB, the following information is required:

- SNMP version
- SNMP community name—*public* or *private*
- The IP Address of the Dell Mobility Controller
- The OID of the MIB value you want to monitor

In addition, MIB files can be placed in the appropriate disk location to assist the user in locating desired OID values for monitoring. If MIB files need to be acquired, contact the support site.

It is assumed that the workstation is connected to the Dell controller and that a MIB browser is available. For most applications, the *root* of the MIB must be included in the OID—the OID begins with a decimal point as shown below.

```
.1.3.6.1.4.1.674.2.2.1.1.2.1
```

## MIB Browsers

If using an application that is run through CLI (a *cmd* window), the command would resemble the following:

```
snmpget -v 2c -c <community name> <controller IP address> <MIB OID>
```

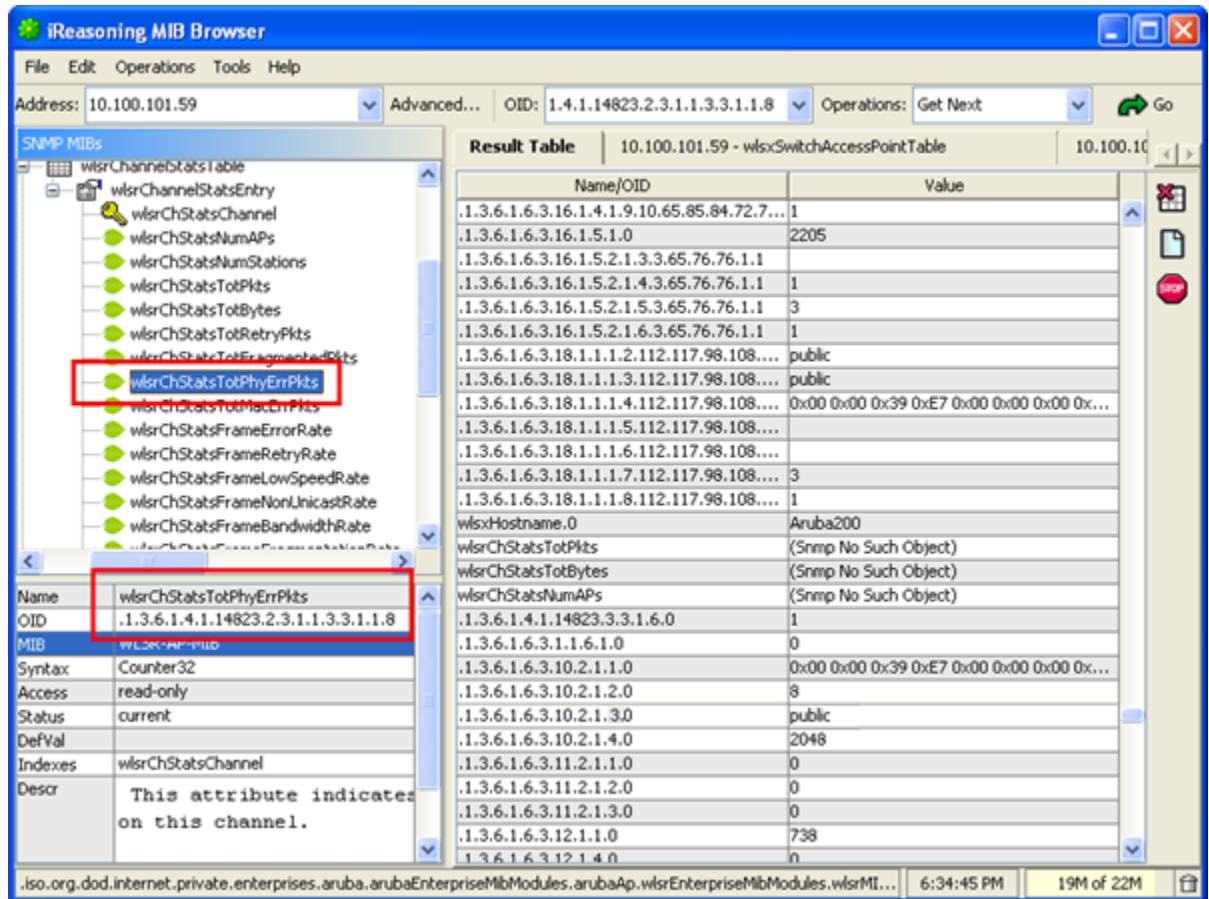
Figure 2 shows an example of submitting a command to obtain information.

**Figure 2** CLI Interface

```
C:\usr\bin>snmpget -v 2c -c public 10.100.101.59 .1.3.6.1.4.1.14823.2.2.1.1.1.1
WLSX-SWITCH-MIB::wlsxHostName = GLOBALS: Aruba200
```

Figure 3 shows how information may be obtained through a graphical user interface (GUI). The user interface and the available features vary by application.

Figure 3 Graphical User Interface



## Reading MIB Files

This section describes how to interpret the basic components of a MIB file. To determine the OIDs, viewing the file `snmp.h` may be necessary, which is described in “SNMP File” on page 25. For additional information about MIB files, see “MIBs” on page 15.

MIB files describe a specific component of a network device. The files are numerical strings that are converted to ASCII text by the compiler of the SNMP manager. A word processor or text editor can be used to open the ASCII file. The contents of an example ArubaOS enterprise MIB file, *aruba-cts.my*, are described below.

### Opening Line

Following is the opening line, the beginning of the MIB file.

```
WLSX-CTS-MIB DEFINITIONS ::= BEGIN
```

### Imports

The `Imports` section lists the objects that are defined in external ASN.1 files and are used in the current MIB file.

```
IMPORTS
    TEXTUAL-CONVENTION,
    MODULE-IDENTITY,
    OBJECT-TYPE,
    snmpModules,
```

```
Integer32,  
Unsigned32,  
Counter32,  
IpAddress,  
NOTIFICATION-TYPE  
    FROM SNMPv2-SMI
```

```
TDomain,  
DisplayString,  
PhysAddress,  
TAddress,  
TimeInterval,  
RowStatus,  
StorageType,  
TestAndIncr,  
MacAddress,  
TruthValue  
    FROM SNMPv2-TC
```

```
OBJECT-GROUP  
    FROM SNMPv2-CONF
```

## Inheritance

This section shows the vendor of the MIB and the inheritance, and provides an overall description.

A significant part of inheritance is the OID. The entire OID is not listed for each MIB object—instead, the parent of the object is shown. The tree for the CTS MIB is illustrated in [Figure 4 on page 25](#). The OID can be determined from the parent object as follows.

wlsxEnterpriseMibModules is the parent object of the CTS MIB—its OID is 1.3.6.1.4.1.14823.2.2.1.

wlsxCtsMIB MODULE-IDENTITY shows wlsxEnterpriseMibModules 11, which indicates 11 is appended to the OID of wlsxEnterpriseMibModules. Its OID is 1.3.6.1.4.1.14823.2.2.1.11.

wlsxCtsOpGroup OBJECT IDENTIFIER ::= { wlsxCtsMIB 1 } indicates the OID is 1.3.6.1.4.1.14823.2.2.1.11.1.

wlsxCtsRequestTable OBJECT-TYPE shows wlsxCtsOpGroup 1, which indicates the OID is 1.3.6.1.4.1.14823.2.2.1.11.1.1.

All MIBs and their related OIDs are listed in the snmp file of ArubaOS. For more information, see [“SNMP File” on page 25](#).

```
wlsxEnterpriseMibModules  
FROM ARUBA-MIB;
```

## Identity

Identity is the opening description of the MIB. The information includes contact information for the vendor and a general description of the MIB.

```
wlsxCtsMIB MODULE-IDENTITY  
    LAST-UPDATED "0609240301Z"
```

```

ORGANIZATION "Aruba Wireless Networks"

CONTACT-INFO
    "Postal:    1322 Crossman Avenue
                Sunnyvale, CA 94089

    E-mail:    dl-support@arubanetworks.com

    Phone:     +1 408 227 4500"

DESCRIPTION
    "This MIB module defines MIB objects which provide
    information about the Controller Transport Service (Cts) in the
    Dell controller."

REVISION      "0609240301Z"

DESCRIPTION
    "The initial revision."

 ::= { wlsxEnterpriseMibModules 11 }

```

## MIB Modules

MIB objects can be placed in logical groups, Group and Table. One MIB file can consist of multiple groups. A group typically contains at least one table. The table lists the MIB objects that contain the information that is exchanged.

The first object of a table is an Entry. The keyword SEQUENCE lists the objects of the table that contain device information. Each subsequent object inherits the OID of the Entry, and contains information sorted by keywords: Syntax, Access, Status, Description. For details about keywords, see “MIBs” on page 15.

The OID of the Entry is `wlsxCtsRequestEntry` is `wlsxCtsRequestTable 1`, which represents 1.3.6.1.4.1.14823.2.2.1.11.1.1.1. The OIDs of the subsequent objects of this table are appended increments of the Entry OID. For example, the OID of `wlsxCtsIndex` is `wlsxCtsRequestEntry 1`, which represents 1.3.6.1.4.1.14823.2.2.1.11.1.1.1.1.

## Group

```
wlsxCtsOpGroup    OBJECT IDENTIFIER ::= { wlsxCtsMIB 1 }
```

## Table

```
wlsxCtsRequestTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF WlsxCtsRequestEntry
```

```
MAX-ACCESS not-accessible
```

```
STATUS current
```

```
DESCRIPTION
```

```
"
```

```
"
```

```
::= { wlsxCtsOpGroup 1 }
```

## Entry

```
wlsxCtsRequestEntry OBJECT-TYPE
```

```
SYNTAX WlsxCtsRequestEntry
```

```
MAX-ACCESS not-accessible
```

```
STATUS current
```

**DESCRIPTION**  
"  
INDEX { wlsxCtsIndex }  
 ::= { wlsxCtsRequestTable 1 }

**WlsxCtsRequestEntry ::=**  
**SEQUENCE**  
{  
wlsxCtsIndexInteger32,  
wlsxCtsOpcodeDisplayString,  
wlsxCtsCookieDisplayString,  
wlsxCtsURLDisplayString,  
wlsxCtsFlagsBITS,  
wlsxCtsStatusRowStatus  
}

### *Informative MIB Objects*

**wlsxCtsIndex OBJECT-TYPE**  
**SYNTAX** Integer32  
**MAX-ACCESS** not-accessible  
**STATUS**current  
**DESCRIPTION**  
"  
CTS transport index  
0 - Config Sync  
1 - Counters Sync  
2 - RF Plan Sync  
"  
 ::= { wlsxCtsRequestEntry 1 }

**wlsxCtsOpcode OBJECT-TYPE**  
**SYNTAX** DisplayString  
**MAX-ACCESS** read-write  
**STATUS**current  
**DESCRIPTION**  
"  
CTS operation opcode  
"  
 ::= { wlsxCtsRequestEntry 2 }

**wlsxCtsStatus OBJECT-TYPE**  
**SYNTAX** RowStatus  
**MAX-ACCESS** read-write  
**STATUS**current

#### DESCRIPTION

```
"  
CTS row status  
"  
 ::= { wlsxCtsRequestEntry 6 }
```

### Closing Line

Following is the closing line—the end of the MIBs file.

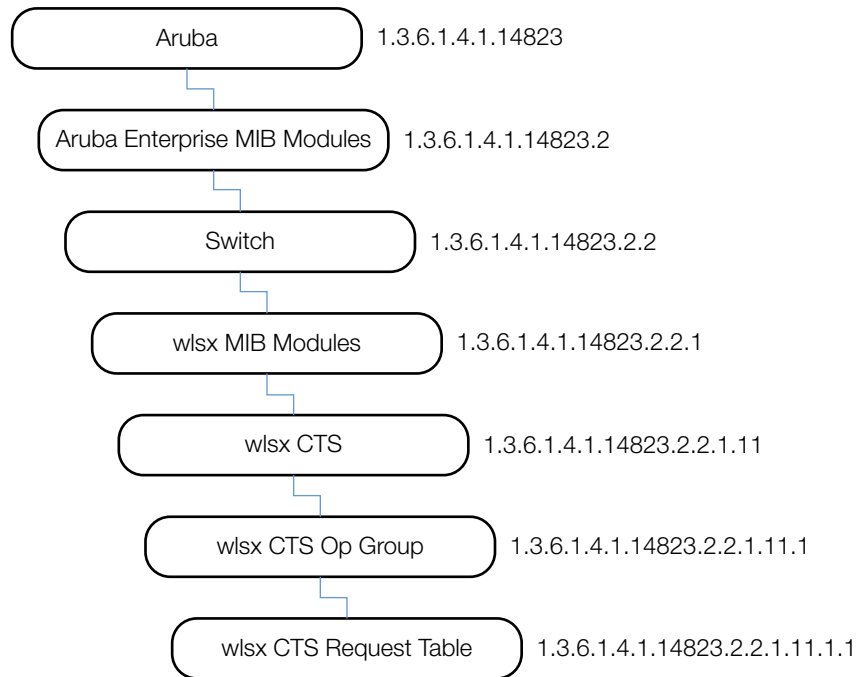
```
END
```



## OID Flow Chart

Figure 4 illustrates the tree of the CTS MIB, relative to the Dell MIB.

Figure 4 CTS OIDs Relative to Dell



## SNMP File

The `snmp.h` file lists the OIDs of all MIBs. Following are sections from `snmp.h` that show the complete OID of each of the Controller Transport Service (CTS) MIB elements. The list starts from the ancestral parent *iso*.

All ArubaOS MIBs inherit their OIDs from the Dell MIB node. The following rows list the MIBs that precede CTS, starting from *iso*.

```
{ "iso",                HASHNEXT("1") },
{ "org",                HASHNEXT("1.3") },
{ "dod",                HASHNEXT("1.3.6") },
{ "internet",          HASHNEXT("1.3.6.1") },
{ "private",           HASHNEXT("1.3.6.1.4") },
{ "enterprises",       HASHNEXT("1.3.6.1.4.1") },
{ "aruba",             HASHNEXT("1.3.6.1.4.1.14823") },
{ "arubaEnterpriseMibModules", HASHNEXT("1.3.6.1.4.1.14823.2") },
{ "switch",            HASHNEXT("1.3.6.1.4.1.14823.2.2") },
```

```
{ "wlsxEnterpriseMibModules", HASHNEXT("1.3.6.1.4.1.14823.2.2.1") },
```

The following rows list the CTS MIB OIDs.

```
{ "wlsxCtsMIB", HASHNEXT("1.3.6.1.4.1.14823.2.2.1.11") },
{ "wlsxCtsOpGroup", HASHNEXT("1.3.6.1.4.1.14823.2.2.1.11.1") },
{ "wlsxCtsRequestTable", HASHNEXT("1.3.6.1.4.1.14823.2.2.1.11.1.1") },
{ "wlsxCtsRequestEntry", HASHNEXT("1.3.6.1.4.1.14823.2.2.1.11.1.1.1") },
{ "wlsxCtsIndex", HASHNEXT("1.3.6.1.4.1.14823.2.2.1.11.1.1.1.1")},
{ "wlsxCtsOpcode", HASHNEXT("1.3.6.1.4.1.14823.2.2.1.11.1.1.1.2")},
{ "wlsxCtsCookie", HASHNEXT("1.3.6.1.4.1.14823.2.2.1.11.1.1.1.3")},
{ "wlsxCtsURL", HASHNEXT("1.3.6.1.4.1.14823.2.2.1.11.1.1.1.4")},
{ "wlsxCtsFlags", HASHNEXT("1.3.6.1.4.1.14823.2.2.1.11.1.1.1.5")},
{ "wlsxCtsStatus", HASHNEXT("1.3.6.1.4.1.14823.2.2.1.11.1.1.1.6")},
```

## HP OpenView

To install the Dell module for HP OpenView, log in as the root user and execute the following script:

```
# $OV_CONTRIB/NNM/Dell/install
```

## MIB Limitations

Following are the known limitations and constraints of ArubaOS MIBs.

**Table 7** *Limitations and Constraints*

MIB	Module	Limitation
Switch Module	wlsxSwitchListTable	Information can only be queried from the master switch—only the table of the master switch is populated. If a local switch is queried, an empty table will be returned.
Switch Module	wlsxSwitchGlobalAPTable	Information can only be queried from the master switch—only the table of the master switch is populated. If a local switch is queried, an empty table is returned.
Textual Conventions	<i>All objects</i>	Textual conventions objects do not include object identification (OID).

This chapter provides an overview of the ArubaOS MIB modules and traps. It all includes textual conventions. This chapter includes the following sections:

- “AP and AM Modules” on page 27
- “Authentication Module” on page 27
- “Controller Transport Service” on page 28
- “External Services Interface (ESI) Module” on page 28
- “IF External (IF EXT)” on page 28
- “Mesh Module” on page 28
- “Mobility Module” on page 28
- “Monitor Module” on page 28
- “Signal Noise Ratio (SNR) Module” on page 28
- “Switch Module” on page 29
- “System External Module” on page 29
- “Textual Conventions” on page 29
- “Traps Module” on page 29
- “Tunneled-Node Module” on page 29
- “User Module” on page 29
- “User6 module” on page 30
- “Voice Module” on page 30
- “Wireless Local Area Network Module” on page 30

## AP and AM Modules

The AP and AM module provides information about access points and air monitors. The access point (AP) is a device or an application that connects the wireless client to a local area network (LAN). APs continually poll the network and report information to the controllers. This feature can be used to enhance the security of wireless communication and to extend the range of a wireless user by connecting to a wireless device through a wired LAN.

The Dell AP can also function as an air monitor (AM), which scans the RF spectrum, and can be used to enhance the performance of the AP.

The AP and AM MIBs are listed in the file *aruba-ap.my*.

## Authentication Module

The Authentication module provides information about the authentication server, as well as entities that are attempting to access the network. Authentication is used to verify the entity that is communicating to a device.

The Authentication MIBs are listed in the file *aruba-auth.my*.



## Controller Transport Service

---

All MIB tables and MIB OIDs in the Controller Transport Service were deprecated in ArubaOS 5.0 and are no longer supported.

---

This module provides information about the Controller Transport Service. The Controller Transport Service (CTS) is used with the Mobility Manager for synchronizing configuration, database, and data sections. The CTS MIBs are used for triggering the data synchronization event with the MMS, such as *config update*.

CTS is not intended to be used with other applications.

The CTS MIBs are listed in the file *aruba-cts.my*.

## External Services Interface (ESI) Module

The External Services Interface (ESI) module provides information about the Wireless Management System (WMS) in the Dell controller. ESI is used for redirecting traffic to a virus scanner, context filter, or other third party network appliances.

The ESI MIBs are listed in the file *aruba-esi.my*.

## IF External (IF EXT)

IF External (IF EXT) MIB objects provide system-level information about the Dell controller—physical ports, configured VLANs, the port memberships, and the interfaces that define the VLANs.

The IF External MIBs are listed in the file *aruba-ifext.my*.

## Mesh Module

The Mesh module provides information about Mesh portal and topology in the Dell controller.

The Mesh MIBs are listed in the file *aruba-mesh.my*.

## Mobility Module

The Mobility module provides information about the subsystem in the Dell controller, such as the home agent (HA) or foreign agent (FA) of a roaming agent.

The Mobility MIBs are listed in the file *aruba-mobility.my*.

## Monitor Module

The Monitor module provides information about network traffic. Monitoring access points can be used to observe network traffic, such as the number of packets transferred at a specific rate, the number of errors per access point, and so on.

The Monitor MIBs are listed in the file *aruba-mon.my*.

## Signal Noise Ratio (SNR) Module

The Signal Noise Ratio (SNR) module provides information about signal quality and packets. One value of SNR is the signal quality during a sample period. The signal quality affects the quality of the transmitted

packets. The available SNR values include signal strength (total, maximum, minimum). Additional information is the number of packets that were transmitted during the sample time.

The SNR MIBs are listed in the file *aruba-snr.my*.

## Switch Module

The Switch module provides statistical information about Dell controllers, including storage and memory utilization, and the wireless stations associated with the access points.

The Switch MIBs are listed in the file *aruba-switch.my*.

## System External Module

The System External module provides information about resource usages such as memory and CPU.

The System External MIBs are listed in the file *aruba-systemext.my*.

## Textual Conventions

Textual conventions define the data structures of Dell object types. Textual Conventions are found in the file *aruba-tc.my*



---

Textual Conventions do not have OIDs.

---

## Traps Module

This module defines the Traps that can be generated by the controller. Traps are MIB objects (variables) that transmit information to the SNMP Manager when an event occurs. Traps are included as varbinds (variable bindings) in the trap protocol data unit (PDU). Varbinds are defined in the *Description* section below.

The Traps are listed in the file *aruba-trap.my* MIB file.

## Tunneled-Node Module

This module defines MIB objects that provide information about the Controller Transport (CTS) in the controller.

The mibs are listed in the *wlsxTunneledNodeMIB* file.

## User Module

The User module provides information about the *user*, the party connected to the controller. Information includes the total number of users, name and access-level of the user, the physical location of the user's station, and so on. *User* MIBs support IPv4.

The User MIBs are listed in the *aruba-user.my* file.

## User6 module

The User6 module supports IPv6 users. This module provides information about the users, the party connected to the controller. Information includes the total number of users, name and access-level of the user, the physical location of the user's station, and so on.

The User MIBs are listed in the file *aruba-user6.my*.

## Voice Module

The Voice module provides information about Voice call status and call detail reporting.

The Voice MIBs are listed in the file *aruba-voice.my*.

## Wireless Local Area Network Module

The wireless local area network (WLAN) module provides information about the Wireless Management System (WMS) in the Dell controller.

The WLAN MIBs are listed in the file *aruba-wlan.my*.

<b>A</b>	
access point .....	27
agent .....	28
air monitor .....	27
Alarm	
analog .....	17
discrete .....	17
ping .....	17
analog alarm inputs.....	17
AP .....	27
authentication.....	27
<b>C</b>	
call status.....	30
control relay .....	18
controller .....	29
CTS .....	28
<b>E</b>	
ESI .....	28
<b>F</b>	
FA .....	28
foreign agent .....	28
<b>H</b>	
HA.....	28
home agent .....	28
<b>I</b>	
inform request .....	17
<b>L</b>	
Location	
user station.....	29
<b>M</b>	
mesh .....	28
MIB files .....	19
modules .....	27
AM.....	27
authentication .....	27
controller transport service .....	28
External Services Interface (ESI) .....	28
IF External (IF EXT) .....	28
Mesh .....	28
mobility .....	28
monitor .....	28
Signal Noise Ratio (SNR) .....	28
switch .....	29
system external .....	29
traps.....	29
tunneled-node .....	29
user .....	29
User6.....	30
voice .....	30
Wireless Local Area Network (WLAN) .....	30
<b>N</b>	
network traffic.....	28
<b>P</b>	
ping alarms .....	17
ports .....	28
<b>R</b>	
roaming agent.....	28
<b>S</b>	
Scan	
RF spectrum.....	27
signal quality.....	28
SNR .....	28
<b>T</b>	
terminal server function .....	18
textual conventions .....	29
Traffic	
redirect .....	28
Traps	
information .....	17
types .....	17
<b>U</b>	
user access .....	29
<b>V</b>	
VLAN .....	28
voice status.....	30
<b>W</b>	
WMS .....	30

