Aruba Instant 6.3.1.1-4.0 MIB Reference Guide

Reference Guide

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. 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

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.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

Contents ... 3
About this Guide ... 16
Intended Audience ... 16
Related Documents ... 16
Conventions ... 16
Contacting Support ... 17
MIBs Overview ... 18
MIBs ... 18
SNMP ... 19
Using MIBs ... 22
Downloading MIB Files ... 22
Reporting WLAN Health ... 22
SNMP Operations on IAPs ... 22
MIB Browsers ... 23
Reading MIB Files ... 24
Opening Line ... 24
Imports ... 24
Inheritance ... 24
Identity ... 25
MIB Modules ... 25
Group ... 25
Table ... 25
Entry ... 25
Closing Line ... 26
SNMP File ... 26
HP OpenView ... 26
Aruba Instant MIBs ... 28
aiInfoGroup ... 29
aiVirtualControllerKey ... 29

aiVirtualControllerName 29
aiVirtualControllerOrganization 30
aiVirtualControllerVersion 30
aiVirtualControllerIPAddress 30
aiMasterIPAddress 30
aiStateGroup 30
aiAccessPointTable 31
aiAccessPointEntry 31
aiAPMACAddress 31
aiAPName 32
aiAPIPAddress 32
aiAPSerialNum 32
aiAPModel 32
aiAPModelName 32
aiAPCPUUtilization 32
aiAPMemoryFree 33
aiAPUptime 33
aiAPTotalMemory 33
aiAPStatus 33
aiRadioTable 33
aiRadioEntry 34
aiRadioAPMacAddress 34
aiRadioIndex 35
aiRadioMACAddress 35
aiRadioChannel 35
aiRadioTransmitPower 35
aiRadioNoiseFloor 35
aiRadioUtilization4 36
aiRadioUtilization64 36
aiRadioTxTotalFrames 36
aiRadioTxMgmtFrames 36
aiRadioTxDataFrames 36

aiRadioTxDataBytes 37
aiRadioTxDrops 37
aiRadioRxTotalFrames 37
aiRadioRxDataFrames 37
aiRadioRxDataBytes 37
aiRadioRxMgmtFrames 37
aiRadioRxBad 38
aiRadioPhyEvents 38
aiRadioStatus 38
aiWlanTable 38
aiWlanEntry 39
aiWlanAPMACAddress 39
aiWlanIndex 39
aiWlanESSID 39
aiWlanMACAddress 40
aiWlanTxTotalFrames 40
aiWlanTxDataFrames 40
aiWlanTxDataBytes 40
aiWlanRxTotalFrames 40
aiWlanRxDataFrames 40
aiWlanRxDataBytes 41
aiClientTable 41
aiClientEntry 42
aiClientMACAddress 42
aiClientWlanMACAddress 42
aiClientIPAddress 42
aiClientAPIPAddress 42
aiClientName 43
aiClientOperatingSystem 43
aiClientSNR 43
aiClientTxDataFrames 43
aiClientTxDataBytes 43

aiClientTxRetries 44
aiClientTxRate 44
aiClientRxDataFrames 44
aiClientRxDataBytes 44
aiClientRxRetries 44
aiClientRxRate 44
aiClientUptime 45
Standard SNMP MIBs 46
system MIB 46
sysDescr 46
sysObjectID 47
sysUpTime 47
sysName 47
sysLocation 47
sysServices 48
dot1qTpFdbTable 48
dot1qFdbId 48
dot1qTpFdbAddress 48
dot1qTpFdbPort 48
dot1qTpFdbStatu 49
ifTable 49
ifIndex 50
ifDescr 50
ifType 50
ifMtu 50
ifSpeed 51
ifPhysAddress 51
ifAdminStatus 51
ifOperStatus 51
ifInOctets 52
ifInUcastPkts 52
ifInNUcastPkts 52

ifInDiscards 52
ifInErrors 52
ifOutOctets 53
ifOutUcastPkts 53
ifOutDiscards 53
ifOutErrors 53
ifXTable 54
ifName 54
ifInMulticastPkts 54
ifInBroadcastPkts 55
ifOutMulticastPkts 55
ifOutBroadcastPkts 55
ifHCInOctets 55
ifHCInUcastPkts 56
ifHCInMulticastPkts 56
ifHCInBroadcastPkts 56
ifHCOutOctets 57
ifHCOutUcastPkts 57
ifHCOutMulticastPkts 57
ifHCOutBroadcastPkts 57
ifLinkUpDownTrapEnable 58
ifPromiscuousMode 58
ifConnectorPresent 58
Traps 60
Trap Hierarchy 60
wlsxTrapAPMacAddress 66
wlsxTrapAPIpAddress 67
wlsxTrapAPBSSID 67
wlsxTrapEssid 67
wlsxTrapTargetAPBSSID 67
wlsxTrapTargetAPSSID 67
wlsxTrapTargetAPChannel 68

wlsxTrapNodeMac 68
wlsxTrapSourceMac 68
wlsxReceiverMac 68
wlsxTrapTransmitterMac 69
wlsxTrapReceiverMac 69
wlsxTrapSnr 69
wlsxTrapSignatureName 69
wlsxTrapFrameType 69
wlsxTrapAddressType 69
wlsxTrapAPLocation 70
wlsxTrapAPChannel 70
wlsxTrapAPTxPower 70
wlsxTrapMatchedMac 70
wlsxTrapMatchedIp 70
wlsxTrapRogueIfoURL 71
wlsxTrapVLANId 71
wlsxTrapAdminStatus 71
wlsxTrapOperStatus 71
wlsxTrapAuthServerName 71
wlsxTrapAuthServerTimeout 72
wlsxTrapCardSlot 72
wlsxTrapTemperatureValue 72
wlsxTrapProcessName 72
wlsxTrapFanNumber 72
wlsxTrapVoltageType 72
wlsxTrapVoltageValue 73
wlsxTrapStationBlackListReason 73
wlsxTrapSpoofedIpAddress 73
wlsxTrapSpoofedOldPhyAddress 73
wlsxTrapSpoofedNewPhyAddress 73
wlsxTrapDBName 74
wlsxTrapDBUserName 74

wlsxTrapDBIpAddress 74
wlsxTrapDBType 74
wlsxTrapVrrpID 74
wlsxTrapVrrpMasterIp 74
wlsxTrapVrrpOperState 75
wlsxTrapESIServerGrpName 75
wlsxTrapESIServerName 75
wlsxTrapESIServerIpAddress 75
wlsxTrapLicenseDaysRemaining 75
wlsxTrapSwitchIp 76
wlsxTrapSwitchRole 76
wlsxTrapUserIpAddress 76
wlsxTrapUserPhyAddress 76
wlsxTrapUserName 76
wlsxTrapUserRole 76
wlsxTrapUserAuthenticationMethod 77
wlsxTrapAPRadioNumber 77
wlsxTrapRogueInfoURL 77
wlsxTrapInterferingAPInfoURL 77
wlsxTrapPortNumber 77
wlsxTrapTime 78
wlsxTrapHostIp 78
wlsxTrapHostPort 78
wlsxTrapConfigurationId 78
wlsxTrapCTSURL 78
wlsxTrapCTSTransferType 79
wlsxTrapConfigurationState 79
wlsxTrapUpdateFailureReason 79
wlsxTrapUpdateFailedObj 79
wlsxTrapTableEntryChangeType 79
wlsxTrapGlobalConfigObj 79
wlsxTrapTableGenNumber 80

wlsxTrapLicenseId 80
wlsxTrapConfidenceLevel 80
wlsxTrapMissingLicenses 80
wlsxVoiceCurrentNumCdr 80
wlsxTrapTunnelId 81
wlsxTrapTunnelStatus 81
wlsxTrapTunnelUpReason 81
wlsxTrapTunnelDownReason 81
wlsxTrapApSerialNumber 81
wlsxTraptimeStr 82
wlsxTrapMasterIp 82
wlsxTrapLocalIp 82
wlsxTrapMasterName 82
wlsxTrapLocalName 82
wlsxTrapPrimaryControllerIp 82
wlsxTrapBackupControllerIp 83
wlsxTrapSpoofedFrameType 83
wlsxTrapAssociationType 83
wlsxTrapDeviceIpAddress 83
wlsxTrapDeviceMac 83
wlsxTrapVcIpAddress 84
wlsxTrapVcMacAddress 84
wlsxTrapAPName 84
wlsxTrapApMode 84
wlsxTrapAPPrevChannel 84
wlsxTrapAPPrevChannelSec 85
wlsxTrapAPPrevTxPower 85
wlsxTrapAPCurMode 85
wlsxTrapAPPrevMode 85
wlsxTrapAPARMChangeReason 85
wlsxTrapAPChannelSec 85
wlsxTrapUserAttributeChangeType 86

wlsxTrapAPControllerIp 86
wlsxTrapApMasterStatus 86
wlsxTrapCaName 86
wlsxTrapCrlName 86
wlsxTrapCount 87
wlsxTrapAPPreviousUplinkType 87
wlsxTrapAPPreviousUplinkActiveTime 87
wlsxTrapAPActiveUplinkType 87
wlsxTrapAPUplinkChangeReason 87
wlsxTrapAPManagedModeConfigFailure 87
ai Traps Definitions Group 88
wlsxNUserEntryCreated 96
wlsxNUserEntryDeleted 96
wlsxNUserEntryAuthenticated 96
wlsxNUserEntryDeAuthenticated 96
wlsxNUserAuthenticationFailed 96
wlsxNAuthServerReqTimedOut 97
wlsxNAuthServerTimedOut 97
wlsxNAuthServerIsUp 97
wlsxNAccessPointIsUp 97
wlsxNChannelChanged 97
wlsxNStationAddedToBlackList 98
wlsxNStationRemovedFromBlackList 98
wlsxNRadioAttributesChanged 98
wlsxUnsecureAPDetected 98
wlsxUnsecureAPResolved 98
wlsxStaImpersonation 99
wlsxReservedChannelViolation 99
wlsxValidSSIDViolation 99
wlsxChannelMisconfiguration 99
wlsxOUIMisconfiguration 99
wlsxSSIDMisconfiguration 100

wlsxShortPreableMisconfiguration 100
wlsxWPAMisconfiguration 100
wlsxAdhocNetworkDetected 100
wlsxAdhocNetworkRemoved 100
wlsxStaPolicyViolation 101
wlsxRepeatWEPIVViolation 101
wlsxWeakWEPIVViolation 101
wlsxChannelInterferenceDetected 101
wlsxChannelInterferenceCleared 101
wlsxAPInterferenceDetected 102
wlsxAPInterferenceCleared 102
wlsxStaInterferenceDetected 102
wlsxStaInterferenceCleared 102
wlsxFrameRetryRateExceeded 102
wlsxFrameReceiveErrorRateExceeded 103
wlsxFrameFragmentationRateExceeded 103
wlsxFrameBandWidthRateExceeded 103
wlsxFrameLowSpeedRateExceeded 103
wlsxFrameNonUnicastRateExceeded 103
wlsxLoadbalancingEnabled 104
wlsxLoadbalancingDisabled 104
wlsxChannelFrameRetryRateExceeded 104
wlsxChannelFrameFragmentationRateExceeded 104
wlsxChannelFrameErrorRateExceeded 104
wlsxSignatureMatchAP 105
wlsxSignatureMatchSta 105
wlsxChannelRateAnomaly 105
wlsxNodeRateAnomaly 105
wlsxNodeRateAnomalyAP 105
wlsxNodeRateAnomalySta 106
wlsxEAPRateAnomaly 106
wlsxSignalAnomaly 106

wlsxSequenceNumberAnomalyAP 106
wlsxSequenceNumberAnomalySta 107
wlsxDisconnectStationAttack 107
wlsxApFloodAttack 107
wlsxAdhocNetwork 107
wlsxWirelessBridge 108
wlsxInvalidMacOUIAP 108
wlsxInvalidMacOUISta 108
wlsxWEPMisconfiguration 108
wlsxStaRepeatWEPIVViolation 108
wlsxStaWeakWEPIVViolation 109
wlsxStaAssociatedToUnsecureAP 109
wlsxStaUnAssociatedFromUnsecureAP 109
wlsxAdhocNetworkBridgeDetected 109
wlsxInterferingApDetected 109
wlsxColdStart 110
wlsxWarmStart 110
wlsxAPImpersonation 110
wlsxNAuthServerIsDown 110
wlsxWindowsBridgeDetected 110
wlsxSignAPNetstumbler 110
wlsxSignStaNetstumbler 111
wlsxSignAPAsleap 111
wlsxSignStaAsleap 111
wlsxSignAPAirjack 111
wlsxSignStaAirjack 111
wlsxSignAPNullProbeResp 112
wlsxSignStaNullProbeResp 112
wlsxSignAPDeauthBcast 112
wlsxSignStaDeauthBcast 112
wlsxNStaUnAssociatedFromUnsecureAP 117
wlsxOmertaAttack 117

wlsxTKIPReplayAttack 117
wlsxChopChopAttack 117
wlsxFataJackAttack 118
wlsxInvalidAddressCombination 118
wlsxValidClientMisassociation 118
wlsxMalformedHTIEDetected 118
wlsxMalformedAssocReqDetected 118
wlsxOverflowIEDetected 119
wlsxOverflowEAPOLKeyDetected 119
wlsxMalformedFrameLargeDurationDetected 119
wlsxMalformedFrameWrongChannelDetected 119
wlsxMalformedAuthFrame 119
wlsxCTSRateAnomaly 120
wlsxRTSRateAnomaly 120
wlsxNRogueAPDetected 120
wlsxNRogueAPResolved 120
wlsxNeighborAPDetected 120
wlsxNInterferingAPDetected 121
wlsxNSuspectRogueAPResolved 121
wlsxBlockAckAttackDetected 121
wlsxHotspotterAttackDetected 121
wlsxNSignatureMatch 122
wlsxNSignatureMatchNetstumbler 122
wlsxNSignatureMatchAsleap 122
wlsxNSignatureMatchAirjack 122
wlsxNSignatureMatchNullProbeResp 122
wlsxNSignatureMatchDeauthBcast 123
wlsxNSignatureMatchDisassocBcast 123
wlsxNSignatureMatchWellenreiter 123
wlsxAPDeauthContainment 124
wlsxClientDeauthContainment 124
wlsxAPWiredContainment 124

wlsxClientWiredContainment 124
wlsxAPTaggedWiredContainment 124
wlsxClientTaggedWiredContainment 125
wlsxTarpitContainment 125
wlsxAPChannelChange 125
wlsxAPPowerChange 125
wlsxAPModeChange 125
wlsxUserEntryAttributesChanged 126
wlsxNAPMasterStatusChange 126
wlsxNAdhocUsingValidSSID 126
wlsxMgmtUserAuthenticationFailed 126
SNMP Traps 127
linkDown 127
linkUp 127

This guide provides information on the MIBs supported by . This guide provides information on Management Information Base (MIBs) supported in Aruba Instant 6.3.1.1-4.0 software release.

Intended Audience

This manual is intended for network administrators and operators responsible for managing the Aruba Instant Access Point (IAP).

Related Documents

In addition to this document, the Instant product documentation includes the following:

- *Aruba Instant 6.3.1.1-4.0 User Guide*
- *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*
- *Aruba Instant 6.3.1.1-4.0 Quick Start Guide*
- *Aruba Instant 6.3.1.1-4.0 Syslog Messages Reference Guide*
- *Aruba Instant 6.3.1.1-4.0 Release Notes*

Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Table 1: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: • Sample screen output • System prompts • Filenames, software devices, and specific commands when mentioned in the text
`Commands`	In the command examples, this style depicts the keywords that must be typed exactly as shown.
<*Arguments*>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: # **send** <*text message*> In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
`[Optional]`	Command examples enclosed in brackets are optional. Do not type the brackets.
`{Item A | Item B}`	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

The following informational icons are used throughout this guide:

Indicates helpful suggestions, pertinent information, and important things to remember.

Indicates a risk of damage to your hardware or loss of data.

Indicates a risk of personal injury or death.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	licensing.arubanetworks.com/login.php
Wireless Security Incident Response Team (WSIRT)	arubanetworks.com/support/wsirt.php
Support Email Addresses	
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

This chapter provides information about Management Information Base (MIBs) supported in Aruba Instant 6.3.1.1-4.0 software release.

MIBs

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

MIB objects, such as a MIB table or a specific object in a MIB table, are identified with Object identifiers (OIDs). The OIDs are designated by text strings and integer sequences. For example, Aruba and *1.3.6.1.4.1.14823* both represent the private enterprise node *Aruba*. *Aruba* is the parent of the proprietary MIBs that are supported on Instant.

Figure 1 illustrates the high-level hierarchy of the Enterprise MIBs.

Figure 1 *High-Level MIB Hierarchy*

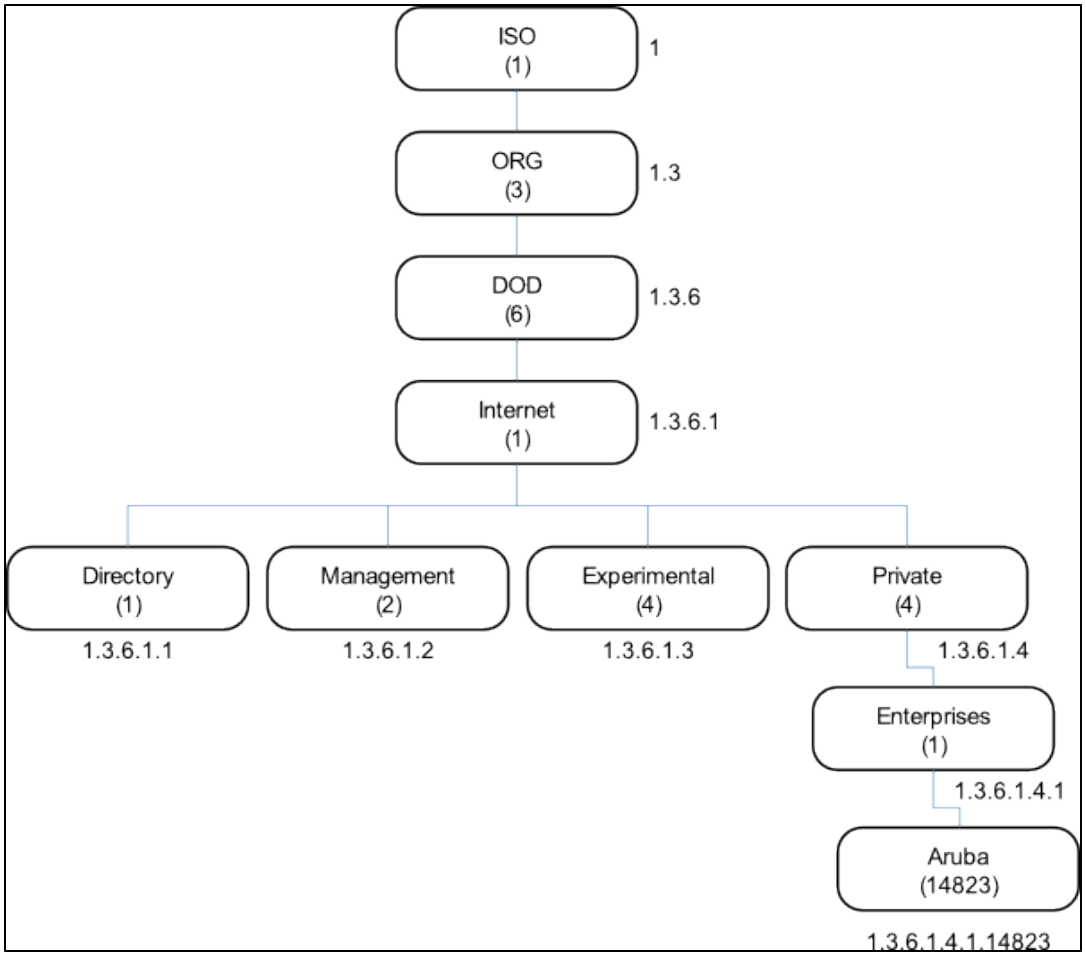


Table 2 indicates the numerical string that lists the nodes of the enterprise MIB hierarchy.

Table 2: *MIB Node Identification - Enterprise Nodes*

		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
14823	1.3.6.1.4.1.14823	Aruba

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 24.

SNMP

MIB objects can be accessed through the Simple Network Management Protocol (SNMP). To deliver information between devices, every object referenced in an SNMP message must be listed in the MIB. A component of a device that is not described in a MIB cannot be recognized by SNMP as there is no information for SNMP managers and SNMP agents to exchange.

The significant elements of SNMP are Managers, Agents, and MIBs:

- SNMP Managers (software application) are used for communicating and managing the devices that support SNMP Agents. SNMP Managers can also be used for sending configuration updates or controlling requests to manage a network device.
- SNMP Agents (software application) provide information from the network devices to the SNMP Managers. Network devices include workstations, routers, microwave radios, and other network components.
- 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.

Aruba Instant MIBs support SNMPv1, SNMPv2, and SNMPv3. For information on configuring SNMP through the Instant UI, see *Aruba Instant 6.3.1.1-4.0 User Guide*.

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

- SNMP version
- SNMP community name–*public* or *private*
- The IP Address of the virtual controller
- The OID of the MIB object

Table 3: *MIB Keywords*

Keyword	Description
Sequence	Refers to the sequence of objects of the MIB. This keyword is used with entry MIB objects to list the MIB objects that exchange information.
Syntax	Textual conventions, for example, *Integer32*.
Max-Access	Defines the object accessibility: • *read-only*: Can be retrieved but not modified • *read-write:* Can be retrieved and modified • *not-accessible*: Cannot be retrieved; it is for internal (device) use only • *accessible-for-notify*: Can be retrieved when a trap message (notification) is sent
Status	Defines the status of the object: • *current*: Indicates that the object status is up-to-date and valid. • *deprecated*: Indicates an obsolete definition. It permits new or continued implementation to maintain interoperability with existing implementations. • *obsolete*: Obsolete. It should not be implemented and/or can be removed if previously implemented.
Description	A text string that describes the object.

In addition, MIB files can be placed in the appropriate disk location to assist the user in locating desired OID values for monitoring.

It is assumed that the workstation is connected to the Instant and 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
```

If you are using an application that is run through the Linux shell, the command will be as follows:

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

The MIB objects can also be viewed from a MIB Browser GUI.

This chapter provides information on using MIBs.

- Downloading MIB Files on page 22
- Reporting WLAN Health on page 22
- Reading MIB Files on page 24
- SNMP File on page 26
- HP OpenView on page 26

Downloading MIB Files

The latest Instant MIB files are available for registered customers at:

https://support.arubanetworks.com

For assistance to set up an account and access files, contact customer service. See Contacting Support on page 17.

Reporting WLAN Health

SNMP MIBs are frequently used for running health checks on Aruba Instant devices, through a MIB browser application.

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

- SNMP version
- SNMP community name—*public* or *private*
- The IP Address of the Virtual Controller and the slave IAPs
- The OID of the MIB value you want to monitor

MIB files can be placed in the appropriate disk location to assist the user in locating desired OID values for monitoring. For most applications, the *root* of the MIB must be included in the OID—the OID begins with a decimal point as shown in the following example:

```
.1.3.6.1.4.1.674.2.2.1.1.2.1
```

SNMP Operations on IAPs

Although the virtual controller address is configured on management station, the following MIBs are specific to a particular IAP and therefore cannot be accessed from the Virtual Controller.

- ifTable
- ifXTable
- dot1qTpFdbTable

To enable the management station to access the IF-MIB and Q-BRIDGE-MIB tables and IAPs to send traps, you must configure the IP address of each IAP on the management station. The management station can automatically configure the IAP details, by obtaining the IP address of each IAP from the AP MIB (aiAccessPointTable), which lists all the slave IAPs in a swarm and is implemented on a virtual controller.

You do not have to set the SNMP community string and security parameters on each IAP as this configuration is common to all IAPs and is inherited from virtual controller.

MIB Browsers

If you are using an application that is run through the Linux shell, the command would be as follows:

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

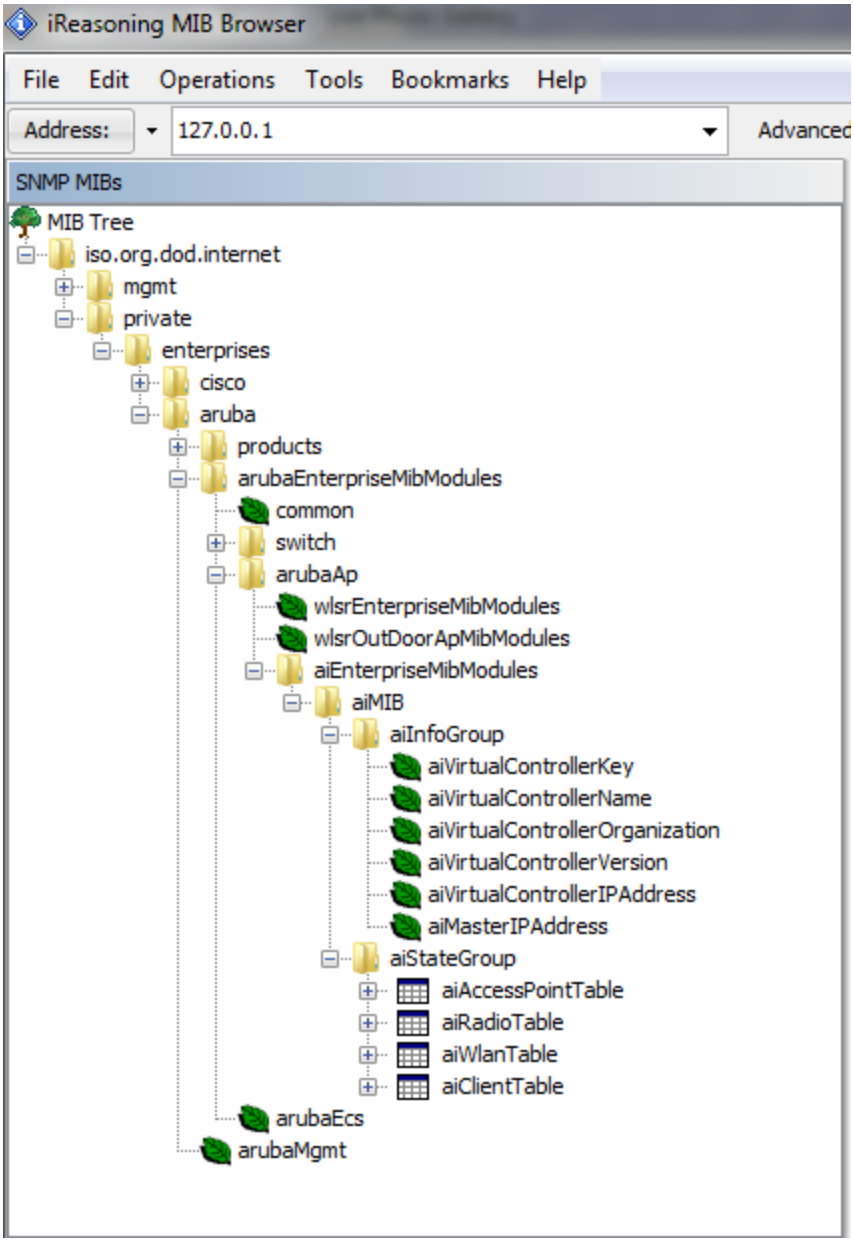
Figure 2 shows an example of submitting a command to obtain information.

Figure 2 *Running the snmpget Command*

```
[root@localhost ~]# snmpget -v 2c -c public 10.65.77.8 .1.3.6.1.4.1.14823.2.3.3.1.1.2.0
SNMPv2-SMI::enterprises.14823.2.3.3.1.1.2.0 = STRING: "Instant-CB:A5:52"
```

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, view the file snmp.h. For more information, see SNMP File on page 26.

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 Aruba enterprise MIB file, *aruba-cts.my*, are as follows.

Opening Line

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

```
AI-AP-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
FROM SNMPv2-TC

MODULE-IDENTITY,
OBJECT-TYPE,
snmpModules,
Integer32,
Counter32,
Counter64,
IpAddress,
NOTIFICATION-TYPE
FROM SNMPv2-SMI

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

OBJECT-GROUP
FROM SNMPv2-CONF
aiEnterpriseMibModules
FROM ARUBA-MIB;
```

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 OID can be determined from the parent object as follows.

aiEnterpriseMibModules is the parent object –its OID is `1.3.6.1.4.1.14823.2.3.3.`

aiStateGroup OBJECT IDENTIFIER ::= { aiMIB 2 }, the OID is `1.3.6.1.4.1.14823.2.3.3.1.2.`

aiVirtualControllerKey OBJECT-TYPE, the OID is 1.3.6.1.4.1.14823.2.3.3.1.1.1.0.

All MIBs and their related OIDs are listed in the snmp file. For more information, see SNMP File on page 26.

aiEnterpriseMibModules

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.

```
aiMIB MODULE-IDENTITY
 LAST-UPDATED "0804160206Z"
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 is for managing Aruba Instant WLAN"
REVISION "0804160206Z"
DESCRIPTION
"The initial revision."
::= { aiEnterpriseMibModules 1 }
```

MIB Modules

MIB objects can be placed in logical groups such as Group and Table. A group typically contains at least one global-object or table. The table lists the MIB objects that contain the information exchanged.

The first object of a table is an Entry. The OIDs of the subsequent objects of this table are appended increments of the Entry OID.

The keyword SEQUENCE lists the objects of the table that contain device information. Each subsequent object (Informative MIB Object) inherits the OID of the Entry, and contains information sorted by the Syntax, Access, Status, and Description keywords.

Group

```
aiStateGroup OBJECT IDENTIFIER ::= { aiMIB 2 }
```

Table

```
aiAccessPointTable OBJECT-TYPE
SYNTAX SEQUENCE OF AiAccessPointEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"This contains all access points connected to the
virtual controller. This table is empty on AP where
virtual controller is not active"
::= { aiStateGroup 1 }
```

Entry

```
 aiAccessPointEntry OBJECT-TYPE
```

```
 SYNTAX AiAccessPointEntry
 MAX-ACCESS not-accessible
 STATUS current
 DESCRIPTION
 " "
 INDEX { aiAPMACAddress }
 ::= { aiAccessPointTable 1 } AiAccessPointEntry ::=
SEQUENCE {
aiAPMACAddress MacAddress,
aiAPName DisplayString,
aiAPIPAddress IpAddress,
aiAPSerialNum DisplayString,
aiAPModel OBJECT IDENTIFIER,
aiAPModelName DisplayString,
aiAPCPUUtilization Integer32,
aiAPMemoryFree Integer32,
aiAPUptime TimeTicks
```

Closing Line

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

```
END
```

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*.

The SNMP file with all Aruba MIBs is listed in Standard SNMP MIBs on page 46.

All Instant MIBs inherit their OIDs from the Aruba 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") },`

HP OpenView

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

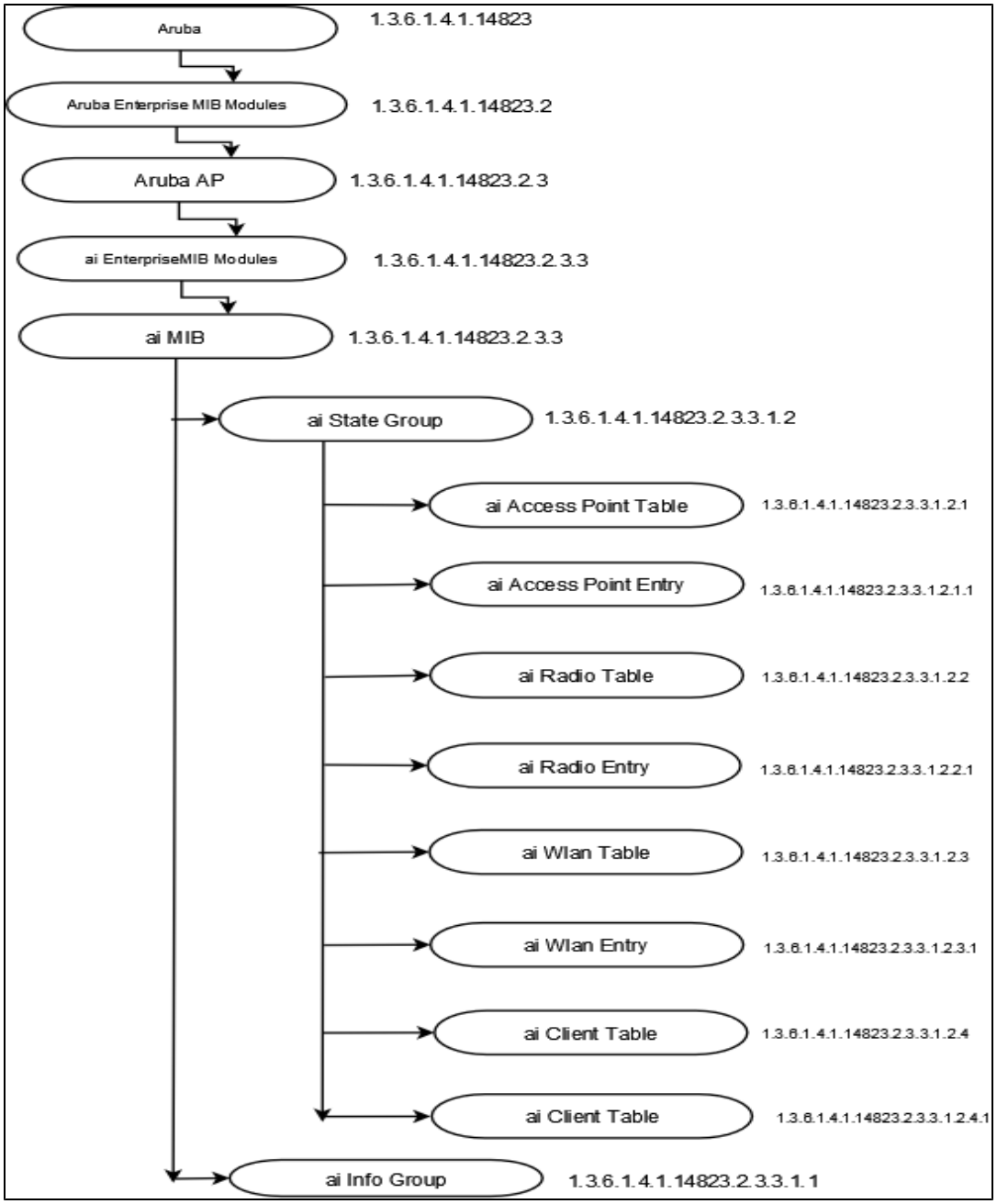
```
# $OV_CONTRIB/NNM/Aruba/install
```

The chapter provides information about the Aruba Instant MIB objects.

Figure 4 shows the architecture of the Aruba Instant MIB relative to 1.3.6.1.4.1.14823 (iso.org.dod.internet.private.enterprise.aruba).

The Instant MIB is listed in the file *aruba-instant.my*. For information about downloading Instant MIB file, see Downloading MIB Files on page 22.

Figure 4 *Instant MIB Hierarchy*



The Instant MIB tree consists of the following MIB groups and tables.

Table 4: *Supported Instant MIBs and MIB Tables*

Group	Description
aiInfoGroup	Contains details of the virtual controller. For more information, see aiInfoGroup on page 29.
aiStateGroup	Contains information about status of the Access Point, Radio, WLAN, and Clients connected to an IAP. The following tables are available in the aiInfoGroup: • **aiAccessPointTable**–Contains all the access points connected to the virtual controller. This table is indexed by the MAC Address of the IAP. • **aiRadioTable**–Contains all the radios of the access points connected to the virtual controller. This table is indexed by the MAC Address and radio number. • **aiWlanTable**–Contains all the BSSIDs that are active on the virtual controller. This table is indexed by the MAC address and a WLAN Index of the IAP. • **aiClientTable**–Contains information about all the clients connected to the virtual controller. When a client roams from one access point to another, all the counters in this table are reset to 0. For more information, see aiStateGroup on page 30.
aiTrapGroup	Contains the details of traps that can be generated on an IAP. For more information, see Trap Hierarchy on page 60.

aiInfoGroup

The aiInfoGroup table provides information about the virtual controller:

- aiVirtualControllerKey
- aiVirtualControllerName
- aiVirtualControllerOrganization
- aiVirtualControllerVersion
- aiVirtualControllerIPAddress
- aiMasterIPAddress

aiVirtualControllerKey

Object ID	1.3.6.1.4.1.14823.2.3.3.1.1.1
Syntax	DisplayString
Max-Access	Read-only
Status	Current
Description	Unique Virtual Controller key

aiVirtualControllerName

Object ID	1.3.6.1.4.1.14823.2.3.3.1.1.2
Syntax	DisplayString
Max-Access	Read-only
Status	Current
Description	Name of the Virtual Controller

aiVirtualControllerOrganization

Object ID	1.3.6.1.4.1.14823.2.3.3.1.1.3
Syntax	DisplayString
Max-Access	Read-only
Status	Current
Description	Virtual Controller organization

aiVirtualControllerVersion

Object ID	1.3.6.1.4.1.14823.2.3.3.1.1.4
Syntax	DisplayString
Max-Access	Read-only
Status	Current
Description	Software version of the controller

aiVirtualControllerIPAddress

Object ID	1.3.6.1.4.1.14823.2.3.3.1.1.5
Syntax	IPAddress
Max-Access	Read-only
Status	Current
Description	IP address of the Virtual Controller. If this is not set, returns 0.0.0.0.

aiMasterIPAddress

Object ID	1.3.6.1.4.1.14823.2.3.3.1.1.6
Syntax	IPAddress
Max-Access	Read-only
Status	Current
Description	

aiStateGroup

The aiStateGroup contains the following tables:

- aiAccessPointTable
- aiRadioTable
- aiWlanTable

- aiClientTable

aiAccessPointTable

The objects of the **aiAccessPointTable** provide information about all the IAPs connected to the virtual controller.

Table 5: *aiAccessPointTable OIDs*

Object	Object ID	Entry OID
aiAccessPointEntry	1.3.6.1.4.1.14823.2.3.3.1.2.1.1	aiAccessPointTable 1
aiAPMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.1	aiAccessPointEntry 1
aiAPName	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.2	aiAccessPointEntry 2
aiAPIPAddress	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.3	aiAccessPointEntry 3
aiAPSerialNum	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.4	aiAccessPointEntry 4
aiAPModel	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.5	aiAccessPointEntry 5
aiAPModelName	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.6	aiAccessPointEntry 6
aiAPCPUUtilization	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.7	aiAccessPointEntry 7
aiAPMemoryFree	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.8	aiAccessPointEntry 8
aiAPUptime	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.9	aiAccessPointEntry 9
aiAPTotalMemory	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.10	aiAccessPointEntry 10
aiAPStatus	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.11	aiAccessPointEntry 11

aiAccessPointEntry

Syntax	aiAccessPointEntry
Max-Access	not-accessible
Status	current
Description	NA
Index	aiAPMACAddress

aiAPMACAddress

Syntax	MacAddress (OCTET STRING). Hint: 1x:
Max-Access	read-only
Status	current
Description	MAC address of the Access Point.

aiAPName

Syntax	DisplayString (SIZE(0..64))
Max-Access	read-only
Status	current
Description	Name of the Access Point.

aiAPIPAddress

Syntax	IpAddress
Max-Access	read-only
Status	current
Description	IP address of the Access Point.

aiAPSerialNum

Syntax	DisplayString (SIZE(0..64))
Max-Access	read-only
Status	current
Description	Serial number of the Access Point.

aiAPModel

Syntax	OBJECT IDENTIFIER
Max-Access	read-only
Status	current
Description	Access Point System OID.

aiAPModelName

Syntax	DisplayString (SIZE(0..32))
Max-Access	read-only
Status	current
Description	Model name of the Access Point.

aiAPCPUUtilization

Syntax	Integer32
Max-Access	read-only

Status	current
Description	CPU utilization of the Access Point.

aiAPMemoryFree

Syntax	Integer32
Max-Access	read-only
Status	current
Description	Amount of memory free in the access point in bytes.

aiAPUptime

Syntax	TimeTicks
Max-Access	read-only
Status	current
Description	Uptime of the Access Point.

aiAPTotalMemory

Syntax	Integer32
Max-Access	read-only
Status	current
Description	Total amount of memory available in the AP in bytes.

aiAPStatus

Syntax	Integer {up(1), down(2)}
Max-Access	read-only
Status	current
Description	Indicates the Access Point Status.

aiRadioTable

The objects of the aiRadioTable provide information about all the radios and the related information of the Access Points.

Table 6: *aiRadioTable OIDs*

Object	Object ID	Entry OID
aiRadioEntry	1.3.6.1.4.1.14823.2.3.3.1.2.2.1	aiRadioTable 1

Object	Object ID	Entry OID
aiRadioAPMacAddress	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.1	aiRadioEntry 1
aiRadioIndex	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.2	aiRadioEntry 2
aiRadioMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.3	aiRadioEntry 3
aiRadioChannel	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.4	aiRadioEntry 4
aiRadioTransmitPower	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.5	aiRadioEntry 5
aiRadioNoiseFloor	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.6	aiRadioEntry 6
aiRadioUtilization4	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.7	aiRadioEntry 7
aiRadioUtilization64	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.8	aiRadioEntry 8
aiRadioTxTotalFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.9	aiRadioEntry 9
aiRadioTxMgmtFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.10	aiRadioEntry 10
aiRadioTxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.11	aiRadioEntry 11
aiRadioTxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.12	aiRadioEntry 12
aiRadioTxDrops	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.13	aiRadioEntry 13
aiRadioTxTotalFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.14	aiRadioEntry 14
aiRadioRxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.15	aiRadioEntry 15
aiRadioRxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.16	aiRadioEntry 16
aiRadioRxMgmtFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.17	aiRadioEntry 17
aiRadioRxBad	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.18	aiRadioEntry 18
aiRadioPhyEvents	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.19	aiRadioEntry 19
aiRadioStatus	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.20	aiRadioEntry 20

aiRadioEntry

Syntax aiRadioEntry

Max-Access not-accessible

Status current

Description NA

Index aiRadioAPMACAddress, aiRadioIndex

aiRadioAPMacAddress

Syntax MacAddress (OCTET STRING). Hint: 1x:

Max-Access	read-only
Status	current
Description	MAC Address of the Access Point where this radio is active.

aiRadioIndex

Syntax	Integer32
Max-Access	read-only
Status	current
Description	Radio number of the Access Point.

aiRadioMACAddress

Syntax	MacAddress
Max-Access	read-only
Status	current
Description	Radio MAC address of the Access Point.

aiRadioChannel

Syntax	Integer32
Max-Access	read-only
Status	current
Description	Radio channel. The first byte contains primary channel and first two bits of second byte contains indicator for the secondary channel. If first two bits of second byte are 0, it is a 20MHz channel. If first two bits of second byte are 01, the secondary channel is above primary channel, if first two bits of second byte are 10, the secondary channel is below the primary channel.

aiRadioTransmitPower

Syntax	Integer32
Max-Access	read-only
Status	current
Description	Radio transmission power of the Access Point.

aiRadioNoiseFloor

Syntax	Integer32

Max-Access	read-only
Status	current
Description	Radio noise of the Access Point in dBm.

aiRadioUtilization4

Syntax	Integer32
Max-Access	read-only
Status	current
Description	Radio channel utilization 4 second average.

aiRadioUtilization64

Syntax	Integer32
Max-Access	read-only
Status	current
Description	Radio channel utilization 64 second average.

aiRadioTxTotalFrames

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of frames transmitted.

aiRadioTxMgmtFrames

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of management frames transmitted.

aiRadioTxDataFrames

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of data frames transmitted.

aiRadioTxDataBytes

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of data bytes transmitted.

aiRadioTxDrops

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of frames dropped during transmission.

aiRadioRxTotalFrames

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of received frames.

aiRadioRxDataFrames

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of received data frames.

aiRadioRxDataBytes

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of received data bytes.

aiRadioRxMgmtFrames

Syntax	Counter32
Max-Access	read-only

Status	current
Description	Total number of received management frames.

aiRadioRxBad

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of frames received in error.

aiRadioPhyEvents

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Number of physical layer events that indicates frames not received because of interference.

aiRadioStatus

Syntax	Integer {up(1), down(2)}
Max-Access	read-only
Status	current
Description	Indicates the radio status of the AP.

aiWlanTable

The objects of the aiWlanTable provide information about all the BSSIDs active on the virtual controller.

Table 7: *aiWlanTable OIDs*

Object	Object ID	Entry OID
aiWlanEntry	1.3.6.1.4.1.14823.2.3.3.1.2.3.1	aiWlanTable 1
aiWlanAPMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.1	aiWlanEntry 1
aiWlanIndex	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.2	aiWlanEntry 2
aiWlanESSID	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.3	aiWlanEntry 3
aiWlanMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.4	aiWlanEntry 4

Object	Object ID	Entry OID
aiWlanTxTotalFrames	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.5	aiWlanEntry 5
aiWlanTxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.6	aiWlanEntry 6
aiWlanTxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.7	aiWlanEntry 7
aiWlanRxTotalFrames	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.8	aiWlanEntry 8
aiWlanRxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.9	aiWlanEntry 9
aiWlanRxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.10	aiWlanEntry 10

aiWlanEntry

Syntax	AiWlanEntry
Max-Access	not-accessible
Status	current
Description	NA
Index	aiWlanAPMACAddress, aiWlanIndex

aiWlanAPMACAddress

Syntax	MacAddress (OCTET STRING). Hint: 1x:
Max-Access	read-only
Status	current
Description	MAC Address of the Access Point where WLAN is active.

aiWlanIndex

Syntax	Integer32
Max-Access	read-only
Status	current
Description	Index of the WLAN. This is a unique index assigned to the active WLAN on the Access Point.

aiWlanESSID

Syntax	DisplayString
Max-Access	read-only
Status	current
Description	ESSID of the WLAN

aiWlanMACAddress

Syntax	MacAddress (OCTET STRING). Hint: 1x:
Max-Access	read-only
Status	current
Description	BSSID of the WLAN

aiWlanTxTotalFrames

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of frames transmitted.

aiWlanTxDataFrames

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of data frames transmitted.

aiWlanTxDataBytes

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of data bytes transmitted.

aiWlanRxTotalFrames

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of received frames.

aiWlanRxDataFrames

Syntax	Counter32
Max-Access	read-only

Status	current
Description	Total number of received data frames.

aiWlanRxDataBytes

Syntax	Counter32
Max-Access	read-only
Status	current
Description	Total number of received data bytes.

aiClientTable

The objects of the aiWlanTable provide information about all the clients connected to the virtual controller.

Table 8: *aiClientTable OID*

Object	Object ID	Entry OID
aiClientEntry	1.3.6.1.4.1.14823.2.3.3.1.2.4.1	aiClientTable 1
aiClientMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.1	aiClientEntry 1
aiClientWlanMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.2	aiClientEntry 2
aiClientIPAddress	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.3	aiClientEntry 3
aiClientAPIPAddress	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.4	aiClientEntry 4
aiClientName	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.5	aiClientEntry 5
aiClientOperatingSystem	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.6	aiClientEntry 6
aiClientSNR	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.7	aiClientEntry 7
aiClientTxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.8	aiClientEntry 8
aiClientTxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.9	aiClientEntry 9
aiClientTxRetries	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.10	aiClientEntry 10
aiClientTxRate	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.11	aiClientEntry 11
aiClientRxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.12	aiClientEntry 12
aiClientRxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.13	aiClientEntry 13
aiClientRxRetries	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.14	aiClientEntry 14
aiClientRxRate	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.15	aiClientEntry 15
aiClientUptime	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.16	aiClientEntry 16

aiClientEntry

Syntax	aiClientEntry
Max-Access	not-accessible
Status	current
Description	NA
Index	aiClientMACAddress

aiClientMACAddress

Syntax	MacAddress (OCTET STRING). Hint: 1x:
Max-Access	read-only
Status	current
Description	MAC Address of the client.

aiClientWlanMACAddress

Syntax	MacAddress
Max-Access	read-only
Status	current
Description	BSSID of WLAN where client is associated.

aiClientIPAddress

Syntax	IpAddress
Max-Access	read-only
Status	current
Description	IP address of the client.

aiClientAPIPAddress

Syntax	IpAddress
Max-Access	read-only
Status	current
Description	Radio channel. First byte contains primary channel and first two bits on second byte contains indicator for secondary channel. If first two bits of second byte is 0, it is a 20MHz channel. If first two bits of second byte is 01, secondary channel is above primary channel, if first two bits of second by is 10, secondary channel is below the primary channel.

aiClientName

Syntax	
Max-Access	read-only
Status	current
Description	Name of the user using the client.

aiClientOperatingSystem

Syntax	
Max-Access	read-only
Status	current
Description	Operating system of the client.

aiClientSNR

Syntax	
Max-Access	read-only
Status	current
Description	Signal to noise ratio of the client connected to the Access Point

aiClientTxDataFrames

Syntax	
Max-Access	read-only
Status	current
Description	Total number of frames transmitted by the client.

aiClientTxDataBytes

Syntax	
Max-Access	read-only
Status	current
Description	Total number of bytes transmitted by the client.

aiClientTxRetries

Syntax	
Max-Access	read-only
Status	current
Description	Total number of retry frames transmitted by the client.

aiClientTxRate

Syntax	Integer32
Max-Access	read-only
Status	current
Description	Transmission rate of the client in mbps.

aiClientRxDataFrames

Syntax	
Max-Access	read-only
Status	current
Description	Total number of frames received by the client in mbps.

aiClientRxDataBytes

Syntax	
Max-Access	read-only
Status	current
Description	Total number of bytes received by the client in mbps.

aiClientRxRetries

Syntax	
Max-Access	read-only
Status	current
Description	Total number of retry frames received by the client.

aiClientRxRate

Syntax	

Max-Access	read-only
Status	current
Description	Receiving rate of the client in mbps.

aiClientUptime

Syntax	TimeTicks
Max-Access	read-only
Status	current
Description	Client uptime. On mobility event all counters are reset to 0 and uptime resets to 0.

This section provides information on the following standard MIBs modules and tables supported in this release of Instant.

- system MIB
- dot1qTpFdbTable
- ifTable
- ifXTable

system MIB

The system MIB contains system-specific information about the IAP. Instant supports the following system MIB objects:

- sysDescr– Provides information on the IAP model and software version of the IAP.
- sysObjectID –Identifies the network management subsystem. The sysObjectID in the standard SNMP MIB can be used to retrieve OIDs for the Aruba Instant products. You can retrieve information on all node devices in *Aruba.my* MIB by extracting the sysObjectId for each device. The sysObjectID returns OIDs for a specific model number of the device within the Instant product family.

  For example, the *iso.org.dod.internet.private.enterprise.aruba.products.apProducts.ap135* (1.3.6.1.4.1.14823.1.2.48) OID is returned for the AP-135 device. For information on the OIDs associated with the AP devices, see the apProducts tree in the *Aruba.my* MIB file.
- sysUpTime –Indicates the system up time since the IAP was initialized and actively connected to the network.
- sysName – Indicates the name of the IAP.
- sysLocation– Indicates the physical location of the IAP. To retrieve information on the AP location, the system location details for the IAP must be configured. For more information on configuring system location details, see Aruba Instant 6.3.1.1-4.0 *User Guide*.
- sysServices–Indicates the services offered by the IAP.

The following system MIB objects are not supported:

- sysContact
- sysORLastChange
- sysORTable

sysDescr

Object ID	1.3.6.1.2.1.1.1
Syntax	DisplayString
Max-Access	read-only
Status	mandatory
Description	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contains printable ASCII characters.

sysObjectID

Object ID	1.3.6.1.2.1.1.2
Syntax	Object Identifier
Max-Access	read-only
Status	mandatory
Description	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining `what kind of box' is being managed.

sysUpTime

Object ID	1.3.6.1.2.1.1.3
Syntax	TimeTicks
Max-Access	read-only
Status	mandatory
Description	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

sysName

Object ID	1.3.6.1.2.1.1.5
Syntax	DisplayString
Max-Access	read-write
Status	mandatory
Description	An administrator-assigned fully-qualified domain name for the managed node.

sysLocation

Object ID	1.3.6.1.2.1.1.6
Syntax	DisplayString
Max-Access	read-write
Status	mandatory
Description	The physical location of the AP.

sysServices

Object ID	1.3.6.1.2.1.1.7
Syntax	Integer
Max-Access	read-only
Status	mandatory
Description	A value which indicates the set of services that the AP primarily offers.

dot1qTpFdbTable

This table contains information about the associated station MAC addresses, the corresponding port from the interface table, and status. The objects of the dot1qTpFdbTable provide information about the forwarding and filtering status of the clients connected to wired ports and wireless interfaces.

The dot1qTpFdbTable contains the following objects:

- dot1qFdbId
- dot1qTpFdbAddress
- dot1qTpFdbPort
- dot1qTpFdbStatu

dot1qFdbId

Object ID	1.3.6.1.2.1.17.7.1.2.1.1.1
Syntax	UNSIGNED32
Max-Access	not-accessible
Status	current
Description	The identity of the filtering database such as VLAN ID of the AP.

dot1qTpFdbAddress

Object ID	1.3.6.1.2.1.17.7.1.2.2.1.1
Syntax	MacAddress
Max-Access	not-accessible
Status	current
Description	MAC address for which the AP has forwarding or filtering information.

dot1qTpFdbPort

Object ID	1.3.6.1.2.1.17.7.1.2.2.1.2

Syntax	Integer32 (0..65535)
Max-Access	read-only
Status	current
Description	Port number on which a frame having a source address equal to the value of the corresponding instance of dot1qTpFdbAddress. The index value of ifTable is set as the port number field in this table. If the self MAC address is used, the index is 0.

dot1qTpFdbStatu

Object ID	1.3.6.1.2.1.17.7.1.2.2.1.3
Syntax	INTEGER { other(1), invalid(2), learned(3), self(4), mgmt(5) }
Max-Access	read-only
Status	current
Description	The status of the bridge entry is set as learned to indicate that the value of the corresponding instance of dot1qTpFdbPort was learned and is being used. If self MAC address is used, the status is set as self to indicate that the value of the corresponding instance of dot1qTpFdbAddress represents one of the device's addresses. The corresponding instance of dot1qTpFdbPort indicates which of the device's ports has this address.

ifTable

This table contains information about wired ports and wireless interfaces. The objects in this MIB provide information about the interfaces configured on an IAP. This table contains the following objects:

- ifIndex
- ifDescr
- ifType
- ifMtu
- ifSpeed
- ifPhysAddress
- ifAdminStatus
- ifOperStatus
- ifInOctets
- ifInUcastPkts
- ifInNUcastPkts
- ifInDiscards
- ifInErrors
- ifOutOctets
- ifOutUcastPkts
- ifInDiscards
- ifInErrors

The following ifTable objects are not supported:

- ifOutQLen
- ifSpecific
- ifInUnknownProtos
- ifLastChange

ifIndex

Object ID	1.3.6.1.2.1.2.2.1.1
Syntax	Integer32
Max-Access	read-only
Status	current
Description	Value assigned to an interface. • Ethernet interface value range: 1–49 • Radio 0 interface value range: 50–69. • Radio 1 interface range: 70–89. • GRE interface range: 90–09 • PPP interface range: 110–129 • VPN interface range: 130–150 • Other interfaces: From 500 onwards

ifDescr

Object ID	1.3.6.1.2.1.2.2.1.2
Syntax	DisplayString (size (0..255))
Max-Access	read-only
Status	current
Description	Description of the interface, for example eth for Ethernet, radio0_ssid_id2,aruba102 for Radio0 interface, and radioX_ssid_idY for Radio1 interface.

ifType

Object ID	1.3.6.1.2.1.2.2.1.3
Syntax	IANAifType
Max-Access	read-only
Status	current
Description	Type of the interface. For example, Gigabit Ethernet interface or Fast Ethernet.

ifMtu

Object ID	1.3.6.1.2.1.2.2.1.4
Syntax	Integer32

Max-Access	read-only
Status	current
Description	The size of the largest packet which can be sent or received on interface.

ifSpeed

Object ID	1.3.6.1.2.1.2.2.1.5
Syntax	Gauge32
Max-Access	read-only
Status	current
Description	The current bandwidth of the interface in bits per second.

ifPhysAddress

Object ID	1.3.6.1.2.1.2.2.1.6
Syntax	PhysAddress
Max-Access	read-only
Status	current
Description	Indicates the MAC address of the client.

ifAdminStatus

Object ID	1.3.6.1.2.1.2.2.1.7
Syntax	INTEGER
Max-Access	read-write
Status	current
Description	Administrative state of the interface.

ifOperStatus

Object ID	1.3.6.1.2.1.2.2.1.8
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	Operational status of the interface.

ifInOctets

Object ID	1.3.6.1.2.1.2.2.1.10
Syntax	Counter32
Max-Access	read-only
Status	current
Description	Number of octets received on the interface.

ifInUcastPkts

Object ID	1.3.6.1.2.1.2.2.1.11
Syntax	Counter32
Max-Access	read-only
Status	current
Description	The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.

ifInNUcastPkts

Object ID	1.3.6.1.2.1.2.2.1.12
Syntax	Counter32
Max-Access	read-only
Status	current
Description	The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a multicast or broadcast address at this sub-layer.

ifInDiscards

Object ID	1.3.6.1.2.1.2.2.1.13
Syntax	Counter32
Max-Access	read-only
Status	current
Description	The number of inbound packets discarded.

ifInErrors

Object ID	1.3.6.1.2.1.2.2.1.14

Syntax	Counter32
Max-Access	read-only
Status	current
Description	The number of packets transmission units with errors.

ifOutOctets

Object ID	1.3.6.1.2.1.2.2.1.16
Syntax	Counter32
Max-Access	read-only
Status	current
Description	The total number of octets transmitted out of the interface.

ifOutUcastPkts

Object ID	1.3.6.1.2.1.2.2.1.17
Syntax	Counter32
Max-Access	read-only
Status	current
Description	The total number of packets that the higher-level protocols request for transmission, and the packets which are not addressed to a multicast or broadcast address at this sub-layer, including those that are discarded or not sent.

ifOutDiscards

Object ID	1.3.6.1.2.1.2.2.1.19
Syntax	Counter32
Max-Access	read-only
Status	current
Description	The number of outbound packets discarded even though no errors that prevented the transmission were detected.

ifOutErrors

Object ID	1.3.6.1.2.1.2.2.1.20
Syntax	Counter32

Max-Access	read-only
Status	current
Description	The number of outbound packets that could not be transmitted because of errors.

ifXTable

The ifXTable table contains the following additional objects for the interface table.

- ifName
- ifInMulticastPkts
- ifInBroadcastPkts
- ifOutMulticastPkts
- ifOutBroadcastPkts
- ifHCInOctets
- ifHCInUcastPkts
- ifHCInMulticastPkts
- ifHCInBroadcastPkts
- ifHCOutOctets
- ifHCOutUcastPkts
- ifHCOutMulticastPkts
- ifHCOutBroadcastPkts
- ifLinkUpDownTrapEnable
- ifPromiscuousMode
- ifConnectorPresent

The following ifXTable objects are not supported:

- ifHighSpeed
- ifAlias
- ifCounterDiscontinuityTime

ifName

Object ID	1.3.6.1.2.1.31.1.1.1.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	Name of the interface

ifInMulticastPkts

Object ID	1.3.6.1.2.1.31.1.1.1.2
Syntax	Counter32

Max-Access	read-only
Status	current
Description	The number of packets, delivered by this sub-layer to a higher layer, which were addressed to a multicast or broadcast address at this sub-layer.

ifInBroadcastPkts

Object ID	1.3.6.1.2.1.31.1.1.1.3
Syntax	Counter32
Max-Access	read-only
Status	current
Description	The number of packets, delivered by this sub-layer to a higher layer, which were addressed to a multicast or broadcast address at this sub-layer

ifOutMulticastPkts

Object ID	1.3.6.1.2.1.31.1.1.1.4
Syntax	Counter32
Max-Access	read-only
Status	current
Description	The total number of packets that the higher-level protocols request for transmission, and which were addressed to a multicast or broadcast address at this sub-layer.

ifOutBroadcastPkts

Object ID	1.3.6.1.2.1.31.1.1.1.5
Syntax	Counter32
Max-Access	read-only
Status	current
Description	The total number of packets that higher-level protocols requested for transmission, and the packets which were addressed to a multicast or broadcast address at this sub-layer.

ifHCInOctets

Object ID	1.3.6.1.2.1.31.1.1.1.6

Syntax	Counter64
Max-Access	read-only
Status	current
Description	The total number of octets received on the interface, including framing characters. This object is a 64-bit version of ifInOctets.

ifHCInUcastPkts

Object ID	1.3.6.1.2.1.31.1.1.1.7
Syntax	Counter64
Max-Access	read-only
Status	current
Description	The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.

ifHCInMulticastPkts

Object ID	1.3.6.1.2.1.31.1.1.1.8
Syntax	Counter64
Max-Access	read-only
Status	current
Description	The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a multicast or broadcast address at this sub-layer.

ifHCInBroadcastPkts

Object ID	1.3.6.1.2.1.31.1.1.1.9
Syntax	Counter64
Max-Access	read-only
Status	current
Description	The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a multicast or broadcast address at this sub-layer.

ifHCOutOctets

Object ID	1.3.6.1.2.1.31.1.1.1.10
Syntax	Counter64
Max-Access	read-only
Status	current
Description	The total number of octets transmitted out of the interface, including framing characters.

ifHCOutUcastPkts

Object ID	1.3.6.1.2.1.31.1.1.1.11
Syntax	Counter64
Max-Access	read-only
Status	current
Description	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.

ifHCOutMulticastPkts

Object ID	1.3.6.1.2.1.31.1.1.1.12
Syntax	Counter64
Max-Access	read-only
Status	current
Description	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.

ifHCOutBroadcastPkts

Object ID	1.3.6.1.2.1.31.1.1.1.13
Syntax	Counter64
Max-Access	read-only
Status	current
Description	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.

ifLinkUpDownTrapEnable

Object ID	1.3.6.1.2.1.31.1.1.1.14
Syntax	Integer
Max-Access	read-write
Status	current
Description	Indicates whether linkUp or linkDown traps must be generated for this interface.

ifPromiscuousMode

Object ID	1.3.6.1.2.1.31.1.1.1.16
Syntax	Integer
Max-Access	TruthValue
Status	current
Description	This object has true (1) and false(2) values.

ifConnectorPresent

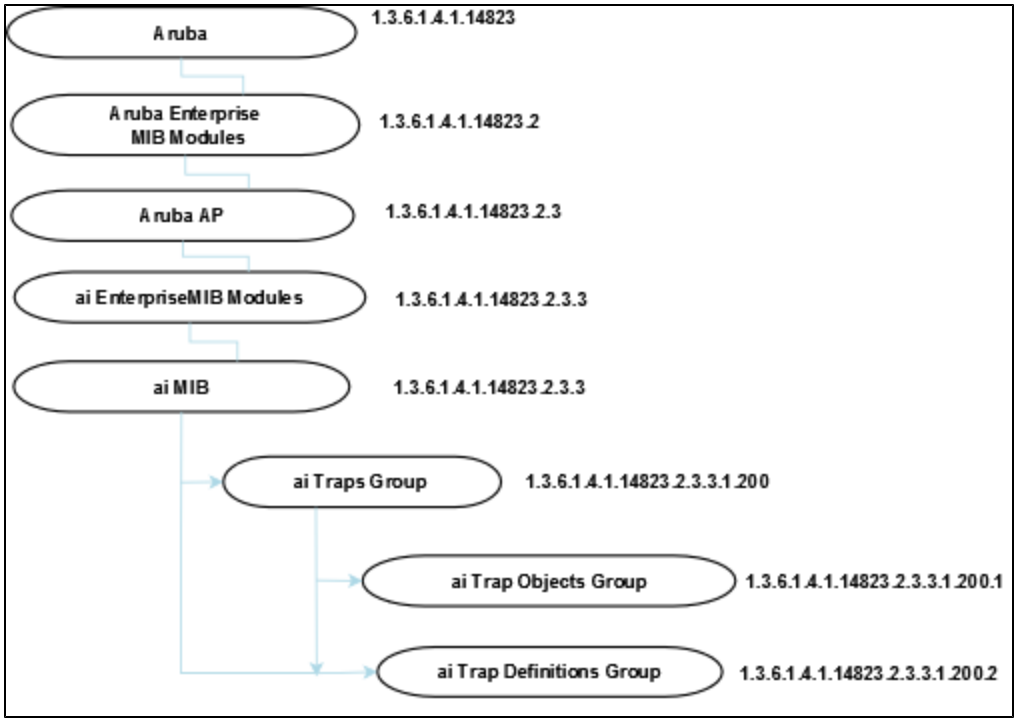
Object ID	1.3.6.1.2.1.31.1.1.1.17
Syntax	Integer
Max-Access	TruthValue
Status	current
Description	This object has True(1) value if there is any physical connector, else false (0) value.

This module defines the traps that can be generated by the IAP. 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.

Figure 5 shows the architecture of the Traps MIB relative to 1.3.6.1.4.1.14823 (iso.org.dod.internet.private.enterprise.aruba). The Traps are listed in the file *aruba-trap.my* MIB file. For information about downloading Instant MIB files, see Downloading MIB Files on page 22.

Trap Hierarchy

Figure 5 *Trap Hierarchy*



The following table lists the supported trap objects in this group:

Table 9: *aiTraps Objects Group OIDs*

Object	Object ID	
wlsxTrapAPMacAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.1	wlsxTrapObjectsGroup 1
wlsxTrapAPIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.2	wlsxTrapObjectsGroup 2
wlsxTrapAPBSSID	1.3.6.1.4.1.14823.2.3.3.1.200.1.3	wlsxTrapObjectsGroup 3
wlsxTrapEssid	1.3.6.1.4.1.14823.2.3.3.1.200.1.4	wlsxTrapObjectsGroup 4

Object	Object ID	
wlsxTrapTargetAPBSSID	1.3.6.1.4.1.14823.2.3.3.1.200.1.5	wlsxTrapObjectsGroup 5
wlsxTrapTargetAPSSID	1.3.6.1.4.1.14823.2.3.3.1.200.1.6	wlsxTrapObjectsGroup 6
wlsxTrapTargetAPChannel	1.3.6.1.4.1.14823.2.3.3.1.200.1.7	wlsxTrapObjectsGroup 7
wlsxTrapNodeMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.8	wlsxTrapObjectsGroup 8
wlsxTrapSourceMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.9	wlsxTrapObjectsGroup 9
wlsxReceiverMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.10	wlsxTrapObjectsGroup 10
wlsxTrapTransmitterMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.11	wlsxTrapObjectsGroup 11
wlsxTrapReceiverMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.12	wlsxTrapObjectsGroup 12
wlsxTrapSnr	1.3.6.1.4.1.14823.2.3.3.1.200.1.13	wlsxTrapObjectsGroup 13
wlsxTrapSignatureName	1.3.6.1.4.1.14823.2.3.3.1.200.1.14	wlsxTrapObjectsGroup 14
wlsxTrapFrameType	1.3.6.1.4.1.14823.2.3.3.1.200.1.15	wlsxTrapObjectsGroup 15
wlsxTrapAddressType	1.3.6.1.4.1.14823.2.3.3.1.200.1.16	wlsxTrapObjectsGroup 16
wlsxTrapAPLocation	1.3.6.1.4.1.14823.2.3.3.1.200.1.17	wlsxTrapObjectsGroup 17
wlsxTrapAPChannel	1.3.6.1.4.1.14823.2.3.3.1.200.1.18	wlsxTrapObjectsGroup 18
wlsxTrapAPTxPower	1.3.6.1.4.1.14823.2.3.3.1.200.1.19	wlsxTrapObjectsGroup 19
wlsxTrapMatchedMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.20	wlsxTrapObjectsGroup 20
wlsxTrapMatchedIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.21	wlsxTrapObjectsGroup 21
wlsxTrapRogueInfoURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.22	wlsxTrapObjectsGroup 22
wlsxTrapVLANId	1.3.6.1.4.1.14823.2.3.3.1.200.1.23	wlsxTrapObjectsGroup 23

Object	Object ID	
wlsxTrapAdminStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.24	wlsxTrapObjectsGroup 24
wlsxTrapOperStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.25	wlsxTrapObjectsGroup 25
wlsxTrapAuthServerName	1.3.6.1.4.1.14823.2.3.3.1.200.1.26	wlsxTrapObjectsGroup 26
wlsxTrapAuthServerTimeout	1.3.6.1.4.1.14823.2.3.3.1.200.1.27	wlsxTrapObjectsGroup 27
wlsxTrapCardSlot	1.3.6.1.4.1.14823.2.3.3.1.200.1.28	wlsxTrapObjectsGroup 28
wlsxTrapTemperatureValue	1.3.6.1.4.1.14823.2.3.3.1.200.1.29	wlsxTrapObjectsGroup 29
wlsxTrapProcessName	1.3.6.1.4.1.14823.2.3.3.1.200.1.30	wlsxTrapObjectsGroup 30
wlsxTrapFanNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.31	wlsxTrapObjectsGroup 31
wlsxTrapVoltageType	1.3.6.1.4.1.14823.2.3.3.1.200.1.32	wlsxTrapObjectsGroup 32
wlsxTrapVoltageValue	1.3.6.1.4.1.14823.2.3.3.1.200.1.33	wlsxTrapObjectsGroup 33
wlsxTrapStationBlackListReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.34	wlsxTrapObjectsGroup 34
wlsxTrapSpoofedIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.35	wlsxTrapObjectsGroup 35
wlsxTrapSpoofedOldPhyAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.36	wlsxTrapObjectsGroup 36
wlsxTrapSpoofedNewPhyAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.37	wlsxTrapObjectsGroup 37
wlsxTrapDBName	1.3.6.1.4.1.14823.2.3.3.1.200.1.38	wlsxTrapObjectsGroup 38
wlsxTrapDBUserName	1.3.6.1.4.1.14823.2.3.3.1.200.1.39	wlsxTrapObjectsGroup 39
wlsxTrapDBIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.40	wlsxTrapObjectsGroup 40
wlsxTrapDBType	1.3.6.1.4.1.14823.2.3.3.1.200.1.41	wlsxTrapObjectsGroup 41
wlsxTrapVrrpID	1.3.6.1.4.1.14823.2.3.3.1.200.1.42	wlsxTrapObjectsGroup 42

Object	Object ID	
wlsxTrapVrrpMasterIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.43	wlsxTrapObjectsGroup 43
wlsxTrapVrrpOperState	1.3.6.1.4.1.14823.2.3.3.1.200.1.44	wlsxTrapObjectsGroup 44
wlsxTrapESIServerGrpName	1.3.6.1.4.1.14823.2.3.3.1.200.1.45	wlsxTrapObjectsGroup 45
wlsxTrapESIServerName	1.3.6.1.4.1.14823.2.3.3.1.200.1.46	wlsxTrapObjectsGroup 46
wlsxTrapESIServerIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.47	wlsxTrapObjectsGroup 47
wlsxTrapLicenseDaysRemaining	1.3.6.1.4.1.14823.2.3.3.1.200.1.48	wlsxTrapObjectsGroup 48
wlsxTrapSwitchIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.49	wlsxTrapObjectsGroup 49
wlsxTrapSwitchRole	1.3.6.1.4.1.14823.2.3.3.1.200.1.50	wlsxTrapObjectsGroup 50
wlsxTrapUserIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.51	wlsxTrapObjectsGroup 51
wlsxTrapUserPhyAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.52	wlsxTrapObjectsGroup 52
wlsxTrapUserName	1.3.6.1.4.1.14823.2.3.3.1.200.1.53	wlsxTrapObjectsGroup 53
wlsxTrapUserRole	1.3.6.1.4.1.14823.2.3.3.1.200.1.54	wlsxTrapObjectsGroup 54
wlsxTrapUserAuthenticationMethod	1.3.6.1.4.1.14823.2.3.3.1.200.1.55	wlsxTrapObjectsGroup 55
wlsxTrapAPRadioNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.56	wlsxTrapObjectsGroup 56
wlsxTrapRogueInfoURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.57	wlsxTrapObjectsGroup 57
wlsxTrapInterferingAPInfoURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.58	wlsxTrapObjectsGroup 58
wlsxTrapPortNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.59	wlsxTrapObjectsGroup 59
wlsxTrapTime	1.3.6.1.4.1.14823.2.3.3.1.200.1.60	wlsxTrapObjectsGroup 60
wlsxTrapHostIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.61	wlsxTrapObjectsGroup 61

Object	Object ID	
wlsxTrapHostPort	1.3.6.1.4.1.14823.2.3.3.1.200.1.63	wlsxTrapObjectsGroup 62
wlsxTrapConfigurationId	1.3.6.1.4.1.14823.2.3.3.1.200.1.63	wlsxTrapObjectsGroup 63
wlsxTrapCTSURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.64	wlsxTrapObjectsGroup 64
wlsxTrapCTSTransferType	1.3.6.1.4.1.14823.2.3.3.1.200.1.65	wlsxTrapObjectsGroup 65
wlsxTrapConfigurationState	1.3.6.1.4.1.14823.2.3.3.1.200.1.66	wlsxTrapObjectsGroup 66
wlsxTrapUpdateFailureReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.67	wlsxTrapObjectsGroup 67
wlsxTrapUpdateFailedObj	1.3.6.1.4.1.14823.2.3.3.1.200.1.68	wlsxTrapObjectsGroup 68
wlsxTrapTableEntryChangeType	1.3.6.1.4.1.14823.2.3.3.1.200.1.69	wlsxTrapObjectsGroup 69
wlsxTrapGlobalConfigObj	1.3.6.1.4.1.14823.2.3.3.1.200.1.70	wlsxTrapObjectsGroup 70
wlsxTrapTableGenNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.71	wlsxTrapObjectsGroup 71
wlsxTrapLicenseId	1.3.6.1.4.1.14823.2.3.3.1.200.1.72	wlsxTrapObjectsGroup 72
wlsxTrapConfidenceLevel	1.3.6.1.4.1.14823.2.3.3.1.200.1.73	wlsxTrapObjectsGroup 73
wlsxTrapMissingLicenses	1.3.6.1.4.1.14823.2.3.3.1.200.1.74	wlsxTrapObjectsGroup 74
wlsxVoiceCurrentNumCdr	1.3.6.1.4.1.14823.2.3.3.1.200.1.75	wlsxTrapObjectsGroup 75
wlsxTrapTunnelId	1.3.6.1.4.1.14823.2.3.3.1.200.1.76	wlsxTrapObjectsGroup 76
wlsxTrapTunnelStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.77	wlsxTrapObjectsGroup 77
wlsxTrapTunnelUpReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.78	wlsxTrapObjectsGroup 78
wlsxTrapTunnelDownReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.79	wlsxTrapObjectsGroup 79
wlsxTrapApSerialNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.80	wlsxTrapObjectsGroup 80

Object	Object ID	
wlsxTraptimeStr	1.3.6.1.4.1.14823.2.3.3.1.200.1.81	wlsxTrapObjectsGroup 81
wlsxTrapMasterIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.82	wlsxTrapObjectsGroup 82
wlsxTrapLocalIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.83	wlsxTrapObjectsGroup 83
wlsxTrapMasterName	1.3.6.1.4.1.14823.2.3.3.1.200.1.84	wlsxTrapObjectsGroup 84
wlsxTrapLocalName	1.3.6.1.4.1.14823.2.3.3.1.200.1.85	wlsxTrapObjectsGroup 85
wlsxTrapPrimaryControllerIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.86	wlsxTrapObjectsGroup 86
wlsxTrapBackupControllerIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.87	wlsxTrapObjectsGroup 87
wlsxTrapSpoofedFrameType	1.3.6.1.4.1.14823.2.3.3.1.200.1.88	wlsxTrapObjectsGroup 88
wlsxTrapAssociationType	1.3.6.1.4.1.14823.2.3.3.1.200.1.89	wlsxTrapObjectsGroup 89
wlsxTrapDeviceIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.90	wlsxTrapObjectsGroup 90
wlsxTrapDeviceMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.91	wlsxTrapObjectsGroup 91
wlsxTrapVcIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.92	wlsxTrapObjectsGroup 92
wlsxTrapVcMacAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.93	wlsxTrapObjectsGroup 93
wlsxTrapAPName	1.3.6.1.4.1.14823.2.3.3.1.200.1.94	wlsxTrapObjectsGroup 94
wlsxTrapApMode	1.3.6.1.4.1.14823.2.3.3.1.200.1.95	wlsxTrapObjectsGroup 95
wlsxTrapAPPrevChannel	1.3.6.1.4.1.14823.2.3.3.1.200.1.96	wlsxTrapObjectsGroup 96
wlsxTrapAPPrevChannelSec	1.3.6.1.4.1.14823.2.3.3.1.200.1.97	wlsxTrapObjectsGroup 97
wlsxTrapAPPrevTxPower	1.3.6.1.4.1.14823.2.3.3.1.200.1.98	wlsxTrapObjectsGroup 98
wlsxTrapAPCurMode	1.3.6.1.4.1.14823.2.3.3.1.200.1.99	wlsxTrapObjectsGroup 99

Object	Object ID	
wlsxTrapAPPrevMode	1.3.6.1.4.1.14823.2.3.3.1.200.1.100	wlsxTrapObjectsGroup 100
wlsxTrapAPARMChangeReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.101	wlsxTrapObjectsGroup 101
wlsxTrapAPChannelSec	1.3.6.1.4.1.14823.2.3.3.1.200.1.102	wlsxTrapObjectsGroup 102
wlsxTrapUserAttributeChangeType	1.3.6.1.4.1.14823.2.3.3.1.200.1.103	wlsxTrapObjectsGroup 103
wlsxTrapAPControllerIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.104	wlsxTrapObjectsGroup 104
wlsxTrapApMasterStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.105	wlsxTrapObjectsGroup 105
wlsxTrapCaName	1.3.6.1.4.1.14823.2.3.3.1.200.1.106	wlsxTrapObjectsGroup 106
wlsxTrapCrlName	1.3.6.1.4.1.14823.2.3.3.1.200.1.107	wlsxTrapObjectsGroup 107
wlsxTrapCount	1.3.6.1.4.1.14823.2.3.3.1.200.1.108	wlsxTrapObjectsGroup 108
wlsxTrapAPPreviousUplinkType	1.3.6.1.4.1.14823.2.3.3.1.200.1.130	wlsxTrapObjectsGroup 130
wlsxTrapAPPreviousUplinkActiveTime	1.3.6.1.4.1.14823.2.3.3.1.200.1.131	wlsxTrapObjectsGroup 131
wlsxTrapAPActiveUplinkType	1.3.6.1.4.1.14823.2.3.3.1.200.1.132	wlsxTrapObjectsGroup 132
wlsxTrapAPUplinkChangeReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.133	wlsxTrapObjectsGroup 133
{Default ¹ Font}{PMS 646} wlsxTrapAPManagedModeConfigFailure	1.3.6.1.4.1.14823.2.3.3.1.200.1.134	wlsxTrapObjectsGroup 134

wlsxTrapAPMacAddress

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the wired MAC address of an access point, for which the trap is being raised.

wlsxTrapAPIpAddress

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the IP address of an access point for which for which the trap is being raised.

wlsxTrapAPBSSID

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the BSSID of the access point for which we are raising the trap.

wlsxTrapEssid

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the SSID of the access point, for which the trap is being raised.

wlsxTrapTargetAPBSSID

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the BSSID of the access point, for which we are raising the trap. If an Air Monitor is sending the trap then this will indicate AP. If an access point is sending the trap, then it will point to itself.

wlsxTrapTargetAPSSID

Syntax	DisplayString(Size(0..64))

Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the SSID of the access point, for which the trap is being raised. If an Air Monitor is sending the trap then this will indicate AP. If an access point is sending the trap, then it will point to itself.

wlsxTrapTargetAPChannel

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the channel of the access point, for which the trap is being raised. If an wlsxr monitor is sending the trap then this will indicate AP. If an access point is sending the trap, then it will point to itself.

wlsxTrapNodeMac

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the MAC address of a node.

wlsxTrapSourceMac

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the MAC address of the source.

wlsxReceiverMac

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the MAC address of the receiver.

wlsxTrapTransmitterMac

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the MAC address of the transmitter.

wlsxTrapReceiverMac

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the MAC address of the receiver.

wlsxTrapSnr

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the signal-to-noise ratio.

wlsxTrapSignatureName

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the signature name.

wlsxTrapFrameType

Syntax	ArubaFrameType
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the frame type.

wlsxTrapAddressType

Syntax	ArubaAddressType

Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the address type.

wlsxTrapAPLocation

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the location of the AP.

wlsxTrapAPChannel

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the current channel.

wlsxTrapAPTxPower

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the AP transmit power.

wlsxTrapMatchedMac

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the MAC address.

wlsxTrapMatchedIp

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the IP address.

wlsxTrapRogueIfoURL

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used to point to the WEBUI Rogue AP information URL.

wlsxTrapVLANId

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the VLAN ID.

wlsxTrapAdminStatus

Syntax	ArubaEnableValue (INTEGER)
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the admin status of VLAN.

wlsxTrapOperStatus

Syntax	ArubaOperStateValue
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the admin status of VLAN.

wlsxTrapAuthServerName

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the authentication server used for authentication.

wlsxTrapAuthServerTimeout

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the Authentication Server Timeout.

wlsxTrapCardSlot

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the slot in which this card is present.

wlsxTrapTemperatureValue

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the temperature value.

wlsxTrapProcessName

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the process name.

wlsxTrapFanNumber

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the fan number.

wlsxTrapVoltageType

Syntax	DisplayString(Size(0..64))

Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the type of voltage.

wlsxTrapVoltageValue

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the voltage value in float.

wlsxTrapStationBlackListReason

Syntax	ArubaBlackListReason
Max-Access	accessible-for-notify
Status	current
Description	The reason for which a station is black listed.

wlsxTrapSpoofedIpAddress

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in a trap to identify a spoofed IP address.

wlsxTrapSpoofedOldPhyAddress

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in a trap to identify an old MAC address.

wlsxTrapSpoofedNewPhyAddress

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object is used in a trap to identify a new MAC address.

wlsxTrapDBName

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in a trap to identify the name of the database.

wlsxTrapDBUserName

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in a trap to identify the name of the database user.

wlsxTrapDBIpAddress

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in a trap to identify the IP address of the database.

wlsxTrapDBType

Syntax	ArubaDBType
Max-Access	accessible-for-notify
Status	current
Description	This object is used in a trap to identify the port of the user.

wlsxTrapVrrpID

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object contains the virtual router identifier.

wlsxTrapVrrpMasterIp

Syntax	IpAddress

Max-Access	accessible-for-notify
Status	current
Description	This object contains the master IP address.

wlsxTrapVrrpOperState

Syntax	ArubaVrrpState
Max-Access	accessible-for-notify
Status	current
Description	This object represents the VRRP operational state.

wlsxTrapESIServerGrpName

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the External Services Interface (ESI) server group name.

wlsxTrapESIServerName

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the External Services Interface (ESI) server name.

wlsxTrapESIServerIpAddress

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the External Services Interface (ESI) server IP address.

wlsxTrapLicenseDaysRemaining

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object represents the number of days remaining prior to a license expiry.

wlsxTrapSwitchIp

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the controller IP address.

wlsxTrapSwitchRole

Syntax	ArubaSwitchRole
Max-Access	accessible-for-notify
Status	current
Description	This object represents the role of the controller.

wlsxTrapUserIpAddress

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the IP address of the user.

wlsxTrapUserPhyAddress

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the MAC address of the user.

wlsxTrapUserName

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the user name.

wlsxTrapUserRole

Syntax	DisplayString(Size(0..64))

Max-Access	accessible-for-notify
Status	current
Description	This object represents the Authentication method of the user.

wlsxTrapUserAuthenticationMethod

Syntax	ArubaAuthenticationMethods
Max-Access	accessible-for-notify
Status	current
Description	This object represents the Authentication method of the user.

wlsxTrapAPRadioNumber

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object represents the radio number.

wlsxTrapRogueInfoURL

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used to point to the WEBGUI Rogue AP information URL.

wlsxTrapInterferingAPInfoURL

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used to point to the WEBGUI Rogue interfering access point information URL.

wlsxTrapPortNumber

Syntax	Integer32
Max-Access	accessible-for-notify

Status	current
Description	This object is used in the traps to indicate the port number.

wlsxTrapTime

Syntax	DateAndTime
Max-Access	accessible-for-notify
Status	current
Description	This object is used in all the enterprise traps to indicate the time when the trap is generated on the controller.

wlsxTrapHostIp

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the trap host.

wlsxTrapHostPort

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object represents the trap host port.

wlsxTrapConfigurationId

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	

wlsxTrapCTSURL

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the URL from which the transfer should happen.

wlsxTrapCTSTransferType

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the transfer type, upload or download.

wlsxTrapConfigurationState

Syntax	ArubaConfigurationState (INTEGER)
Max-Access	accessible-for-notify
Status	current
Description	This object represents the state of the configuration transfer.

wlsxTrapUpdateFailureReason

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the reason for the update failure.

wlsxTrapUpdateFailedObj

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This variable represents the AMAPI object which is the reason for the update failure.

wlsxTrapTableEntryChangeType

Syntax	ArubaConfigurationChangeType (INTEGER)
Max-Access	accessible-for-notify
Status	current
Description	This object represents the type of the configuration change.

wlsxTrapGlobalConfigObj

Syntax	DisplayString(Size(0..64))

Max-Access	accessible-for-notify
Status	current
Description	This variable represents the AMAPI object corresponding to the global configuration change.

wlsxTrapTableGenNumber

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object represents the generation number of a table. Used in the MMS to keep track of the table content changes.

wlsxTrapLicenseId

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the license ID.

wlsxTrapConfidenceLevel

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the confidence level as a percentage.

wlsxTrapMissingLicenses

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This variable indicates any licenses that are not present during a configuration update.

wlsxVoiceCurrentNumCdr

Syntax	Integer32

Max-Access	accessible-for-notify
Status	current
Description	This object represents the number of CDRs in buffer.

wlsxTrapTunnelId

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object represents the tunnel ID.

wlsxTrapTunnelStatus

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object represents the tunnel status.

wlsxTrapTunnelUpReason

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the tunnel up reason.

wlsxTrapTunnelDownReason

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the tunnel down reason.

wlsxTrapApSerialNumber

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the AP serial number.

wlsxTraptimeStr

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the Time in String format.

wlsxTrapMasterIp

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the master IP address.

wlsxTrapLocalIp

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the local IP address.

wlsxTrapMasterName

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the master controller name.

wlsxTrapLocalName

Syntax	DisplayString(Size(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object represents the local controller name.

wlsxTrapPrimaryControllerIp

Syntax	IpAddress

Max-Access	accessible-for-notify
Status	current
Description	This object represents the IP address of the AP's primary controller.

wlsxTrapBackupControllerIp

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the IP address of the AP's backup controller.

wlsxTrapSpoofedFrameType

Syntax	DisplayString (SIZE(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the Spoofed Frame Type

wlsxTrapAssociationType

Syntax	DisplayString (SIZE(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the type of association.

wlsxTrapDeviceIpAddress

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the IP address of a device seen by an AP.

wlsxTrapDeviceMac

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the MAC address of a device seen by an AP.

wlsxTrapVcIpAddress

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the IP Address of a Voice client.

wlsxTrapVcMacAddress

Syntax	MacAddress
Max-Access	accessible-for-notify
Status	current
Description	This object represents the MAC address of a Voice client.

wlsxTrapAPName

Syntax	DisplayString (SIZE(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the Name of the AP.

wlsxTrapApMode

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	

wlsxTrapAPPrevChannel

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the Previous Channel.

wlsxTrapAPPrevChannelSec

Syntax	ArubaHTExtChannel (INTEGER)
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the Previous Secondary Channel.

wlsxTrapAPPrevTxPower

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate previous AP Transmit Power.

wlsxTrapAPCurMode

Syntax	ArubaAccessPointMode (INTEGER)
Max-Access	accessible-for-notify
Status	current
Description	This Object represents the APs Current Mode.

wlsxTrapAPPrevMode

Syntax	ArubaAccessPointMode (INTEGER)
Max-Access	accessible-for-notify
Status	current
Description	This Object represents the APs Previous Mode.

wlsxTrapAPARMChangeReason

Syntax	ArubaARMChangeReason (INTEGER)
Max-Access	accessible-for-notify
Status	current
Description	This Object represents the APs Previous Mode.

wlsxTrapAPChannelSec

Syntax	ArubaHTExtChannel (INTEGER)

Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the Current Secondary Channel.

wlsxTrapUserAttributeChangeType

Syntax	ArubaConfigurationChangeType (INTEGER)
Max-Access	accessible-for-notify
Status	current
Description	This object represents type of the configuration change.

wlsxTrapAPControllerIp

Syntax	IpAddress
Max-Access	accessible-for-notify
Status	current
Description	

wlsxTrapApMasterStatus

Syntax	ArubaAPMasterStatus (INTEGER)
Max-Access	accessible-for-notify
Status	current
Description	Status of the AP as seen by the master when the status changes.

wlsxTrapCaName

Syntax	DisplayString (SIZE(0..64))
Max-Access	accessible-for-notify
Status	current
Description	

wlsxTrapCrlName

Syntax	DisplayString (SIZE(0..64))
Max-Access	accessible-for-notify
Status	current
Description	This object is used in the traps to indicate the name of the CRL.

wlsxTrapCount

Syntax	Integer32
Max-Access	accessible-for-notify
Status	current
Description	This object represents the number of occurrence of this trap.

wlsxTrapAPPreviousUplinkType

Syntax	ArubaAPUplinkType
Max-Access	accessible-for-notify
Status	current
Description	This object represents the previous uplink type of an AP.

wlsxTrapAPPreviousUplinkActiveTime

Syntax	TimeTicks
Max-Access	accessible-for-notify
Status	current
Description	This object represents the active time of the previous uplink of an AP.

wlsxTrapAPActiveUplinkType

Syntax	ArubaAPUplinkType
Max-Access	accessible-for-notify
Status	current
Description	This object represents the active uplink type of an AP.

wlsxTrapAPUplinkChangeReason

Syntax	ArubaAPUplinkChangeReason
Max-Access	accessible-for-notify
Status	current
Description	This object represents the uplink change reason.

wlsxTrapAPManagedModeConfigFailure

Syntax	DisplayString (SIZE(0..64)

Max-Access	accessible-for-notify
Status	current
Description	This object indicates that the configuration application has failed on the AP.

ai Traps Definitions Group

Table 10: *ai Traps Definitions Group OIDs*

Object	Object ID	
wlsxNUserEntryCreated	1.3.6.1.4.1.14823.2.3.3.1.200.2.1014	wlsxTrapDefinitionsGroup 1014
wlsxNUserEntryDeleted	1.3.6.1.4.1.14823.2.3.3.1.200.2.1015	wlsxTrapDefinitionsGroup 1015
wlsxNUserEntryAuthenticated	1.3.6.1.4.1.14823.2.3.3.1.200.2.1016	wlsxTrapDefinitionsGroup 1016
wlsxNUserEntryDeAuthenticated	1.3.6.1.4.1.14823.2.3.3.1.200.2.1017	wlsxTrapDefinitionsGroup 1017
wlsxNUserAuthenticationFailed	1.3.6.1.4.1.14823.2.3.3.1.200.2.1018	wlsxTrapDefinitionsGroup 1018
wlsxNAuthServerReqTimedOut	1.3.6.1.4.1.14823.2.3.3.1.200.2.1019	wlsxTrapDefinitionsGroup 1019
wlsxNAuthServerTimedOut	1.3.6.1.4.1.14823.2.3.3.1.200.2.1020	wlsxTrapDefinitionsGroup 1020
wlsxNAuthServerIsUp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1021	wlsxTrapDefinitionsGroup 1021
wlsxNAccessPointIsUp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1040	wlsxTrapDefinitionsGroup 1040
wlsxNAccessPointIsDown	1.3.6.1.4.1.14823.2.3.3.1.200.2.1041	wlsxTrapDefinitionsGroup 1041
wlsxNChannelChanged	1.3.6.1.4.1.14823.2.3.3.1.200.2.1043	wlsxTrapDefinitionsGroup 1043
wlsxNStationAddedToBlackList	1.3.6.1.4.1.14823.2.3.3.1.200.2.1044	wlsxTrapDefinitionsGroup 1044
wlsxNStationRemovedFromBlackList	1.3.6.1.4.1.14823.2.3.3.1.200.2.1045	wlsxTrapDefinitionsGroup 1045
wlsxNRadioAttributesChanged	1.3.6.1.4.1.14823.2.3.3.1.200.2.1049	wlsxTrapDefinitionsGroup 1049
wlsxUnsecureAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1053	wlsxTrapDefinitionsGroup 1053

Object	Object ID	
wlsxUnsecureAPResolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1054	wlsxTrapDefinitionsGroup 1054
wlsxStaImpersonation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1055	wlsxTrapDefinitionsGroup 1055
wlsxReservedChannelViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1056	wlsxTrapDefinitionsGroup 1056
wlsxValidSSIDViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1057	wlsxTrapDefinitionsGroup 1057
wlsxChannelMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1058	wlsxTrapDefinitionsGroup 1058
wlsxOUIMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1059	wlsxTrapDefinitionsGroup 1059
wlsxSSIDMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1060	wlsxTrapDefinitionsGroup 1060
wlsxShortPreableMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1061	wlsxTrapDefinitionsGroup 1061
wlsxWPAMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1062	wlsxTrapDefinitionsGroup 1062
wlsxAdhocNetworkDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1063	wlsxTrapDefinitionsGroup 1063
wlsxAdhocNetworkRemoved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1064	wlsxTrapDefinitionsGroup 1064
wlsxStaPolicyViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1065	wlsxTrapDefinitionsGroup 1065
wlsxRepeatWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1066	wlsxTrapDefinitionsGroup 1066
wlsxWeakWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1067	wlsxTrapDefinitionsGroup 1067
wlsxChannelInterferenceDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1068	wlsxTrapDefinitionsGroup 1068
wlsxChannelInterferenceCleared	1.3.6.1.4.1.14823.2.3.3.1.200.2.1069	wlsxTrapDefinitionsGroup 1069
wlsxAPInterferenceDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1070	wlsxTrapDefinitionsGroup 1070
wlsxAPInterferenceCleared	1.3.6.1.4.1.14823.2.3.3.1.200.2.1071	wlsxTrapDefinitionsGroup 1071
wlsxStaInterferenceDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1072	wlsxTrapDefinitionsGroup 1072

Object	Object ID	
wlsxStaInterferenceCleared	1.3.6.1.4.1.14823.2.3.3.1.200.2.1073	wlsxTrapDefinitionsGroup 1073
wlsxFrameRetryRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1074	wlsxTrapDefinitionsGroup 1074
wlsxFrameReceiveErrorRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1075	wlsxTrapDefinitionsGroup 1075
wlsxFrameFragmentationRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1076	wlsxTrapDefinitionsGroup 1076
wlsxFrameBandWidthRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1077	wlsxTrapDefinitionsGroup 1077
wlsxFrameLowSpeedRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1078	wlsxTrapDefinitionsGroup 1078
wlsxFrameNonUnicastRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1079	wlsxTrapDefinitionsGroup 1079
wlsxLoadbalancingEnabled	1.3.6.1.4.1.14823.2.3.3.1.200.2.1080	wlsxTrapDefinitionsGroup 1080
wlsxLoadbalancingDisabled	1.3.6.1.4.1.14823.2.3.3.1.200.2.1081	wlsxTrapDefinitionsGroup 1081
wlsxChannelFrameRetryRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1082	wlsxTrapDefinitionsGroup 1082
wlsxChannelFrameFragmentationRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1083	wlsxTrapDefinitionsGroup 1083
wlsxChannelFrameErrorRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1084	wlsxTrapDefinitionsGroup 1084
wlsxSignatureMatchAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1085	wlsxTrapDefinitionsGroup 1085
wlsxSignatureMatchSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1086	wlsxTrapDefinitionsGroup 1086
wlsxChannelRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1087	wlsxTrapDefinitionsGroup 1087
wlsxNodeRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1003	wlsxTrapDefinitionsGroup 1003
wlsxNodeRateAnomalyAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1088	wlsxTrapDefinitionsGroup 1088
wlsxNodeRateAnomalySta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1089	wlsxTrapDefinitionsGroup 1089
wlsxEAPRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1090	wlsxTrapDefinitionsGroup 1090

Object	Object ID	
wlsxSignalAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1091	wlsxTrapDefinitionsGroup 1091
wlsxSequenceNumberAnomalyAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1092	wlsxTrapDefinitionsGroup 1092
wlsxSequenceNumberAnomalySta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1093	wlsxTrapDefinitionsGroup 1093
wlsxDisconnectStationAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1094	wlsxTrapDefinitionsGroup 1094
wlsxApFloodAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1095	wlsxTrapDefinitionsGroup 1095
wlsxAdhocNetwork	1.3.6.1.4.1.14823.2.3.3.1.200.2.1096	wlsxTrapDefinitionsGroup 1096
wlsxWirelessBridge	1.3.6.1.4.1.14823.2.3.3.1.200.2.1097	wlsxTrapDefinitionsGroup 1097
wlsxInvalidMacOUIAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1098	wlsxTrapDefinitionsGroup 1098
wlsxInvalidMacOUISta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1099	wlsxTrapDefinitionsGroup 1099
wlsxWEPMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1100	wlsxTrapDefinitionsGroup 1100
wlsxStaRepeatWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1101	wlsxTrapDefinitionsGroup 1101
wlsxStaWeakWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1102	wlsxTrapDefinitionsGroup 1102
wlsxStaAssociatedToUnsecureAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1103	wlsxTrapDefinitionsGroup 1103
wlsxStaUnAssociatedFromUnsecureAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1104	wlsxTrapDefinitionsGroup 1104
wlsxAdhocNetworkBridgeDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1105	wlsxTrapDefinitionsGroup 1105
wlsxInterferingApDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1106	wlsxTrapDefinitionsGroup 1106
wlsxColdStart	1.3.6.1.4.1.14823.2.3.3.1.200.2.1111	wlsxTrapDefinitionsGroup 1111
wlsxWarmStart	1.3.6.1.4.1.14823.2.3.3.1.200.2.1112	wlsxTrapDefinitionsGroup 1112
wlsxAPImpersonation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1113	wlsxTrapDefinitionsGroup 1113

Object	Object ID	
wlsxNAuthServerIsDown	1.3.6.1.4.1.14823.2.3.3.1.200.2.1115	wlsxTrapDefinitionsGroup 1115
wlsxWindowsBridgeDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1129	wlsxTrapDefinitionsGroup 1129
wlsxSignAPNetstumbler	1.3.6.1.4.1.14823.2.3.3.1.200.2.1134	wlsxTrapDefinitionsGroup 1134
wlsxSignStaNetstumbler	1.3.6.1.4.1.14823.2.3.3.1.200.2.1135	wlsxTrapDefinitionsGroup 1135
wlsxSignAPAsleap	1.3.6.1.4.1.14823.2.3.3.1.200.2.1136	wlsxTrapDefinitionsGroup 1136
wlsxSignStaAsleap	1.3.6.1.4.1.14823.2.3.3.1.200.2.1137	wlsxTrapDefinitionsGroup 1137
wlsxSignAPAirjack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1138	wlsxTrapDefinitionsGroup 1138
wlsxSignStaAirjack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1139	wlsxTrapDefinitionsGroup 1139
wlsxSignAPNullProbeResp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1140	wlsxTrapDefinitionsGroup 1140
wlsxSignStaNullProbeResp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1141	wlsxTrapDefinitionsGroup 1141
wlsxSignAPDeauthBcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1142	wlsxTrapDefinitionsGroup 1142
wlsxSignStaDeauthBcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1143	wlsxTrapDefinitionsGroup 1143
wlsxWindowsBridgeDetectedAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1144	wlsxTrapDefinitionsGroup 1144
wlsxWindowsBridgeDetectedSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1145	wlsxTrapDefinitionsGroup 1145
wlsxAdhocNetworkBridgeDetectedAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1146	wlsxTrapDefinitionsGroup 1146
wlsxAdhocNetworkBridgeDetectedSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1147	wlsxTrapDefinitionsGroup 1147
wlsxDisconnectStationAttackAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1148	wlsxTrapDefinitionsGroup 1148
wlsxDisconnectStationAttackSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1149	wlsxTrapDefinitionsGroup 1149
wlsxSuspectUnsecureAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1150	wlsxTrapDefinitionsGroup 1150

Object	Object ID	
wlsxSuspectUnsecureAPResolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1151	wlsxTrapDefinitionsGroup 1151
wlsxHtGreenfieldSupported	1.3.6.1.4.1.14823.2.3.3.1.200.2.1157	wlsxTrapDefinitionsGroup 1157
wlsxHT40MHzIntoleranceAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1158	wlsxTrapDefinitionsGroup 1158
wlsxHT40MHzIntoleranceSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1159	wlsxTrapDefinitionsGroup 1159
wlsxNAdhocNetwork	1.3.6.1.4.1.14823.2.3.3.1.200.2.1161	wlsxTrapDefinitionsGroup 1161
wlsxNAdhocNetworkBridgeDetectedAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1162	wlsxTrapDefinitionsGroup 1162
wlsxNAdhocNetworkBridgeDetectedSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1163	wlsxTrapDefinitionsGroup 1163
wlsxClientFloodAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1170	wlsxTrapDefinitionsGroup 1170
wlsxValidClientNotUsingEncryption	1.3.6.1.4.1.14823.2.3.3.1.200.2.1171	wlsxTrapDefinitionsGroup 1171
wlsxAdhocUsingValidSSID	1.3.6.1.4.1.14823.2.3.3.1.200.2.1172	wlsxTrapDefinitionsGroup 1172
wlsxAPSpoofingDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1173	wlsxTrapDefinitionsGroup 1173
wlsxClientAssociatingOnWrongChannel	1.3.6.1.4.1.14823.2.3.3.1.200.2.1174	wlsxTrapDefinitionsGroup 1174
wlsxNDisconnectStationAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1175	wlsxTrapDefinitionsGroup 1175
wlsxNStaUnAssociatedFromUnsecureAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1176	wlsxTrapDefinitionsGroup 1176
wlsxOmertaAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1177	wlsxTrapDefinitionsGroup 1177
wlsxTKIPReplayAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1178	wlsxTrapDefinitionsGroup 1178
wlsxChopChopAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1179	wlsxTrapDefinitionsGroup 1179
wlsxFataJackAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1180	wlsxTrapDefinitionsGroup 1180
wlsxInvalidAddressCombination	1.3.6.1.4.1.14823.2.3.3.1.200.2.1181	wlsxTrapDefinitionsGroup 1181

Object	Object ID	
wlsxValidClientMisassociation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1182	wlsxTrapDefinitionsGroup 1182
wlsxMalformedHTIEDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1183	wlsxTrapDefinitionsGroup 1183
wlsxMalformedAssocReqDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1184	wlsxTrapDefinitionsGroup 1184
wlsxOverflowIEDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1185	wlsxTrapDefinitionsGroup 1185
wlsxOverflowEAPOLKeyDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1186	wlsxTrapDefinitionsGroup 1186
wlsxMalformedFrameLargeDurationDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1187	wlsxTrapDefinitionsGroup 1187
wlsxMalformedFrameWrongChannelDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1188	wlsxTrapDefinitionsGroup 1188
wlsxMalformedAuthFrame	1.3.6.1.4.1.14823.2.3.3.1.200.2.1189	wlsxTrapDefinitionsGroup 1189
wlsxCTSRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1190	wlsxTrapDefinitionsGroup 1190
wlsxRTSRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1191	wlsxTrapDefinitionsGroup 1191
wlsxNRogueAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1192	wlsxTrapDefinitionsGroup 1192
wlsxNRogueAPResolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1193	wlsxTrapDefinitionsGroup 1193
wlsxNeighborAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1194	wlsxTrapDefinitionsGroup 1194
wlsxNInterferingAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1195	wlsxTrapDefinitionsGroup 1195
wlsxNSuspectRogueAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1196	wlsxTrapDefinitionsGroup 1196
wlsxNSuspectRogueAPResolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1197	wlsxTrapDefinitionsGroup 1197
wlsxBlockAckAttackDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1198	wlsxTrapDefinitionsGroup 1198
wlsxHotspotterAttackDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1199	wlsxTrapDefinitionsGroup 1199
wlsxNSignatureMatch	1.3.6.1.4.1.14823.2.3.3.1.200.2.1200	wlsxTrapDefinitionsGroup 1200

Object	Object ID	
wlsxNSignatureMatchNetstumbler	1.3.6.1.4.1.14823.2.3.3.1.200.2.1201	wlsxTrapDefinitionsGroup 1201
wlsxNSignatureMatchAsleap	1.3.6.1.4.1.14823.2.3.3.1.200.2.1202	wlsxTrapDefinitionsGroup 1202
wlsxNSignatureMatchAirjack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1203	wlsxTrapDefinitionsGroup 1203
wlsxNSignatureMatchNullProbeResp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1204	wlsxTrapDefinitionsGroup 1204
wlsxNSignatureMatchDeauthBcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1205	wlsxTrapDefinitionsGroup 1205
wlsxNSignatureMatchDisassocBcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1206	wlsxTrapDefinitionsGroup 1206
wlsxNSignatureMatchWellenreiter	1.3.6.1.4.1.14823.2.3.3.1.200.2.1207	wlsxTrapDefinitionsGroup 1207
wlsxAPDeauthContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1208	wlsxTrapDefinitionsGroup 1208
wlsxClientDeauthContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1209	wlsxTrapDefinitionsGroup 1209
wlsxAPWiredContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1210	wlsxTrapDefinitionsGroup 1210
wlsxClientWiredContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1211	wlsxTrapDefinitionsGroup 1211
wlsxAPTaggedWiredContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1212	wlsxTrapDefinitionsGroup 1212
wlsxClientTaggedWiredContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1213	wlsxTrapDefinitionsGroup 1213
wlsxTarpitContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1214	wlsxTrapDefinitionsGroup 1214
wlsxAPChannelChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1216	wlsxTrapDefinitionsGroup 1216
wlsxAPPowerChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1217	wlsxTrapDefinitionsGroup 1217
wlsxAPModeChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1218	wlsxTrapDefinitionsGroup 1218
wlsxUserEntryAttributesChanged	1.3.6.1.4.1.14823.2.3.3.1.200.2.1219	wlsxTrapDefinitionsGroup 1219
wlsxPowerSaveDosAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1220	wlsxTrapDefinitionsGroup 1220

Object	Object ID	
wlsxNAPMasterStatusChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1221	wlsxTrapDefinitionsGroup 1221
wlsxNAdhocUsingValidSSID	1.3.6.1.4.1.14823.2.3.3.1.200.2.1222	wlsxTrapDefinitionsGroup 1222
wlsxMgmtUserAuthenticationFailed	1.3.6.1.4.1.14823.2.3.3.1.200.2.1224	wlsxTrapDefinitionsGroup 1224

wlsxNUserEntryCreated

Objects	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress
Status	current
Description	This trap indicates that a new user was created.

wlsxNUserEntryDeleted

Objects	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress
Status	current
Description	This trap indicates that a user was deleted.

wlsxNUserEntryAuthenticated

Objects	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress, wlsxTrapUserName, wlsxTrapUserAuthenticatio Method, wlsxTrapUserRole
Status	current
Description	This trap indicates that a user is Authenticated.

wlsxNUserEntryDeAuthenticated

Objects	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress
Status	current
Description	This trap indicates that a user is Deauthenticated.

wlsxNUserAuthenticationFailed

Objects	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress
Status	current
Description	This trap indicates that a user authentication has failed.

wlsxNAuthServerReqTimedOut

Objects	wlsxTrapTime, wlsxTrapAuthServerName
Status	current
Description	This trap indicates that the authentication server request timed out.

wlsxNAuthServerTimedOut

Objects	wlsxTrapTime, wlsxTrapAuthServerName, wlsxTrapAuthServerTimeout
Status	current
Description	This trap indicates that the authentication server timed out.

wlsxNAuthServerIsUp

Objects	wlsxTrapTime, wlsxTrapAuthServerName
Status	current
Description	This trap indicates that an authentication server is up.

wlsxNAccessPointIsUp

Objects	wlsxTrapTime, wlsxTrapAPMacAddress
Status	current
Description	A Trap which indicates that an access point up.

wlsxNAccessPointIsDown

Objects	wlsxTrapTime, wlsxTrapAPMacAddress
Status	current
Description	A Trap which indicates that an access point down.

wlsxNChannelChanged

Objects	wlsxTrapTime, wlsxTrapAPBSSID, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an access point at Location wlsxTrapAPLocation has changed the channel.

wlsxNStationAddedToBlackList

Objects	wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapStationBlackListReason
Status	current
Description	This trap indicates that the station is black listed.

wlsxNStationRemovedFromBlackList

Objects	wlsxTrapTime, wlsxTrapNodeMac
Status	current
Description	This trap indicates that the station is removed from the black list. the frame type.

wlsxNRadioAttributesChanged

Objects	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPIpAddress, wlsxTrapAPChannel, wlsxTrapAPTxPower }
Status	current
Description	A Trap which indicates changes in the Radio attributes of an access point.

wlsxUnsecureAPDetected

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel, wlsxTrapMatchedMac, wlsxTrapMatchedIp, wlsxTrapRogueInfoURL}
Status	current
Description	This trap indicates that an unauthorized access point is connected to the wired network. The access point is declared Rogue because it was matched to a MAC address.

wlsxUnsecureAPResolved

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that a previously detected access point, classified as Rogue, is no longer present in the network.

wlsxStaImpersonation

Objects	{ wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
Status	current
Description	This trap indicates that an AM detected Station Impersonation.

wlsxReservedChannelViolation

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AM detected an access point which is violating the Reserved Channel configuration.

wlsxValidSSIDViolation

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP has detected an access point is violating Valid SSID configuration by using an SSID that is reserved for use by a valid AP only.

wlsxChannelMisconfiguration

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP detected an access point that has a channel misconfiguration because it is using a channel that is not valid.

wlsxOUIMisconfiguration

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP detected an access point that has an OUI misconfiguration because it is using an OUI that is not valid.

wlsxSSIDMisconfiguration

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP detected an access point that has an SSID misconfiguration because it is using an SSID that is not valid.

wlsxShortPreableMisconfiguration

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an access point has bad short preamble configuration.

wlsxWPAMisconfiguration

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP detected an access point that is misconfigured because it is not using WPA.

wlsxAdhocNetworkDetected

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AM has detected an adhoc network.

wlsxAdhocNetworkRemoved

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that a previously detected adhoc network is no longer present in the network.

wlsxStaPolicyViolation

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapNodeMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that Protection was enforced because a valid station's association to a non-valid access point violated Valid Station policy. For more information check http://www.wve.org/entries/show/WVE-2005-0008 and http://www.wve.org/entries/show/WVE-2005-0019.

wlsxRepeatWEPIVViolation

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP detected that a valid access point is using the same WEP initialization vector in consecutive packets.

wlsxWeakWEPIVViolation

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP detected that a valid access point is using a Weak WEP initialization vector. For more information check http://www.wve.org/entries/show/WVE-2005-0021

wlsxChannelInterferenceDetected

Objects	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation,wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP has detected channel interference.

wlsxChannelInterferenceCleared

Objects	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that a previously detected channel interference is no longer present.

wlsxAPInterferenceDetected

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP has detected interference for an access point.

wlsxAPInterferenceCleared

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that the previously detected interference for an access point is no longer present.

wlsxStaInterferenceDetected

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapNodeMac, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP has detected interference for a station.

wlsxStaInterferenceCleared

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapNodeMac, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that the previously detected interference for a station is no longer present.

wlsxFrameRetryRateExceeded

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP detected that an access point has exceeded the configured upper threshold for Frame Retry Rate.

wlsxFrameReceiveErrorRateExceeded

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapTargetAPChannel, wlsxTrapAPLocation }
Status	current
Description	This trap indicates that an AP detected that an access point has exceeded the configured upper threshold for Frame Receive Error Rate.

wlsxFrameFragmentationRateExceeded

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapTargetAPChannel, wlsxTrapAPLocation }
Status	current
Description	This trap indicates that an AP detected that an access point exceeded the configured upper threshold for Frame Fragmentation Rate.

wlsxFrameBandWidthRateExceeded

Objects	{ wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP detected that a station or access point has exceeded the configured upper threshold for Bandwidth rate.

wlsxFrameLowSpeedRateExceeded

Objects	{ wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP detected that a station has exceeded the configured upper threshold for Low speed rate.

wlsxFrameNonUnicastRateExceeded

Objects	{ wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP detected that station has exceeded the configured upper threshold for Non Unicast traffic rate.

wlsxLoadbalancingEnabled

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	

wlsxLoadbalancingDisabled

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AM is reporting that an AP has enabled Load balancing.

wlsxChannelFrameRetryRateExceeded

Objects	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP has detected that the configured upper threshold for Frame Retry Rate was exceeded on a channel.

wlsxChannelFrameFragmentationRateExceeded

Objects	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP has detected that the configured upper threshold for Frame Fragmentation Rate was exceeded on a channel.

wlsxChannelFrameErrorRateExceeded

Objects	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP has detected that the configured upper threshold for Frame Receive Error Rate was exceeded on a channel.

wlsxSignatureMatchAP

Objects	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AP detected a signature match in a frame from an access point.

wlsxSignatureMatchSta

Objects	{ wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
Status	current
Description	This trap indicates that an AP detected a signature match in a frame from a Station.

wlsxChannelRateAnomaly

Objects	{ wlsxTrapTime, wlsxTrapFrameType, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP detected frames on a channel which exceed the configured IDS rate threshold. For more information check: http://www.wve.org/entries/show/WVE-2005-0052 http://www.wve.org/entries/show/WVE-2005-0045 http://www.wve.org/entries/show/WVE-2005-0046 http://www.wve.org/entries/show/WVE-2005-0047 http://www.wve.org/entries/show/WVE-2005-0048

wlsxNodeRateAnomaly

Objects	wlsxTrapTime, wlsxTrapFrameType, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPBSSID, wlsxTrapAPLocation
Status	current
Description	This trap indicates that a node is exceeding the threshold set for the frame type.

wlsxNodeRateAnomalyAP

Objects	{wlsxTrapTime, wlsxTrapFrameType, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AP detected frames transmitted or received by an

	access point, which exceed the configured IDS rate threshold. For more information check: http://www.wve.org/entries/show/WVE-2005-0052 http://www.wve.org/entries/show/WVE-2005-0045 http://www.wve.org/entries/show/WVE-2005-0046 http://www.wve.org/entries/show/WVE-2005-0047 http://www.wve.org/entries/show/WVE-2005-0048

wlsxNodeRateAnomalySta

Objects	{wlsxTrapTime, wlsxTrapFrameType, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AP detected frames transmitted or received by a node, which exceed the configured IDS rate threshold.

wlsxEAPRateAnomaly

Objects	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that the rate of EAP Handshake packets received by an AP has exceeded the configured IDS EAP Handshake rate threshold. For more information check http://www.wve.org/entries/show/WVE-2005-0049

wlsxSignalAnomaly

Objects	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AM detected a Signal Anomaly.

wlsxSequenceNumberAnomalyAP

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
Status	current
Description	This trap indicates that an AM received packets from an AP which exceeds the acceptable sequence number difference. The acceptable sequence number difference is an IDS configuration object. For more information check: http://www.wve.org/entries/show/WVE-2005-0061 http://www.wve.org/entries/show/WVE-2005-0019 http://www.wve.org/entries/show/WVE-2005-0008 http://www.wve.org/entries/show/WVE-2005-0045 http://www.wve.org/entries/show/WVE-2005-0046 http://www.wve.org/entries/show/WVE-2005-0047 http://www.wve.org/entries/show/WVE-2005-0048

wlsxSequenceNumberAnomalySta

Objects	wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that an AM received packets from a Node which exceeds the acceptable sequence number difference. The acceptable sequence number difference is an IDS configuration object. For more information check http://www.wve.org/entries/show/WVE-2005-0061 http://www.wve.org/entries/show/WVE-2005-0019 http://www.wve.org/entries/show/WVE-2005-0008 http://www.wve.org/entries/show/WVE-2005-0045 http://www.wve.org/entries/show/WVE-2005-0046 http://www.wve.org/entries/show/WVE-2005-0047 http://www.wve.org/entries/show/WVE-2005-0048

wlsxDisconnectStationAttack

Objects	{ wlsxTrapTime, wlsxTrapFrameType, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AM detected a station Disconnect attack. For more information check: http://www.wve.org/entries/show/WVE-2005-0045 http://www.wve.org/entries/show/WVE-2005-0046 http://www.wve.org/entries/show/WVE-2005-0048

wlsxApFloodAttack

Objects	{ wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that the number of potential fake APs detected by an AP has exceeded the configured IDS threshold. This is the total number of fake APs observed across all bands. For more information check http://www.wve.org/entries/show/WVE-2005-0056

wlsxAdhocNetwork

Objects	{ wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
Status	current
Description	This trap indicates that an AM detected an Adhoc Network. A station is connected to an adhoc AP.

wlsxWirelessBridge

Objects	{ wlsxTrapTime, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AP detected a Wireless Bridge when a WDS frame was seen between the transmitter and receiver addresses.

wlsxInvalidMacOUIAP

Objects	{wlsxTrapTime, wlsxTrapAddressType, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AP detected an invalid MAC OUI in the BSSID of a frame. An invalid MAC OUI suggests that the frame may be spoofed.

wlsxInvalidMacOUISta

Objects	{wlsxTrapTime, wlsxTrapAddressType, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AP detected an invalid MAC OUI in the SRC or DST address of a frame. An invalid MAC OUI suggests that the frame may be spoofed.

wlsxWEPMisconfiguration

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP detected an access point that is misconfigured because it does not have Privacy enabled.

wlsxStaRepeatWEPIVViolation

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP detected that a valid station is using the same WEP initialization vector in consecutive packets.

wlsxStaWeakWEPIVViolation

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP detected that a valid station is using a Weak WEP initialization vector.

wlsxStaAssociatedToUnsecureAP

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapNodeMac, wlsxTrapAPLocation, wlsxTrapAPChannel, wlsxTrapRogueInfoURL}
Status	current
Description	This trap indicates that an AM detected a client associated with a Rogue access point.

wlsxStaUnAssociatedFromUnsecureAP

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapNodeMac}
Status	current
Description	This trap indicates that a previously detected rogue access point association is no longer present.

wlsxAdhocNetworkBridgeDetected

Objects	{ wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AM has detected an Adhoc network that is bridging to a wired network.

wlsxInterferingApDetected

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel, wlsxTrapInterferingAPInfoURL }
Status	current
Description	This trap indicates that an AP detected an access point classified as Interfering. The access point is declared Interfering because it is neither authorized nor classified as Rogue.

wlsxColdStart

Objects	wlsxTrapTime
Status	current
Description	An enterprise version of cold start trap, which contains the controller time stamp.

wlsxWarmStart

Objects	wlsxTrapTime
Status	current
Description	An enterprise version of warm start trap, which contains the controller time stamp.

wlsxAPImpersonation

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP detected AP Impersonation because the number of beacons seen has exceeded the expected number by the configured percentage threshold.The expected number is calculated based on the Beacon Interval Field in the Beacon frame.

wlsxNAuthServerIsDown

Objects	{ wlsxTrapTime, wlsxTrapAuthServerName }
Status	current
Description	This trap indicates that an authentication server is down.

wlsxWindowsBridgeDetected

Objects	{ wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AM has detected a station that is bridging from a wireless network to a wired network.

wlsxSignAPNetstumbler

Objects	{ wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }

Status	current
Description	This trap indicates that an AP detected a signature match for Netstumbler from an access point. For more information check http://www.wve.org/entries/show/WVE-2005-0025

wlsxSignStaNetstumbler

Objects	{ wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
Status	current
Description	This trap indicates that an AP detected a signature match for Netstumbler from a Station. For more information check http://www.wve.org/entries/show/WVE-2005-0025.

wlsxSignAPAsleap

Objects	{ wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
Status	current
Description	This trap indicates that an AP detected a signature match for ASLEAP from an access point. For more information check http://www.wve.org/entries/show/WVE-2005-0027

wlsxSignStaAsleap

Objects	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AP detected a signature match for ASLEAP from a Station.For more information check http://www.wve.org/entries/show/WVE-2005-0027

wlsxSignAPAirjack

Objects	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
Status	current
Description	This trap indicates that an AP detected a signature match for AirJack from an access point. For more information check http://www.wve.org/entries/show/WVE-2005-0018

wlsxSignStaAirjack

Objects	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}

Status	current
Description	This trap indicates that an AP detected a signature match for AirJack from a Station. For more information check http://www.wve.org/entries/show/WVE-2005-0018

wlsxSignAPNullProbeResp

Objects	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AP detected a signature match for Null-Probe-Response from an access point. For more information check http://www.wve.org/entries/show/WVE-2006-0064

wlsxSignStaNullProbeResp

Objects	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AP detected a signature match for Null-Probe-Response from a Station. For more information check http://www.wve.org/entries/show/WVE-2006-0064

wlsxSignAPDeauthBcast

Objects	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AP detected a signature match for Deauth-Broadcast from an access point. For more information check: http://www.wve.org/entries/show/WVE-2005-0019 http://www.wve.org/entries/show/WVE-2005-0045

wlsxSignStaDeauthBcast

Objects	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AP detected a signature match for Deauth-Broadcast from a Station.For more information check: http://www.wve.org/entries/show/WVE-2005-0019 http://www.wve.org/entries/show/WVE-2005-0045

wlsxWindowsBridgeDetectedAP

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP is detecting an access point that is bridging from a wireless network to a wired network.

wlsxWindowsBridgeDetectedSta

Objects	{ wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP is detecting a station that is bridging from a wireless network to a wired network.

wlsxAdhocNetworkBridgeDetectedAP

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AM has detected an adhoc network that is bridging to a wired network

wlsxAdhocNetworkBridgeDetectedSta

Objects	wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AM has detected an adhoc network that is bridging to a wired network

wlsxDisconnectStationAttackAP

Objects	{wlsxTrapTime, wlsxTrapFrameType, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that an AM detected a station Disconnect attack. For more information check: http://www.wve.org/entries/show/WVE-2005-0045 http://www.wve.org/entries/show/WVE-2005-0046 http://www.wve.org/entries/show/WVE-2005-0048

wlsxDisconnectStationAttackSta

Objects	wlsxTrapTime, wlsxTrapFrameType, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that an AM detected a station Disconnect attack. For more information check: http://www.wve.org/entries/show/WVE-2005-0045 http://www.wve.org/entries/show/WVE-2005-0046 http://www.wve.org/entries/show/WVE-2005-0048

wlsxSuspectUnsecureAPDetected

Objects	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPRadioNumber, wlsxTrapMatchedMac, wlsxTrapMatchedIp, wlsxTrapConfidenceLevel, wlsxTrapAPLocation, wlsxTrapRogueInfoURL}
Status	current
Description	This trap indicates that an access point, classified as Suspected Rogue, has been detected by a Controller. The AP is suspected to be rogue, with the supplied confidence level, because it was matched to the wired MAC address.

wlsxSuspectUnsecureAPResolved

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPRadioNumber
Status	current
Description	This trap indicates that a previously detected access point, classified Suspected Rogue, is either no longer present in the network or has changed its state.

wlsxHtGreenfieldSupported

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected an access point that supports HT Greenfield mode. For more information check http://www.wve.org/entries/show/WVE-2008-0005

wlsxHT40MHzIntoleranceAP

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID,wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress,wlsxTrapAPRadioNumber, wlsxTrapAPLocation,wlsxTrapAPChannel }
Status	current
Description	This trap indicates that an AP is detecting an access point with the HT 40MHz intolerance setting. For more information check http://www.wve.org/entries/show/WVE-2008-0004

wlsxHT40MHzIntoleranceSta

Objects	{wlsxTrapTime, wlsxTrapSourceMac,wlsxTrapSnr, wlsxTrapAPChannel,wlsxTrapFrameType, wlsxTrapAPMacAddress,wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
Status	current
Description	This trap indicates that the system is detecting an HT 40MHz Intolerance setting from a Station. For more information check http://www.wve.org/entries/show/WVE-2008-0004

wlsxNAdhocNetwork

Objects	{wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP detected an adhoc network where a station is connected to an adhoc access point.

wlsxNAdhocNetworkBridgeDetectedAP

Objects	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP detected an adhoc network that is bridging to a wired network.

wlsxNAdhocNetworkBridgeDetectedSta

Objects	{ wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
Status	current
Description	This trap indicates that an AP detected an adhoc network that is bridging to a wired network.

wlsxClientFloodAttack

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that the number of potential fake clients detected by an AP has exceeded the configured IDS threshold. This is the total number of fake clients observed across all bands. For more information check http://www.wve.org/entries/show/WVE-2005-0056

wlsxValidClientNotUsingEncryption

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected an unencrypted data frame between a valid client and an access point.

wlsxAdhocUsingValidSSID

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected an adhoc network using a valid/protected SSID. For more information check http://www.wve.org/entries/show/WVE-2005-0008

wlsxAPSpoofingDetected

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapSpoofedFrameType, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected that one of its virtual APs is being spoofed using MAC spoofing. For more information check http://www.wve.org/entries/show/WVE-2005-0019

wlsxClientAssociatingOnWrongChannel

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapSpoofedFrameType, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected a client trying to associate to one of its BSSIDs on the wrong channel. This can be a sign that the BSSID is being spoofed in order to fool the client into thinking the AP is operating on another channel.

wlsxNDisconnectStationAttack

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current

Description	This trap indicates that an AP has determined that a client is under Disconnect Attack because the rate of Assoc/Reassoc Response packets received by that client exceeds the configured threshold. For more information check: http://www.wve.org/entries/show/WVE-2005-0045 http://www.wve.org/entries/show/WVE-2005-0046 http://www.wve.org/entries/show/WVE-2005-0048

wlsxNStaUnAssociatedFromUnsecureAP

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapNodeMac, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP that had previously detected a client association to a Rogue access point is no longer detecting that association.

wlsxOmertaAttack

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected an Omerta attack. For more information check http://www.wve.org/entries/show/WVE-2005-0053

wlsxTKIPReplayAttack

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
Status	current
Description	This trap indicates that an AP detected a TKIP replay attack. If successful this could be the precursor to more advanced attacks. For more information check http://www.wve.org/entries/show/WVE-2008-0013

wlsxChopChopAttack

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
Status	current
Description	This trap indicates that an AP detected a ChopChop attack. For more information check http://www.wve.org/entries/show/WVE-2006-0038

wlsxFataJackAttack

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected a FATA-Jack attack. For more information check http://www.wve.org/entries/show/WVE-2006-0057

wlsxInvalidAddressCombination

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapAPChannel, wlsxTrapSnr
Status	current
Description	This trap indicates that an AP detected an invalid source and destination combination. For more information check http://www.wve.org/entries/show/WVE-2008-0011

wlsxValidClientMisassociation

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapAssociationType, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected a misassociation between a valid client and an unsafe AP.

wlsxMalformedHTIEDetected

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
Status	current
Description	This trap indicates that an AP detected a malformed HT Information Element. This can be the result of a misbehaving wireless driver or it may be an indication of a new wireless attack.

wlsxMalformedAssocReqDetected

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
Status	current
Description	This trap indicates that an AP detected a malformed association request with a NULL SSID. For more information check http://www.wve.org/entries/show/WVE-2008-0010

wlsxOverflowIEDetected

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
Status	current
Description	This trap indicates that an AP detected a management frame with a malformed information element. The declared length of the element is larger than the entire frame containing the element. This may be used to corrupt or crash wireless drivers. For more information check http://www.wve.org/entries/show/WVE-2008-0008

wlsxOverflowEAPOLKeyDetected

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
Status	current
Description	This trap indicates that an AP detected a key in an EAPOL Key message with a specified length greater than the length of the entire message. For more information check http://www.wve.org/entries/show/WVE-2008-0009

wlsxMalformedFrameLargeDurationDetected

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapAPChannel, wlsxTrapSnr
Status	current
Description	This trap indicates that an AP detected an unusually large duration in a wireless frame. This may be an attempt to block other devices from transmitting. For more information check http://www.wve.org/entries/show/WVE-2005-0051

wlsxMalformedFrameWrongChannelDetected

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapTargetAPChannel, wlsxTrapAPChannel, wlsxTrapSnr
Status	current
Description	This trap indicates that an AP detected a beacon on one channel advertising another channel. This could be an attempt to lure clients away from a valid AP. For more information check http://www.wve.org/entries/show/WVE-2006-0050

wlsxMalformedAuthFrame

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel

Status	current
Description	This trap indicates that an AP detected an authentication frame with either a bad algorithm (similar to Fata-Jack) or a bad transaction. For more information check http://www.wve.org/entries/show/WVE-2006-0057

wlsxCTSRateAnomaly

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that the rate of CTS packets received by an AP exceeds the configured IDS threshold.

wlsxRTSRateAnomaly

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that the rate of RTS packets received by an AP exceeds the configured IDS threshold.

wlsxNRogueAPDetected

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an unauthorized access point is connected to the wired network. The access point is classified as Rogue by the system.

wlsxNRogueAPResolved

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel
Status	current
Description	This trap indicates that a previously detected access point, classified as Rogue, is either no longer present in the network or it changed its state.

wlsxNeighborAPDetected

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an access point has been classified as a Neighbor by the system.

wlsxNInterferingAPDetected

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an access point has been classified as Interfering by the system. The access point is declared Interfering because it is not authorized, nor has it been classified as a rogue.

wlsxNSuspectRogueAPDetected

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel, wlsxTrapConfidenceLevel
Status	current
Description	This trap indicates that an access point, classified as suspected rogue, is detected by the system. The AP is suspected to be rogue with the supplied confidence level.

wlsxNSuspectRogueAPResolved

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel
Status	current
Description	This trap indicates that a previously detected access point, classified as suspected rogue, is either no longer present in the network or has changed its state.

wlsxBlockAckAttackDetected

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
Status	current
Description	This trap indicates that an attempt has been made to deny service to the source address by spoofing a block ACK add request that sets a sequence number window outside the currently used window. For more information check http://www.wve.org/entries/show/WVE-2008-0006

wlsxHotspotterAttackDetected

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapNodeMac, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr, wlsxTrapTargetAPSSID
Status	current
Description	This trap indicates that a new AP has appeared immediately following a client probe request. This is indicative of the Hotspotter tool or similar that attempts to trap clients with a fake hotspot or other wireless network. For more information check http://www.wve.org/entries/show/WVE-2005-0054

wlsxNSignatureMatch

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected a signature match in a frame.

wlsxNSignatureMatchNetstumbler

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected a signature match for Netstumbler in a frame. For more information check http://www.wve.org/entries/show/WVE-2005-0025

wlsxNSignatureMatchAsleap

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected a signature match for ASLEAP in a frame. For more information check http://www.wve.org/entries/show/WVE-2005-0027

wlsxNSignatureMatchAirjack

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected a signature match for Airjack in a frame. For more information check http://www.wve.org/entries/show/WVE-2005-0018

wlsxNSignatureMatchNullProbeResp

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel

Max-Access	
Status	current
Description	This trap indicates that an AP detected a signature match for Null-Probe-Response in a frame. For more information check http://www.wve.org/entries/show/WVE-2006-0064

wlsxNSignatureMatchDeauthBcast

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Max-Access	
Status	current
Description	This trap indicates that an AP detected a signature match for Deauth-Broadcast in a frame. For more information check: http://www.wve.org/entries/show/WVE-2005-0019 http://www.wve.org/entries/show/WVE-2005-0045

wlsxNSignatureMatchDisassocBcast

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Max-Access	
Status	current
Description	This trap indicates that an AP detected a signature match for Disassoc-Broadcast in a frame. For more information check: http://www.wve.org/entries/show/WVE-2005-0019 http://www.wve.org/entries/show/WVE-2005-0046

wlsxNSignatureMatchWellenreiter

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected a signature match for Wellenreiter in a frame. For more information check http://www.wve.org/entries/show/WVE-2006-0058

wlsxAPDeauthContainment

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapNodeMac, wlsxTrapAPChannel, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that an AP has attempted to contain an access point by disconnecting its client.

wlsxClientDeauthContainment

Objects	wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that an AP has attempted to contain a client by disconnecting it from the AP that it is associated with.

wlsxAPWiredContainment

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapNodeMac, wlsxTrapDeviceIpAddress, wlsxTrapDeviceMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that an AP has attempted to contain an access point by disrupting traffic to its client on the wired interface.

wlsxClientWiredContainment

Objects	wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapDeviceIpAddress, wlsxTrapDeviceMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that an AP has attempted to contain a client by disrupting traffic to it on the wired interface.

wlsxAPTaggedWiredContainment

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapNodeMac, wlsxTrapDeviceIpAddress, wlsxTrapDeviceMac, wlsxTrapVlanId, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that an AP has attempted to contain an access point by disrupting traffic to its client on the wired interface.

wlsxClientTaggedWiredContainment

Objects	wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapDeviceIpAddress, wlsxTrapDeviceMac, wlsxTrapVlanId, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that an AP has attempted to contain a client by disrupting traffic to it on the wired interface.

wlsxTarpitContainment

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapNodeMac, wlsxTrapAPChannel, wlsxTrapTargetAPChannel, wlsxTrapSourceMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that an AP has attempted to contain an access point by moving a client that is attempting to associate to it to a tarpit.

wlsxAPChannelChange

Objects	wlsxTrapTime, wlsxTrapAPChannel, wlsxTrapAPChannelSec, wlsxTrapAPPrevChannel, wlsxTrapAPPrevChannelSec, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPARMChangeReason
Status	current
Description	This trap indicates that an AP changed its channel.

wlsxAPPowerChange

Objects	wlsxTrapTime, wlsxTrapAPTxPower, wlsxTrapAPPrevTxPower, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that an AP changed its transmit power level.

wlsxAPModeChange

Objects	wlsxTrapTime, wlsxTrapAPCurMode, wlsxTrapAPPrevMode, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
Status	current
Description	This trap indicates that an AP changed its mode from AP to AP Monitor or vice versa.

wlsxUserEntryAttributesChanged

Objects	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress, wlsxTrapAPBSSID, wlsxTrapAPName, wlsxTrapCardSlot, wlsxTrapPortNumber, wlsxTrapUserAttributeChangeType
Status	current
Description	This trap indicates that the user entry attributes have changed.

wlsxPowerSaveDosAttack

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected a Power Save DoS attack.

wlsxNAPMasterStatusChange

Objects	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapApControllerIp, wlsxTrapApMasterStatus
Status	current
Description	This trap indicates that the status of the AP as seen by the master controller has changed.

wlsxNAdhocUsingValidSSID

Objects	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
Status	current
Description	This trap indicates that an AP detected an adhoc network node using a valid/protected SSID. For more information check http://www.wve.org/entries/show/WVE-2005-0008

wlsxMgmtUserAuthenticationFailed

Objects	wlsxTrapTime, wlsxTrapUserName, wlsxTrapUserIpAddress, wlsxTrapAuthServerName
Status	current
Description	

SNMP Traps

SNMP 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).

The following traps are supported for the ifTable objects:

- linkDown
- linkUp

These traps are sent when there is change on a specific interface such as GRE or Ethernet.

linkDown

Object ID	1.3.6.1.6.3.1.1.5.3
Syntax	NA
Max-Access	Current
Objects	• ifIndex • ifAdminStatus • ifOperStatus
Status	current
Description	Indicates that change of state in communication link.

linkUp

Object ID	1.3.6.1.6.3.1.1.5.4
Syntax	NA
Max-Access	Current
Objects	• ifIndex • ifAdminStatus • ifOperStatus
Status	current
Description	Indicates that change of state in communication link.