CHAPTER 13

Alarm and Event Dictionary

This chapter describes the event and alarm notifications that the wireless LAN controller, access points, and location appliances can receive. It also identifies specific actions the administrator can take to address these alarms and events.

It describes the event and alarm notifications that the wireless LAN controller, access points, and location appliances can receive. In addition, specific actions an administrator can do to address these alarms and events are described.

Note Not all traps which are seen on the WLC GUI are supported by NCS.

This chapter includes the following sections:

Notification Format

For each alarm and event notification, the following information is provided (see Table 13-1).

Table 13-1 Trap Notification Format

Field	NCS Message
MIB Name	The MIB Name is the name of the notification as defined in the management information base (MIB). In some cases, if the event is specific only to the NMS, this field is not relevant. You can define multiple events in NCS from the same trap based on the values of the variables present in the trap. In such cases, multiple subentries appear with the same MIB Name. In addition, this field displays the value of the variable that caused NCS to generate this event.
Alarm Condition	This filed displays the condition for which the trap was generated.
NCS Message	The NCS Message is a text string that reflects the message displayed in the NCS alarm or event browser associated with this event. Numbers such as "{0}" reflect internal NCS variables that typically are retrieved from variables in the trap. However, the order of the variables as they appear in the trap cannot be derived from the numbers.
Symptoms	This field displays the symptoms associated with this event.
Severity	This field displays the severity assigned to this event in NCS.
Category	This field displays the category of the trap.
Probable Causes	This field lists the probable causes of the notification.
Recommended Actions	This field lists any actions recommended for the administrator managing the wireless network.

Traps Added in Release 2.0

The following traps were added to WCS Release 2.0:

AP_BIG_NAV_DOS_ATTACK

MIB Name	bsnApBigNavDosAttack.
Alarm Condition	AP big nav DOS attack.
NCS Message	The AP "{0}" with protocol "{1}" receives a message with a large NAV field and all traffic on the channel is suspended. This is most likely a malicious denial of service attack.
Symptoms	The system detected a possible denial of service attack and suspended all traffic to the affected channel.
Severity	Critical.
Category	Security
Probable Causes	A malicious denial of service attack is underway.
Recommended Actions	Identify the source of the attack in the network and take the appropriate action immediately.

AP_CONTAINED_AS_ROGUE

MIB Name	bsnAPContainedAsARogue.
Alarm Condition	AP contained as rogue.
NCS Message	AP "{0}" with protocol "{1}" on Switch "{2}" is contained as a Rogue preventing service.
Symptoms	An access point is reporting that it is being contained as a rogue.
Severity	Critical.
Category	Access Point.
Probable Causes	Another system is containing this access point.
Recommended Actions	Identify the system containing this access point. You may need to use a wireless sniffer.

AP_HAS_NO_RADIOS

MIB Name	bsnApHasNoRadioCards.
Alarm Condition	AP has no radios.
NCS Message	AP "{0}" on Controller "{1}" has no Radio cards.
Symptoms	An access point is reporting that it has no radio cards.
Severity	Critical.
Category	Access Point.

MIB Name	bsnApHasNoRadioCards.
Alarm Condition	AP has no radios.
Probable Causes	Manufacturing fault or damage to the system during shipping.
Recommended Actions	Call customer support.

AP_MAX_ROGUE_COUNT_CLEAR

MIB Name	bsnApMaxRogueCountClear.
Alarm Condition	AP maximum rogue count cleared.
NCS Message	Fake AP or other attack on AP with MAC address "{0}" associated with Switch "{2}" is cleared now. Rogue AP count is within the threshold of "{1}'."
Symptoms	The number of rogues detected by a switch (controller) is within acceptable limits.
Severity	Clear.
Category	Rogue AP
Probable Causes	None.
Recommended Actions	None.

AP_MAX_ROGUE_COUNT_EXCEEDED

MIB Name	bsnApMaxRogueCountExceeded.
Alarm Condition	AP maximum rogue count exceeded.
NCS Message	Fake AP or other attack may be in progress. Rogue AP count on AP with MAC address "{0}" associated with Switch "{2}" has exceeded the severity warning threshold of "{1}."
Symptoms	The number of rogues detected by a switch (controller) exceeds the internal threshold.
Severity	Critical.
Category	Rogue AP
Probable Causes	• There may be too many rogue access points in the network. • A fake access point attack may be in progress.
Recommended Actions	Identify the source of the rogue access points.

AUTHENTICATION_FAILURE (From MIB-II standard)

MIB Name	AuthenticationFailure.
Alarm Condition	Authentication failure reported by controller.
NCS Message	Switch "{0}". Authentication failure reported.
Symptoms	There was an SNMP authentication failure on the switch (controller).
Severity	Minor.
Category	Security
Probable Causes	An incorrect community string is in use by a management application.
Recommended Actions	Identify the source of the incorrect community string and correct the string within the management application.

BSN_AUTHENTICATION_FAILURE

MIB Name	bsnAuthenticationFailure.
Alarm Condition	Client authentication failure.
NCS Message	Switch "{0}." User authentication from Switch "{0}" failed for user name "{1}" and user type "{2}."
Symptoms	A user authentication failure is reported for a local management user or a MAC filter is configured on the controller.
Severity	Minor.
Category	Clients
Probable Causes	Incorrect login attempt by an admin user from the controller CLI or controller GUI, or a client accessing the WLAN system.
Recommended Actions	If the user has forgotten the password, the superuser may need to reset it.

IPSEC_IKE_NEG_FAILURE

MIB Name	bsnIpsecIkeNegFailure.
Alarm Condition	IPsec IKE negotiation failure.
NCS Message	IPsec IKE Negotiation failure from remote IP address "{0}."
Symptoms	Unable to establish an IPsec tunnel between a client and a WLAN appliance.
Severity	Minor.
Category	Security
Probable Causes	Configuration mismatch.
Recommended Actions	Validate configuration, verify that authentication credentials match (preshared keys or certificates); and verify that encryption algorithms and strengths match.

IPSEC_INVALID_COOKIE

MIB Name	bsnIpsecInvalidCookieTrap.
Alarm Condition	IPsec invalid cookie.
NCS Message	IPsec Invalid cookie from remote IP address "{0}."
Symptoms	Cannot successfully negotiate an IPsec session.
Severity	Minor.
Category	Security
Probable Causes	Synchronization problem. The client believes a tunnel exists while the WLAN appliance does not. This problem often happens when the IPsec client does not detect a disassociation event.
Recommended Actions	Reset the IPsec client and then restart tunnel establishment.

LINK_DOWN (FROM MIB-II STANDARD)

MIB Name	linkDown.
Alarm Condition	Interface state change.
NCS Message	Port "{0}" is down on Switch "{1}."
Symptoms	The physical link on one of the switch (controller) ports is down.
Severity	Critical.
Category	Controller.
Probable Causes	• An access point or a port was manually disconnected from the network. • A port failure.
Recommended Actions	Troubleshoot physical network connectivity to the affected port.

LINK_UP (FROM MIB-II STANDARD)

MIB Name	linkUp.
Alarm Condition	Interface state change.
NCS Message	Port "{0}" is up on Switch "{1}."
Symptoms	The physical link is up on a switch (controller) port.
Severity	Clear.
Category	Controller.
Probable Causes	A physical link to the switch (controller) is restored.
Recommended Actions	None.

LRAD_ASSOCIATED

MIB Name	bsnAPAssociated.
Alarm Condition	AP associated with controller.
NCS Message	AP "{0}" associated with Switch "{2}" on Port number "{1}."

Symptoms	An access point has associated with a switch (controller).
Severity	Clear.
Category	Access Point.
Probable Causes	• A new access point has joined the network. • An access point has associated with a standby switch (controller) due to a failover. • An access point rebooted and reassociated with a switch (controller).
Recommended Actions	Power recycled; Software reset.

LRAD_DISASSOCIATED

MIB Name	bsnAPDisassociated.
Alarm Condition	AP disassociated from controller.
NCS Message	AP "{0}" disassociated from Switch "{1}."
Symptoms	The switch (controller) is no longer detecting an access point.
Severity	Critical.
Category	Access Point.
Probable Causes	• A failure in the access point. • An access point is no longer on the network.
Recommended Actions	Check if the access point is powered up and has network connectivity to the switch (controller).

LRADIF_COVERAGE_PROFILE_PASSED

MIB Name	bsnAPCoverageProfileUpdatedToPass.
Alarm Condition	Radio coverage threshold violation.
NCS Message	AP "{0},” interface "{1}." Coverage changed to acceptable.
Symptoms	A radio interface that was reporting coverage profile failure has reverted to an acceptable level.
Severity	Informational.
Category	Performance
Probable Causes	The number of clients on this radio interface with suboptimal performance has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_CURRENT_CHANNEL_CHANGED

MIB Name	bsnAPCurrentChannelChanged.
Alarm Condition	Radio current channel changed.
NCS Message	AP "{0},” interface "{1}." Channel changed to "{2}." Interference Energy before update was "{3}" and after update is "{4}."
Symptoms	The current channel assigned to a radio interface has automatically changed.
Severity	Informational.
Category	Access Point.
Probable Causes	Possible interference on a channel has caused the radio management software on the controller to change the channel.
Recommended Actions	None.

LRADIF_CURRENT_TXPOWER_CHANGED

MIB Name	bsnAPCurrentTxPowerChanged.
Alarm Condition	Radio transmit power level changed
NCS Message	AP "{0},” interface "{1}." Transmit Power Level changed to "{2}."
Symptoms	The power level has automatically changed on a radio interface.
Severity	Informational.
Category	Access Point.
Probable Causes	The radio management software on the controller has modified the power level for optimal performance.
Recommended Actions	None.

LRADIF_DOWN

MIB Name	bsnAPIfDown.
Alarm Condition	Radio administratively up and operationally down.
NCS Message	AP "{0},” interface "{1}" is down.
Symptoms	A radio interface is out of service.
Severity	Critical if not disabled, otherwise Informational.
Category	Access Point.
Probable Causes	• A radio interface has failed. • An administrator has disabled a radio interface. • An access point has failed and is no longer detected by the controller.
Recommended Actions	If the access point is not administratively disabled, call customer support.

LRADIF_INTERFERENCE_PROFILE_FAILED

MIB Name	bsnAPInterferenceProfileFailed.
Alarm Condition	Radio interference threshold violation.
NCS Message	AP "{0}," interface "{1}." Interference threshold violated.
Symptoms	The interference detected on one or more channels is violated.
Severity	Minor.
Category	SE Detected Interferers
Probable Causes	There are other 802.11 devices in the same band that are causing interference on channels used by this system.
Recommended Actions	• If the interference threshold is configured to be too low, you may need to readjust it to a more optimum value. • Investigate interference sources such as other 802.11 devices in the vicinity of this radio interface. A possible workaround is adding one or more access points to distribute the current load or slightly increasing the threshold of the access point which is displaying this message. To perform this workaround, follow the steps below: 1. Choose **Configure > Controllers**. 2. Click any IP address in that column of the All Controllers page. 3. From the left sidebar menu, choose **802.11a/n** or **802.11b/g/n** and then **RRM Thresholds**. 4. Adjust the Interference Threshold (%) in the Other Thresholds section.

LRADIF_INTERFERENCE_PROFILE_PASSED

MIB Name	bsnAPInterferenceProfileUpdatedToPass.
Alarm Condition	Radio interference threshold violation.
NCS Message	AP "{0}," interface "{1}." Interference changed to acceptable.
Symptoms	A radio interface reporting interference profile failure has reverted to an acceptable level.
Severity	Clear.
Category	Access Point.
Probable Causes	The interference on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_LOAD_PROFILE_FAILED

MIB Name	bsnAPLoadProfileFailed.
Alarm Condition	Radio load threshold violation.
NCS Message	AP "{0},” interface "{1}." Load threshold violated.
Symptoms	A radio interface of an access point is reporting that the client load has crossed a configured threshold.
Severity	Minor.
Category	Access Point.
Probable Causes	There are too many clients associated with this radio interface.
Recommended Actions	• Verify the client count on this radio interface. If the threshold for this trap is too low, you may need to readjust it. • Add new capacity to the physical location if the client count is a frequent issue on this radio.

LRADIF_LOAD_PROFILE_PASSED

MIB Name	bsnAPLoadProfileUpdatedToPass.
Alarm Condition	Radio load threshold violation.
NCS Message	AP "{0}," interface "{1}." Load changed to acceptable.
Symptoms	A radio interface that was reporting load profile failure has reverted to an acceptable level.
Severity	Clear.
Category	Access Point.
Probable Causes	The load on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_NOISE_PROFILE_FAILED

MIB Name	bsnAPNoiseProfileFailed.
Alarm Condition	Radio noise threshold violation.
NCS Message	AP "{0}," interface "{1}." Noise threshold violated.
Symptoms	The monitored noise level on this radio has crossed the configured threshold.
Severity	Minor.
Category	Access Point.
Probable Causes	Noise sources that adversely affect the frequencies on which the radio interface operates.
Recommended Actions	• If the noise threshold is too low, you may need to readjust it to a more optimal value. • Investigate noise sources in the vicinity of the radio interface (for example, a microwave oven).

LRADIF_NOISE_PROFILE_PASSED

MIB Name	bsnAPNoiseProfileUpdatedToPass.
Alarm Condition	Radio noise threshold violation..
NCS Message	AP "{0}," interface "{1}." Noise changed to acceptable.
Symptoms	A radio interface that was reporting noise profile failure has reverted to an acceptable level.
Severity	Clear.
Category	Access Point.
Probable Causes	The noise on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_UP

MIB Name	bsnAPIfUp.
Alarm Condition	Radio administratively up and operationally down.
NCS Message	AP "{0}," interface "{1}" is up.
Symptoms	A radio interface is back up.
Severity	Clear.
Category	Access Point.
Probable Causes	• An administrator has enabled a radio interface. • An access point has turned on. • A new access point has joined the network.
Recommended Actions	None.

MAX_ROGUE_COUNT_CLEAR

MIB Name	bsnMaxRogueCountClear.
Alarm Condition	AP maximum rogue count cleared.
NCS Message	Fake AP or other attack is cleared now. Rogue AP count on system "{0}" is within the threshold of "{1}."
Symptoms	The number of rogues detected by a controller is within acceptable limits.
Severity	Clear.
Category	Rogue APs
Probable Causes	N/A.
Recommended Actions	None.

MAX_ROGUE_COUNT_EXCEEDED

MIB Name	bsnMaxRogueCountExceeded.
Alarm Condition	Maximum rogue count exceeded.
NCS Message	Fake AP or other attack may be in progress. Rogue AP count on system "{0}" has exceeded the severity warning threshold of "{1}."
Symptoms	The number of rogues detected by a controller exceeds the internal threshold.
Severity	Critical.
Category	Security
Probable Causes	• There are too many rogue access points in the network. • A fake access point attack is in progress.
Recommended Actions	Identify the source of the rogue access points.

MULTIPLE_USERS

MIB Name	multipleUsersTrap.
Alarm Condition	Multiple users.
NCS Message	Switch "{0}." Multiple users logged in.
Symptoms	Multiple users with the same login ID are logged in through the CLI.
Severity	Informational.
Category	Controller
Probable Causes	The same user has logged in multiple times through the CLI interface.
Recommended Actions	Verify that the expected login sessions for the same user are valid.

NETWORK_DISABLED

MIB Name	bsnNetworkStateChanged (bsnNetworkState set to disabled).
Alarm Condition	Network disabled
NCS Message	Global "{1}" network status disabled on Switch with IP Address "{0}."
Symptoms	An administrator has disabled the global network for 802.11a/n and 802.11b/g/n.
Severity	Informational.
Category	Controller
Probable Causes	Administrative command.
Recommended Actions	None.

NO_ACTIVITY_FOR_ROGUE_AP

MIB Name	This is a NCS-only event generated when no rogue activity is seen for a specific duration.
Alarm Condition	No activity for Rogue AP.
NCS Message	Rogue AP "{0}" is cleared explicitly. It is not detected anymore.
Symptoms	A rogue access point is cleared from the management system due to inactivity.
Severity	Informational.
Category	Rogue APs
Probable Causes	A rogue access point is not located on any managed controller for a specified duration.
Recommended Actions	None.

POE_CONTROLLER_FAILURE

MIB Name	bsnPOEControllerFailure.
Alarm Condition	PoE Controller Failure.
NCS Message	The POE controller has failed on the Switch "{0}."
Symptom	A failure in the Power Over Ethernet (POE) unit is detected.
Severity	Critical.
Category	Controller
Probable Causes	The power of the Ethernet unit has failed.
Recommended Actions	Call customer support. The unit may need to be repaired.

RADIO_ADMIN_UP_OPER_DOWN

MIB Name	bsnAPRadioCardRxFailure
Alarm Condition	Radio administratively up and operationally down
NCS Message	{1} interface of AP {0} is down: Controller {2}
Symptom	None.
Severity	Critical
Category	Access Point
Probable Causes	None.
Recommended Actions	None.

RADIOS_EXCEEDED

MIB Name	bsnRadiosExceedLicenseCount.
Alarm Condition	Radios exceeded.
NCS Message	The Radios associated with Switch "{0}" exceeded license count "{1}." The current number of radios on this switch is "{2}."
Symptoms	The number of supported radios for a switch (controller) has exceeded the licensing limit.
Severity	Major.
Category	Controller
Probable Causes	The number of access points associated with the switch (controller) has exceeded the licensing limits.
Recommended Actions	Upgrade the license for the switch (controller) to support a higher number of access points.

RADIUS_SERVERS_FAILED

MIB Name	bsnRADIUSServerNotResponding.
Alarm Condition	RADIUS servers failure.
NCS Message	Switch "{0}." RADIUS server(s) are not responding to authentication requests.
Symptoms	The switch (controller) is unable to reach any RADIUS server for authentication.
Severity	Critical.
Category	Controller
Probable Causes	Network connectivity to the RADIUS server is lost or the RADIUS server is down.
Recommended Actions	Verify the status of all configured RADIUS servers and their network connectivity.

ROGUE_ADHOC_DETECTED

MIB Name	bsnRogueAPDetected.
Alarm Condition	Adhoc Rogue detected.
NCS Message	Rogue Adhoc "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Symptoms	A rogue adhoc was detected by the system.
Severity	Minor if not on wired network, critical if on wired network.
Category	Adhoc Rogue.
Probable Causes	• An illegal access point or adhoc has been connected to the network • A known internal or external adhoc unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the adhoc point by tracing it through the MAC address/SSID or by using location features to locate it physically. • "If adhoc is a known internal or external or adhoc, acknowledge it or mark it as a known or adhoc. Consider adding it to the known access point template within WCS. • If the adhoc is deemed to be a security threat, the rogue can be contained using the management interface.

ROGUE_ADHOC_ON_NETWORK

MIB Name	bsnRogueAPDetectedOnWiredNetwork
Alarm Condition	None.
NCS Message	Rogue ADHOC "{0}" is on wired network.
Symptoms	A rogue adhoc is found to be reachable through the wired network
Severity	Critical
Category	Switch
Probable Causes	• An illegal adhoc was detected to be reachable through the wired network. As a result its severity is escalated to critical
Recommended Actions	• "Determine if this is a known or valid adhoc in the system. If so, place it in the known adhoc list. • "Contain the rogue using the system to prevent anyone from accessing it until the adhoc has been traced down using location or other features.

ROGUE_AP_DETECTED

MIB Name	bsnRogueAPDetected.
Alarm Condition	ROGUE_AP_DETECTED

NCS Message	Rogue AP or ad hoc rogue "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}."
Symptoms	The system has detected a rogue access point.
Severity	Minor if not on a wired network; Critical if on a wired network.
Category	Rogue APs
Probable Causes	• An illegal access point is connected to the network. • A known internal or external access point unknown to this system is detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it using its MAC address or the SSID, or by using location features to locate it physically. • If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within NCS. • If the access point is deemed to be a severity threat, contain it using the management interface.

ROGUE_AP_ON_NETWORK

MIB Name	bsnRogueAPDetectedOnWiredNetwork
Alarm Condition	ROGUE_AP_ON_NETWORK
NCS Message	Rogue AP or ad hoc rogue "{0}" is on the wired network.
Symptoms	A rogue access point is found reachable through the wired network.
Severity	Critical.
Category	Rogue AP
Probable Causes	An illegal access point was detected as reachable through the wired network.
Recommended Actions	• Determine if this is a known or valid access point in the system. If it is valid, place it in the known access point list. • Contain the rogue. Prevent anyone from accessing it until the access point has been traced down using location or other features.

ROGUE_AP_REMOVED

MIB Name	bsnRogueAPRemoved.
Alarm Condition	ROGUE_AP_REMOVED
NCS Message	Rogue AP or ad hoc rogue "{0}" is removed; it was detected as Rogue AP by AP "{1}" Radio type "{2}."
Symptoms	The system is no longer detecting a rogue access point.
Severity	Clear
Category	Rogue APs

Probable Causes	A rogue access point has powered off or moved away and therefore the system no longer detects it.
Recommended Actions	None.

RRM_DOT11_A_GROUPING_DONE

MIB Name	bsnRrmDot11aGroupingDone.
Alarm Condition	RRM
NCS Message	RRM 802.11a/n grouping done; the new group leader's MAC address is "{0}."
Symptoms	The radio resource module is finished grouping for the A band, and a new group leader is chosen.
Severity	Informational.
Category	RRM
Probable Causes	The older RRM group leader may have gone down.
Recommended Actions	None.

RRM_DOT11_B_GROUPING_DONE

MIB Name	bsnRrmDot11bGroupingDone.
Alarm Condition	RRM
NCS Message	RRM 802.11b/g/n grouping done; the new group leader's MAC address is "{0}."
Symptoms	The radio resource module finished its grouping for the B band and chose a new group leader.
Severity	Informational.
Category	RRM
Probable Causes	The older RRM group leader may have gone down.
Recommended Actions	None.

SENSED_TEMPERATURE_HIGH

MIB Name	bsnSensedTemperatureTooHigh.
Alarm Condition	Sensed temperature high.
NCS Message	The sensed temperature on the Switch "{0}" is too high. The current sensed temperature is "{1}."
Symptoms	The system's internal temperature has crossed the configured thresholds.
Severity	Major.
Category	Controller

Probable Causes	• Fan failure. • Fault in the device.
Recommended Actions	• Verify the configured thresholds and increase the value if it is too low. • Call customer support.

SENSED_TEMPERATURE_LOW

MIB Name	bsnSensedTemperatureTooLow.
Alarm Condition	Sensed temperature low.
NCS Message	The sensed temperature on the Switch "{0}" is too low. The current sensed temperature is "{1}."
Symptoms	The internal temperature of the device is below the configured limit in the system.
Severity	Major.
Category	Controller
Probable Causes	• Operating environment. • Hardware fault.
Recommended Actions	• Verify the configured thresholds and ensure that the limit is appropriate. • Call customer support.

STATION_ASSOCIATE

MIB Name	bsnDot11StationAssociate.
Alarm Condition	Client associated to AP.
NCS Message	Client "{0}" is associated with AP "{1}," interface "{2}."
Symptoms	A client has associated with an access point.
Severity	Informational.
Category	Clients
Probable Causes	A client has associated with an access point.
Recommended Actions	None.

STATION_ASSOCIATE_FAIL

MIB Name	bsnDot11StationAssociateFail.
Alarm Condition	Client associated failure with AP.
NCS Message	Client "{0}" failed to associate with AP "{1}," interface "{2}." The reason code is "{3}."
Symptoms	A client station failed to associate with the system.
Severity	Informational.
Category	Clients

Probable Causes	The access point was busy.
Recommended Actions	Check whether the access point is busy and reporting load profile failures.

STATION_AUTHENTICATE

MIB Name	bsnDot11StationAssociate (bsnStationUserName is set).
Alarm Condition	Client authenticated.
NCS Message	Client "{0}" with user name "{3}" is authenticated with AP "{1}," interface "{2}."
Symptoms	A client has successfully authenticated with the system.
Severity	Informational.
Category	Clients
Probable Causes	A client has successfully authenticated with the system.
Recommended Actions	None.

STATION_AUTHENTICATION_FAIL

MIB Name	bsnDot11StationAuthenticateFail.
Alarm Condition	Client authentication failure.
NCS Message	Client "{0}" has failed authenticating with AP "{1}," interface "{2}." The reason code is "{3}."
Symptoms	The system failed to authenticate a client.
Severity	Informational.
Category	Clients
Probable Causes	Failed client authentication.
Recommended Actions	Check client configuration and configured keys or passwords in the system.

STATION_BLACKLISTED

MIB Name	bsnDot11StationBlacklisted.
Alarm Condition	Client excluded.
NCS Message	Client "{0}" which was associated with AP "{1}," interface "{2}" is excluded. The reason code is "{3}."
Symptoms	A client is in the exclusion list and is not allowed to authenticate for a configured interval.
Severity	Minor.
Category	Security

Probable Causes	• Repeated authentication or association failures from the client station. • A client is attempting to use an IP address assigned to another device.
Recommended Actions	• Verify the configuration or the client along with its credentials. • Remove the client from the exclusion list by using the management interface if the client needs to be allowed back into the network.

STATION_DEAUTHENTICATE

MIB Name	bsnDot11StationDeauthenticate.
Alarm Condition	Client deauthenticated from AP.
NCS Message	Client "{0}" is deauthenticated from AP "{1}," interface "{2}" with reason code "{3}."
Symptoms	A client is no longer authenticated by the system.
Severity	Informational.
Category	Clients
Probable Causes	A client is no longer authenticated by the system.
Recommended Actions	None.

STATION_DISASSOCIATE

MIB Name	bsnDot11StationDisassociate.
Alarm Condition	Client disassociated from AP.
NCS Message	Client "{0}" is disassociated from AP "{1}," interface "{2}" with reason code "{3}."
Symptoms	A client has disassociated with an access point in the system.
Severity	Informational.
Category	Clients
Probable Causes	A station may disassociate due to various reasons such as inactivity timeout or a forced action from the management interface.
Recommended Actions	None.

STATION_WEP_KEY_DECRYPT_ERROR

MIB Name	bsnWepKeyDecryptError.
Alarm Condition	Client WEP key decryption error.
NCS Message	The WEP Key configured at the station may be wrong. Station MAC Address is "{0}," AP MAC is "{1}" and Slot ID is "{2}."
Symptoms	A client station seems to have the wrong WEP key.
Severity	Minor.
Category	Security

Probable Causes	A client has an incorrectly configured WEP key.
Recommended Actions	Identify the client and correct the WEP key configuration.

STATION_WPA_MIC_ERROR_COUNTER_ACTIVATED

MIB Name	bsnWpaMicErrorCounterActivated.
Alarm Condition	Client WPA MIC error counter activated.
NCS Message	The AP "{1}" received a WPA MIC error on protocol "{2}" from Station "{0}." Counter measures have been activated and traffic has been suspended for 60 seconds.
Symptoms	A client station has detected a WPA MIC error.
Severity	Critical.
Category	Security
Probable Causes	A possible hacking attempt is underway.
Recommended Actions	Identify the station that is the source of this threat.

SWITCH_DETECTED_DUPLICATE_IP

MIB Name	bsnDuplicateIpAddressReported.
Alarm Condition	Controller Detected Duplicate IP.
NCS Message	Switch "{0}" detected duplicate IP address "{0}" being used by machine with mac address "{1}."
Symptoms	The system has detected a duplicate IP address in the network that is assigned to the switch (controller).
Severity	Critical.
Category	Security
Probable Causes	Another device in the network is configured with the same IP address as that of the switch (controller).
Recommended Actions	Correct the misconfiguration of IP addresses in the network.

SWITCH_UP

MIB Name	This is a NCS-only event.
Alarm Condition	Controller up.
NCS Message	Switch "{0}" is reachable.
Symptoms	A switch (controller) is now reachable from the management station.
Severity	Clear.
Category	Switch
Probable Causes	A switch (controller) is reachable from the management station.
Recommended Actions	None.

TEMPERATURE_SENSOR_CLEAR

MIB Name	bsnTemperatureSensorClear.
Alarm Condition	Temperature sensure clear
NCS Message	The temperature sensor is working now on the switch "{0}." The sensed temperature is "{1}."
Symptoms	The temperature sensor is operational.
Severity	Clear.
Category	Controller
Probable Causes	The system is detecting the temperature sensor to be operational now.
Recommended Actions	None.

TEMPERATURE_SENSOR_FAILURE

MIB Name	bsnTemperatureSensorFailure.
Alarm Condition	Temperature sensor failure
NCS Message	The temperature sensor failed on the Switch "{0}." Temperature is unknown.
Symptoms	The system is reporting that a temperature sensor has failed and the system is unable to report accurate temperature.
Severity	Major.
Category	Controller
Probable Causes	The temperature sensor has failed due to hardware failure.
Recommended Actions	Call customer support.

TOO_MANY_USER_UNSUCCESSFUL_LOGINS

MIB Name	bsnTooManyUnsuccessLoginAttempts.
Alarm Condition	Too many user unsuccessful logins.
NCS Message	User "{1}" with IP Address "{0}" has made too many unsuccessful login attempts.
Symptoms	A management user has made too many login attempts.
Severity	Critical.
Category	Security
Probable Causes	• An admin user has made too many login attempts. • A user attempted to break into the administration account of the management system.
Recommended Actions	• Identify the source of the login attempts and take the appropriate action. • Increase the value of the login attempt threshold if it is too low.

Traps Added in Release 2.1

The following traps were added for WCS Release 2.1:

ADHOC_ROGUE_AUTO_CONTAINED

MIB Name	bsnAdhocRogueAutoContained.
Alarm Condition	Adhoc Rogue auto contained.
NCS Message	Adhoc Rogue "{0}" was found and is auto contained as per WPS policy.
Symptoms	The system detected an ad hoc rogue and automatically contained it.
Severity	Major.
Category	Security
Probable Causes	The system detected an ad hoc rogue and automatically contained it as configured in the system's wireless prevention policy.
Recommended Actions	Identify the ad hoc rogue through the location application and take the appropriate action.

ADHOC_ROGUE_AUTO_CONTAINED_CLEAR

MIB Name	bsnAdhocRogueAutoContained (bsnClearTrapVariable set to true).
Alarm Condition	Adhoc Rogue auto contained cleared.
NCS Message	Adhoc Rogue "{0}" was found and was auto contained. The alert state is clear now.
Symptoms	An ad hoc rogue that the system has detected earlier is now clear.
Severity	Clear.
Category	Security
Probable Causes	The system no longer detects an ad hoc rogue.
Recommended Actions	None.

NETWORK_ENABLED

MIB Name	bsnNetworkStateChanged (bsnNetworkState set to enabled).
Alarm Condition	Network enabled.
NCS Message	Global "{1}" network status enabled on Switch with IP Address "{0}."
Symptoms	An administrator has enabled the global network for 802.11a/n or 802.11b/g/n.
Severity	Informational.
Category	Controller
Probable Causes	Administrative command.
Recommended Actions	None.

ROGUE_AP_AUTO_CONTAINED

MIB Name	bsnRogueApAutoContained.
Alarm Condition	Rogue AP auto contained.
NCS Message	Rogue AP "{0}" is advertising our SSID and is auto contained as per WPS policy.
Symptoms	The system has automatically contained a rogue access point.
Severity	Major.
Category	Rogue APs
Probable Causes	The system detected an ad hoc rogue and automatically contained it as configured in the system's wireless prevention policy.
Recommended Actions	• Track the location of the rogue and take the appropriate action. • If this is a known valid access point, clear the rogue from containment.

ROGUE_AP_AUTO_CONTAINED_CLEAR

MIB Name	bsnRogueApAutoContained (bsnClearTrapVariable set to true).
Alarm Condition	Rogue AP cleared.
NCS Message	Rogue AP "{0}" was advertising our SSID and was auto contained. The alert state is clear now.
Symptoms	The system has cleared a previously contained rogue.
Severity	Clear.
Category	Rogue APs
Probable Causes	The system has cleared a previously contained rogue.
Recommended Actions	None.

TRUSTED_AP_INVALID_ENCRYPTION

MIB Name	bsnTrustedApHasInvalidEncryption.
Alarm Condition	Trusted AP with invalid encryption.
NCS Message	Trusted AP "{0}" is invalid encryption. It is using "{1}" instead of "{2}." It is auto contained as per WPS policy.
Symptoms	The system automatically contained a trusted access point that has invalid encryption.
Severity	Major.
Category	Security
Probable Causes	The system automatically contained a trusted access point that violated the configured encryption policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_ENCRYPTION_CLEAR

MIB Name	bsnTrustedApHasInvalidEncryption (bsnClearTrapVariable set to true).
Alarm Condition	Trusted AP with invalid encryption cleared.
NCS Message	Trusted AP "{0}" had invalid encryption. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
Severity	Clear.
Category	Security
Probable Causes	The trusted access point has now conformed to the configured encryption policy.
Recommended Actions	None.

TRUSTED_AP_INVALID_RADIO_POLICY

MIB Name	bsnTrustedApHasInvalidRadioPolicy.
Alarm Condition	Trusted AP with invalid radio policy.
NCS Message	Trusted AP "{0}" has invalid radio policy. It is using "{1}" instead of "{2}." It has been auto contained as per WPS policy.
Symptoms	The system has contained a trusted access point with an invalid radio policy.
Severity	Major.
Category	Security
Probable Causes	The system has contained a trusted access point connected to the wireless system for violating the configured radio policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_RADIO_POLICY_CLEAR

MIB Name	bsnTrustedApHasInvalidRadioPolicy (bsnClearTrapVariable set to true).
Alarm Condition	Trusted AP with invalid radio policy cleared.
NCS Message	Trusted AP "{0}" had invalid radio policy. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
Severity	Clear.
Category	Security
Probable Causes	The trusted access point has now conformed to the configured encryption policy.
Recommended Actions	None.

TRUSTED_AP_INVALID_SSID

MIB Name	bsnTrustedApHasInvalidSsid.
Alarm Condition	Trusted AP with invalid SSID

NCS Message	Trusted AP "{0}" has invalid SSID. It was auto contained as per WPS policy.
Symptoms	The system has automatically contained a trusted access point for advertising an invalid SSID.
Severity	Major.
Category	Security
Probable Causes	The system has automatically contained a trusted access point for violating the configured SSID policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_SSID_CLEAR

MIB Name	bsnTrustedApHasInvalidSsid (bsnClearTrapVariable set to true).
Alarm Condition	Trusted AP with invalid SSID clear.
NCS Message	Trusted AP "{0}" had invalid SSID. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
Severity	Clear.
Category	Security
Probable Causes	The trusted access point has now conformed to the configured policy.
Recommended Actions	None.

TRUSTED_AP_MISSING

MIB Name	bsnTrustedApIsMissing.
Alarm Condition	Trusted AP missing.
NCS Message	Trusted AP "{0}" is missing or has failed.
Symptoms	The wireless system no longer detects a trusted access point.
Severity	Major.
Category	Security
Probable Causes	A trusted access point has left the network or has failed.
Recommended Actions	Track down the trusted access point and take the appropriate action.

TRUSTED_AP_MISSING_CLEAR

MIB Name	bsnTrustedApIsMissing (bsnClearTrapVariable set to true).
Alarm Condition	Trusted AP missing clear.
NCS Message	Trusted AP "{0}" is missing or has failed. The alert state is clear now.
Symptoms	The system has found a trusted access point again.
Severity	Clear.
Category	Security

Probable Causes	The system has detected a previously missing trusted access point.
Recommended Actions	None.

Traps Added in Release 2.2

The following traps were added in WCS Release 2.2:

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
Alarm Condition	AP impersonation detected.
NCS Message	AP Impersonation with MAC "{0}" is detected by authenticated AP "{1}" on "{2}" radio and Slot ID "{3}."
Symptoms	A radio of an authenticated access point has heard from another access point whose MAC address neither matches that of a rogue nor is it an authenticated neighbor of the detecting access point.
Severity	Critical.
Category	Security
Probable Causes	A severity breach related to access point impersonation may be under way.
Recommended Actions	Track down the MAC address of the impersonating access point in the network and contain it.

AP_RADIO_CARD_RX_FAILURE

MIB Name	bsnAPRadioCardRxFailure.
Alarm Condition	AP impersonation detected.
NCS Message	Receiver failure detected on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio card is unable to receive data.
Severity	Critical.
Category	Security

Probable Causes	• A radio card is experiencing reception failure. • The antenna of the radio is disconnected.
Recommended Actions	• Check the access point's antenna connection. • Call customer support.

AP_RADIO_CARD_RX_FAILURE_CLEAR

MIB Name	bsnAPRadioCardRxFailureClear.
Alarm Condition	Radiocard failure clear.
NCS Message	Receiver failure cleared on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio is no longer experiencing reception failure.
Severity	Clear.
Category	Access Point.
Probable Causes	A malfunction in the access point has been corrected.
Recommended Actions	None.

AP_RADIO_CARD_TX_FAILURE

MIB Name	bsnAPRadioCardTxFailure.
Alarm Condition	Radiocard failure.
NCS Message	Transmitter failure detected on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio card is unable to transmit.
Severity	Critical.
Category	Access Point.
Probable Causes	• A radio card is experiencing transmission failure. • The antenna of the radio may be disconnected.
Recommended Actions	• Check the antenna of the access point. • Call customer support.

AP_RADIO_CARD_TX_FAILURE_CLEAR

MIB Name	bsnAPRadioCardTxFailureClear.
Alarm Condition	NA
NCS Message	Transmitter failure cleared on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio is no longer experiencing transmission failure.
Severity	Clear.
Category	Access Point.
Probable Causes	A malfunction in the access point has been corrected.
Recommended Actions	None.

SIGNATURE_ATTACK_CLEARED

MIB Name	bsnSignatureAttackDetected (bsnClearTrapVariable is set to True).
Alarm Condition	Signature attack cleared.
NCS Message	Switch "{0}" is cleared from IDS signature attack. The wireless system is no longer detecting the intrusion.
Symptoms	The switch (controller) no longer detects a signature attack.
Severity	Clear.
Category	Security
Probable Causes	The signature attack that the system previously detected has stopped.
Recommended Actions	None.

SIGNATURE_ATTACK_DETECTED

MIB Name	bsnSignatureAttackDetected
Alarm Condition	Signature attack detected
NCS Message	IDS Signature attack detected on Switch "{0}." The Signature Type is "{1}," Signature Name is "{2}," and Signature description is "{3}."
Symptoms	The switch (controller) is detecting a signature attack. The switch (controller) has a list of signatures that it monitors. When it detects a signature, it provides the name of the signature attack in the alert it generates.
Severity	Critical.
Category	Security
Probable Causes	Someone is mounting a malevolent signature attack.
Recommended Actions	Track down the source of the signature attack in the wireless network and take the appropriate action.

TRUSTED_AP_INVALID_PREAMBLE

MIB Name	bsnTrustedApHasInvalidPreamble.
Alarm Condition	Trusted AP with invalid preamble.
NCS Message	Trusted AP "{0}" on Switch "{3}" has invalid preamble. It is using "{1}" instead of "{2}." It has been auto contained as per WPS policy.
Symptoms	The system has contained a trusted rogue access point for using an invalid preamble.
Severity	Major.
Category	Security
Probable Causes	The system has detected a possible severity breach because a rogue is transmitting an invalid preamble.
Recommended Actions	Locate the rogue access point using location features or the access point detecting it and take the appropriate actions.

TRUSTED_AP_INVALID_PREAMBLE_CLEARED

MIB Name	bsnTrustedApHasInvalidPreamble (bsnClearTrapVariable is set to true).
Alarm Condition	Trusted AP with invalid preamble cleared.
NCS Message	Trusted AP "{0}" on Switch "{3}" had invalid preamble. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
Severity	Clear.
Category	Security
Probable Causes	The system has cleared a previous alert about a trusted access point.
Recommended Actions	None.

Traps Added in Release 3.0

The following traps were added in WCS Release 3.0:

- AP_FUNCTIONALITY_DISABLED, page 13-33
- AP_IP_ADDRESS_FALLBACK, page 13-33
- AP_REGULATORY_DOMAIN_MISMATCH, page 13-34
- RX_MULTICAST_QUEUE_FULL, page 13-34

AP_FUNCTIONALITY_DISABLED

MIB Name	bsnAPFunctionalityDisabled.
Alarm Condition	AP functionality disabled.
NCS Message	AP functionality has been disabled for key "{0}," reason being "{1}" for feature-set "{2}."
Symptoms	The system sends this trap out when the controller disables access point functionality because the license key has expired.
Severity	Critical.
Category	Controller
Probable Causes	When the controller boots up, it checks whether the feature license key matches the controller's software image. If it does not, the controller disables access point functionality.
Recommended Actions	Configure the correct license key on the controller and reboot it to restore access point functionality.

AP_IP_ADDRESS_FALLBACK

MIB Name	bsnAPIPAddressFallback.
Alarm Condition	AP IP fallback.
NCS Message	AP "{0}" with static-ip configured as "{2}" has fallen back to the working DHCP address "{1}."
Symptoms	This trap is sent out when an access point, with the configured static ip-address, fails to establish connection with the outside world and starts using DHCP as a fallback option.
Severity	Minor.
Category	Access Point.
Probable Causes	If the configured IP address on the access point is incorrect or obsolete, and if the AP Fallback option is enabled on the switch (controller), the access point starts using DHCP.
Recommended Actions	Reconfigure the access point's static IP to the correct IP address if desired.

AP_REGULATORY_DOMAIN_MISMATCH

MIB Name	bsnAPRegulatoryDomainMismatch.
Alarm Condition	AP regulatory domain mismatch.
NCS Message	AP "{1}" is unable to associate. The Regulatory Domain configured on it "{3}" does not match the Controller "{0}" country code "{2}."
Symptoms	The system generates this trap when an access point's regulatory domain does not match the country code configured on the controller. Due to the country code mismatch, the access point will fail to associate with the controller.
Severity	Critical.
Category	Access Point.
Probable Causes	• If someone changes the controller's country code configuration and some of the existing access points support a different country code, these access points fail to associate. • An access point on the controller's network sends join requests to the controller, but the regulatory domain is outside the domain in which the controller is operating.
Recommended Actions	Either remove the access points that are not meant for inclusion in the controller's domain or correct the controller's country code setting.

RX_MULTICAST_QUEUE_FULL

MIB Name	bsnRxMulticastQueueFull.
Alarm Condition	CPU RX Multicast queue full.
NCS Message	CPU Receive Multicast Queue is full on Controller "{0}."
Symptoms	This trap indicates that the CPU's Receive Multicast queue is full.
Severity	Critical.
Category	Controller
Probable Causes	An ARP storm.
Recommended Actions	None.

Traps Added in Release 3.1

The following traps were added in WCS Release 3.1:

AP_AUTHORIZATION_FAILURE

MIB Name	bsnAPAuthorizationFailure
Alarm Condition	AP Authorization Failure.
NCS Message	• Failed to authorize AP “{0}." Authorization entry does not exist in Controllers “{1}” AP Authorization List. • Failed to authorize AP “{0}." AP’s authorization key does not match with SHA1 key in Controllers “{1}” AP Authorization List. • Failed to authorize AP “{0}." Controller “{1}” could not verify the Self Signed Certificate from the AP. • Failed to authorize AP “{0}." AP has a self signed certificate where as the Controllers “{1}” AP authorization list has Manufactured Installed Certificate for this AP.
Symptoms	An alert is generated when an access point fails to associate with a controller due to authorization issues.
Severity	Critical.
Category	Access Point.

Probable Causes	• The access point is not on the controller's access point authorization list. • The key entry in the controller's access point authorization list does not match the SHA1 key received from the access point. • The access point self-signed certificate is not valid. • The access point has a self-signed certificate and the controller's access point authorization list (for the given access point) references a manufactured installed certificate.
Recommended Actions	• Add the access point to the controller's authorization list. • Update the access point's authorization key to match the controller's access point key. • Check the accuracy of the access point's self-signed certificate. • Check the certificate type of the access point in the controller's access point authorization list.

HEARTBEAT_LOSS_TRAP

MIB Name	heartbeatLossTrap.
Alarm Condition	Heart beat loss.
NCS Message	Keepalive messages are lost between Master and Controller"{0}."
Symptoms	This trap is generated when the controller loses connection with the Supervisor Switch (in which it is physically embedded) and the controller cannot hear the heartbeat (keepalives) from the Supervisor.
Severity	Major.
Category	Controller
Probable Causes	• Port on the WiSM controller could be down. • Loss of connection with the Supervisor Switch.
Recommended Actions	None.

INVALID_RADIO_INTERFACE

MIB Name	invalidRadioTrap.
Alarm Condition	Invalid radio interface.
NCS Message	Radio with MAC address "{0}" and protocol "{1}" that has joined controller "{2}" has invalid interface. The reason is "{3}."
Symptoms	If a Cisco access point joins the network but has unsupported radios, the controller detects this and generates a trap. This symptom propogates an alert in NCS.
Severity	Critical.
Category	Controller
Probable Causes	The radio hardware is not supported by the controller.
Recommended Actions	None.

RADAR_CLEARED

MIB Name	bsnRadarChannelCleared
Alarm Condition	NA
NCS Message	Radar has been cleared on channel "{1}" which was detected by AP base radio MAC "{0}" on radio 802.11a/n.
Symptoms	Trap is generated after the expiry of a non-occupancy period for a channel that previously generated a radar trap.
Severity	Clear.
Category	Access Point.
Probable Causes	Trap is cleared on a channel.
Recommended Actions	None.

RADAR_DETECTED

MIB Name	bsnRadarChannelDetected
Alarm Condition	NA
NCS Message	Radar has been detected on channel "{1}" by AP base radio MAC "{0}" on radio 802.11a/n.
Symptoms	This trap is generated when radar is detected on the channel on which an access point is currently operating.
Severity	Informational.
Category	Access Point.
Probable Causes	Radar is detected on a channel.
Recommended Actions	None.

RADIO_CORE_DUMP

MIB Name	radioCoreDumpTrap
Alarm Condition	Radio Core Dump.
NCS Message	Radio with MAC address “{0}” and protocol “{1}” has core dump on controller “{2}."
Symptoms	When a Cisco radio fails and a core dump occurs, the controller generates a trap and NCS generates an event for this trap.
Severity	Informational.
Category	Access Point.
Probable Causes	Radio failure.
Recommended Actions	Capture the core dump file using the controller’s command-line interface and send to TAC support.

RADIO_INTERFACE_DOWN

MIB Name	bsnAPIfDown.
Alarm Condition	Radio Interface Down
NCS Message	Radio with MAC address "{0}" and protocol "{1}" is down. The reason is "{2}."
Symptoms	When a radio interface is down, NCS generates an alert. Reason for the radio outage is also noted.
Severity	Critical if not manually disabled. Informational if radio interface was manually disabled.
Category	Access Point.
Probable Causes	• The radio interface has failed. • The access point cannot draw enough power. • The maximum number of transmissions for the access point is reached. • The access point has lost connection with the controller heart beat. • The admin status of the access point admin is disabled. • The admin status of the radio is disabled.
Recommended Actions	None.

RADIO_INTERFACE_UP

MIB Name	bsnAPIfUp.
Alarm Condition	Radio interface up.
NCS Message	Radio with MAC address "{0}" and protocol "{1}" is up. The reason is "{2}."
Symptoms	When a radio interface is operational again, NCS clears the previous alert. Reason for the radio being up again is also noted.
Severity	Clear.
Category	Access Point.
Probable Causes	• Admin status of access point is enabled. • Admin status of radio is enabled. • Global network admin status is enabled.
Recommended Actions	None.

UNSUPPORTED_AP

MIB Name	unsupportedAPTrap.
Alarm Condition	Unsupported AP.
NCS Message	AP "{0}" tried to join controller "{1}" and failed. The controller does not support this kind of AP.

Symptoms	When unsupported access points try to join 40xx/410x controllers or 3500 controller with 64 MB flash, these controllers generate a trap, and the trap is propagated as an event in NCS.
Severity	Informational.
Category	Access Point.
Probable Causes	Access point is not supported by the controller.
Recommended Actions	None.

Traps Added in Release 3.2

The following trap was added in WCS Release 3.2:

LOCATION_NOTIFY_TRAP

MIB Name	locationNotifyTrap.
Alarm Condition	Location notify.
NCS Message	Depending on the notification condition reported, the trap is sent out in an XML format and is reflected in NCS with the following alert messages: • Absence of <Element> with MAC <macAddress>, last seen at <timestamp>. • <Element> with MAC <macAddress> is <In | Out> the Area <campus | building | floor | coverageArea>. • <Element> with MAC <macAddress> has moved beyond <specifiedDistance> ft. of marker <MarkerName>, located at a range of <foundDistance> ft. For detailed info on the XML format for the trap content, consult the *2700 Location Appliance Configuration Guide*.
Symptoms	A 2700 location appliance sends this trap out when the defined location notification conditions are met (such at element outside area, elements missing, and elements exceeded specified distance). NCS uses this trap to display alarms about location notification conditions.
Severity	Minor (under the Location Notification dashboard).
Category	Context Aware Notifications
Probable Causes	The location notification conditions configured for a 2700 location appliance are met for certain elements on the network.
Recommended Actions	None.

Traps Added In Release 4.0

The following traps were added in WCS Release 4.0:

- CISCO_LWAPP_MESH_POOR_SNR, page 13-40
- CISCO_LWAPP_MESH_PARENT_CHANGE, page 13-40

CISCO_LWAPP_MESH_POOR_SNR

MIB Name	ciscoLwappMeshPoorSNR
Alarm Condition	NA
NCS Message	Poor SNR.
Symptoms	SNR (signal-to-noise) ratio is important because high signal strength is not enough to ensure good receiver performance. The incoming signal must be stronger than any noise or interference that is present. For example, you can have high signal strength and still have poor wireless performance if there is strong interference or a high noise level.
Severity	Major.
Category	Mesh
Probable Causes	The link SNR fell below 12 db. The threshold level cannot be changed. If poor SNR is detected on the backhaul link for a child or parent, the trap is generated and contains SNR values and MAC addresses.
Recommended Actions	None.

CISCO_LWAPP_MESH_PARENT_CHANGE

MIB Name	ciscoLwappMeshParentChange
Alarm Condition	NA
NCS Message	Parent changed.
Symptoms	When the parent is lost, the child joins with another parent, and the child sends traps containing both old and new parent's MAC addresses.
Severity	Informational
Category	Mesh

Probable Causes	The child moved to another parent.
Recommended Actions	None.

CISCO_LWAPP_MESH_CHILD_MOVED

MIB Name	ciscoLwappMeshChildMoved
Alarm Condition	Done.
NCS Message	Child moved.
Symptoms	When the parent access point detects a child being lost and communication is halted, the child lost trap is sent to NCS, along with the child MAC address.
Severity	Informational
Category	Mesh
Probable Causes	The child moved from the parent.
Recommended Actions	None.

CISCO_LWAPP_MESH_CONSOLE_LOGIN

MIB Name	ciscoLwappMeshConsoleLogin
Alarm Condition	NA
NCS Message	Console login successful or failed.
Symptoms	The console port provides the ability for the customer to change the user name and password to recover the stranded outdoor access point. To prevent any unauthorized user access to the access point, NCS sends an alarm when someone tries to log in. This alarm is required to provide protection because the access point is physically vulnerable being located outdoors.
Severity	A login is of critical severity.
Category	Mesh
Probable Causes	You have successfully logged in to the access point console port or failed on three consecutive tries.
Recommended Actions	None.

CISCO_LWAPP_MESH_AUTHORIZATION_FAILURE

MIB Name	ciscoLwappMeshAuthorizationFailure
Alarm Condition	NA
NCS Message	Fails to authenticate with controller.
Symptoms	NCS receives a trap from the controller. The trap contains the MAC addresses of those access points that failed authorization.
Severity	Minor.

Category	Mesh
Probable Causes	The access point tried to join the MESH but failed to authenticate because the MESH node MAC address was not on the MAC filter list.
Recommended Actions	None.

EXCESSIVE_ASSOCIATION

MIB Name	ciscoLwappMeshExcessiveAssociationFailure
Alarm Condition	NA
NCS Message	Excessive association failures.
Symptoms	This trap is raised after a failed-association-attempt exceeds the threshold (which is not user configurable). Association failures are cumulative of the total failures from different MAPs. The trap sent by the controller contains the MAC address of the access point on which the association failed and the number of association failures.
Severity	Major.
Category	Mesh
Probable Causes	The controller encountered excessive association failures.
Recommended Actions	None.

CISCO_LWAPP_MESH_PARENT_EXCLUDED_CHILD

MIB Name	ciscoLwappMeshParentExcludedChild
Alarm Condition	NA
NCS Message	Excluded by parent AP due to failed authentication.
Symptoms	When a child keeps failing authentication at the controller, the parent can mark that child for exclusion. The child cannot associate with the parent during this exclusion period. The trap contains the excluded child MAC address.
Severity	Informational
Category	Mesh
Probable Causes	A parent marked a child for exclusion.
Recommended Actions	None.

CISCO_LWAPP_MESH_CHILD_EXCLUDED_PARENT

MIB Name	ciscoLwappMeshChildExcludedParent
Alarm Condition	NA
NCS Message	Parent AP being excluded by child AP.
Symptoms	When a child fails authentication at the controller after a fixed number of attempts, the child can exclude that parent. The child remembers the excluded parent so that when it joins the network, it sends the trap which contains the excluded parent MAC address and the duration of the exclusion period.
Severity	Informational
Category	Mesh
Probable Causes	A child marked a parent for exclusion.
Recommended Actions	None.

CISCO_LWAPP_MESH_EXCESSIVE_PARENT_CHANGE

MIB Name	ciscoLwappMeshExcessiveParentChange
Alarm Condition	NA
NCS Message	Parent changed frequently.
Symptoms	When MAP parent-change-counter exceeds the threshold within a given duration, it sends a trap to NCS. The trap contains the number of times the MAP changes and the duration of the time. The threshold is user configurable.
Severity	Major.
Category	Mesh
Probable Causes	The MESH access point changed its parent frequently.
Recommended Actions	None.

IDS_SHUN_CLIENT_TRAP

MIB Name	CISCO-LWAPP-IDS-MIB. CLIdsNewShunClient.
Alarm Condition	IDS Shun client.
NCS Message	The Cisco Intrusion Detection System "{0}" has detected a possible intrusion attack by the wireless client "{1}."
Symptoms	This trap is generated in response to a shun client clear alert originated from a Cisco IDS/IPs appliance ("{0}") installed in the data path between the wireless client ("{1}") and the site's intranet.
Severity	Critical.
Category	Security

Probable Causes	The designated client is generating a packet-traffic pattern which shares properties with a well-known form of attack on the customer's network.
Recommended Actions	Investigate the designated client and determine if it is an intruder, a virus, or a false alarm.

IDS_SHUN_CLIENT_CLEAR_TRAP

MIB Name	CISCO-LWAPP-IDS-MIB. cLIdsNewShunClientClear.
Alarm Condition	IDS Shun client clear.
NCS Message	The Cisco Intrusion Detection System "{0}" has cleared the wireless client "{1}" from possibly having generated an intrusion attack.
Symptoms	This trap is generated is response to one of two things: 1) a shun client clear alert originated from a Cisco IDS/IPS appliance ("{0}") installed in the data path between the wireless client ("{1"}) and the site's intranet, or 2) a scheduled timeout of the original IDS_SHUN_CLIENT_TRAP for the wireless client.
Severity	Clear.
Category	Security
Probable Causes	The designated client is no longer generating a suspicious packet-traffic pattern.
Recommended Actions	None.

MFP_TIMEBASE_STATUS_TRAP

MIB Name	CISCO-LWAPP-MFP-MIB. ciscoLwappMfpTimebaseStatus.
Alarm Condition	MFP timebase out of sync.
NCS Message	Controller "{0}" is "{1}" with the Central time server.
Symptoms	This notification is sent by the agent to indicate when the synchronization of the controller's time base with the Central time base last occurred.
Severity	Critical (not in sync trap) and clear (sync trap).
Category	Security
Probable Causes	The controller's time base is not in sync with the Central time base.
Recommended Actions	None.

MFP_ANOMALY_DETECTED_TRAP

MIB Name	CISCO-LWAPP-MFP-MIB. ciscoLwappMfpAnomalyDetected.
Alarm Condition	MFP anomaly detected.
NCS Message	MFP configuration of the WLAN was violated by the radio interface "{0}" and detected by the radio interface "{1}" of the access point with MAC address "{2}." The violation is "{3}."

Symptoms	This notification is sent by the agent when the MFP configuration of the WLAN was violated by the radio interface cLApIfSmtDot11Bssid and detected by the radio interface cLApDot11IfSlotId of the access point cLApSysMacAddress. This violation is indicated by cLMfpEventType. When observing the management frame(s) given by cLMfpEventFrames for the last cLMfpEventPeriod time units, the controller reports the occurrence of a total of cLMfpEventTotal violation events of type cLMfpEventType. When the cLMfpEventTotal is 0, no further anomalies have recently been detected, and the NMS should clear any alarm raised about the MFP errors. **Note** This notification is generated by the controller only if MFP was configured as the protection mechanism through cLMfpProtectType.
Severity	Critical.
Category	Security
Probable Causes	The MFP configuration of the WLAN was violated. Various types of violations are invalidMic, invalidSeq, noMic, and unexpectedMic.
Recommended Actions	None.

GUEST_USER_REMOVED_TRAP

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserRemoved.
Alarm Condition	Guest user removed.
NCS Message	Guest user "{1}" deleted on controller "{0}."
Symptoms	This notification is generated when the lifetime of the guest user {1} expires and the guest user's accounts are removed from the controller "{0}."
Severity	Critical.
Category	NCS
Probable Causes	GuestUserAccountLifetime expired.
Recommended Actions	None.

Traps Added or Updated in Release 4.0.96.0

The following traps were added in WCS Release 4.0.96.0:

- AP_IMPERSONATION_DETECTED, page 13-46
- RADIUS_SERVER_DEACTIVATED, page 13-46
- RADIUS_SERVER_ACTIVATED, page 13-46
- RADIUS_SERVER_WLAN_DEACTIVATED, page 13-47
- RADIUS_SERVER_WLAN_ACTIVATED, page 13-47
- RADIUS_SERVER_TIMEOUT, page 13-47
- DECRYPT_ERROR_FOR_WRONG_WPA_WPA2, page 13-47

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
Alarm Condition	AP impersonation detected.
NCS Message	AP Impersonation with MAC "{0}" using source MAC "{1}" is detected by authenticated AP "{2}" on "{3}" radio and slot ID "{4}."
Symptoms	A radio of an authenticated access point had communication with another access point whose MAC address neither matches that of a rogue nor is an authenticated neighbor of the detecting access point.
Severity	Critical.
Category	Security
Probable Causes	A security breach related to access point impersonation may be occurring.
Recommended Actions	Track down the MAC address of the impersonating access point and contain it.

RADIUS_SERVER_DEACTIVATED

MIB Name	ciscoLwappAAARadiusServerGlobalDeactivated.
Alarm Condition	RADIUS Server deactivated.
NCS Message	RADIUS server "{0}" (port {1}) is deactivated.
Symptoms	The controller detects that the RADIUS server is deactivated in the global list.
Severity	Major.
Category	Controller
Probable Causes	RADIUS server is deactivated in the global list.
Recommended Actions	None.

RADIUS_SERVER_ACTIVATED

MIB Name	ciscoLwappAAARadiusServerGlobalDeactivated.
Alarm Condition	Radius server activated.
NCS Message	RADIUS server "{0}" (port {1}) is activated.
Symptoms	The controller detects that the RADIUS server is deactivated in the global list.
Severity	Clear.
Category	Controller
Probable Causes	RADIUS server is activated in the global list.
Recommended Actions	None.

RADIUS_SERVER_WLAN_DEACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanDeactivated.
Alarm Condition	RADIUS Server WLAN deactivated
NCS Message	RADIUS server "{0}" (port {1}) is deactivated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is deactivated on the WLAN.
Severity	Major.
Category	Controller
Probable Causes	RADIUS server is deactivated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_WLAN_ACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanActivated.
Alarm Condition	Radius server WLAN activated.
NCS Message	RADIUS server "{0}" (port {1}) is activated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is activated on the WLAN.
Severity	Clear.
Category	Controller
Probable Causes	RADIUS server is activated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_TIMEOUT

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusReqTimedOut.
Alarm Condition	RADIUS Server timeout.
NCS Message	RADIUS server "{0}" (port {1}) failed to respond to request from client "{2}" with MAC "{3}."
Symptoms	The controller detects that the RADIUS server failed to respond to a request from a client or user.
Severity	Informational.
Category	Controller
Probable Causes	RADIUS server fails to process the request from the client or user.
Recommended Actions	None.

DECRYPT_ERROR_FOR_WRONG_WPA_WPA2

MIB Name	CISCO-LWAPP-DOT11-CLIENT-MIB. CiscoLwappDot11ClientKeyDecryptError.
Alarm Condition	Client decrypt error occurred

NCS Message	Decrypt error occurred at AP with MAC "{0}" running TKIP with wrong WPA/WPA2 by client with MAC "{1}."
Symptoms	The controller detects that a user is trying to connect with an invalid security policy for WPA/WPA2 types.
Severity	Minor.
Category	Security
Probable Causes	The user failed to authenticate and join the controller.
Recommended Actions	None.

Traps Added or Updated in Release 4.1

The following traps were added for WCS Release 4.1:

- LRAD_UNSUPPORTED, page 13-58

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
Alarm Condition	AP impersonation detected.
NCS Message	AP impersonation of MAC "{0}" using source MAC "{1}" is detected by an authenticated AP "{2}" on "{3}" radio and slot ID "{4}."
Symptoms	A radio of an authenticated access point received signals from another access point whose MAC address neither matches that of a rogue nor is an authenticated neighbor of the detecting access point.
Severity	Critical.
Category	Access Point..
Probable Causes	A security breach related to access point impersonation has occurred.
Recommended Actions	Track down the MAC address of the impersonating access point and contain it.

INTERFERENCE_DETECTED

MIB Name	cognioInterferenceAlarm.
Alarm Condition	None.
NCS Message	Interference detected by type {0} with power {1}.
Symptoms	A Cognio spectrum agent detected interference over its configured thresholds.
Severity	Minor.
Category	SE Detected Interferers
Probable Causes	Excessive wireless interference or noise.
Recommended Actions	None.

INTERFERENCE_CLEAR

MIB Name	COGNIO-TRAPS-MIB. cognioInterferenceClear
Alarm Condition	None.
NCS Message	Interference cleared.
Symptoms	The Cognio spectrum expert agent no longer detects an interference source over its configured threshold.
Severity	Clear.
Category	SE Detected Interferers
Probable Causes	Previous excessive wireless interference or noise is gone.
Recommended Actions	None.

ONE_ANCHOR_ON_WLAN_UP

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityOneAnchorOnWlanUp.
Alarm Condition	
NCS Message	Controller "{0}." An anchor of WLAN "{1}" is up.
Symptoms	Successive EoIP and UDP ping to at least one anchor on the WLAN is up.
Severity	Clear.
Category	Controller
Probable Causes	At least one anchor is reachable from an EoIP/UDP ping.
Recommended Actions	None.

RADIUS_SERVER_DEACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerGlobalDeactivated.
Alarm Condition	RADIUS Server deactivated.
NCS Message	RADIUS server "{0}" (port {1}) is deactivated.
Symptoms	The controller detects that the RADIUS server is deactivated in the global list.
Severity	Major.
Category	Controller
Probable Causes	RADIUS server is deactivated in the global list.
Recommended Actions	None.

RADIUS_SERVER_ACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerGlobalActivated.
Alarm Condition	Radius server activated.
NCS Message	RADIUS server "{0}" (port {1}) is activated.
Symptoms	The controller detects that the RADIUS server is activated in the global list.
Severity	Clear.
Category	Controller
Probable Causes	RADIUS server is activated in the global list.
Recommended Actions	None.

RADIUS_SERVER_WLAN_DEACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanDeactivated.
Alarm Condition	Radius server WLAN deactivated.
NCS Message	RADIUS server "{0}" (port {1}) is deactivated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is deactivated on the WLAN.
Severity	Major.
Category	Controller
Probable Causes	RADIUS server is deactivated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_WLAN_ACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerGlobalWlanActivated.
Alarm Condition	Radius server WLAN activated.
NCS Message	RADIUS server "{0}" (port {1}) is activated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is activated on the WLAN.
Severity	Clear.
Category	Controller
Probable Causes	RADIUS server is activated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_TIMEOUT

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusReqTimedOut.
Alarm Condition	RADIUS Server timeout.
NCS Message	RADIUS server "{0}" (port {1}) failed to respond to request from client "{2}" with MAC "{3}."
Symptoms	The controller detects that the RADIUS server failed to respond to a request from the client or user.
Severity	Informational.
Category	Controller
Probable Causes	The RADIUS server fails to process the request from a client or user.
Recommended Actions	None.

MOBILITY_ANCHOR_CTRL_PATH_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorControlPathDown.
Alarm Condition	Mobility anchor control path down.

NCS Message	Controller "{0}." Control path on anchor "{1}" is down.
Symptoms	When successive ICMP ping attempts to the anchor fails, the anchor is conclusively down.
Severity	Major.
Category	Controller
Probable Causes	Anchor not reachable by ICMP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_CTRL_PATH_UP

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorControlUp.
Alarm Condition	Mobility anchor control path up.
NCS Message	Controller "{0}." Control path on anchor "{1}" is up.
Symptoms	The ICMP ping to the anchor is restored, and the anchor is conclusively up.
Severity	Clear.
Category	Controller
Probable Causes	The anchor is reachable by an ICMP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_DATA_PATH_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorDataPathDown.
Alarm Condition	Mobility anchor data path down.
NCS Message	Controller "{0}." Data path on anchor "{1}" is down.
Symptoms	Successive EoIP ping attempts to the anchor fails, and the anchor is conclusively down.
Severity	Major.
Category	Controller
Probable Causes	The anchor is not reachable by an EoIP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_DATA_PATH_UP

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorDataPathUp.
Alarm Condition	Mobility anchor data path up.
NCS Message	Controller "{0}." Data path on anchor "{1}" is up.
Symptoms	The EoIP ping to the anchor is restored, and the anchor is conclusively up.
Severity	Clear.
Category	Controller
Probable Causes	Anchor is reachable by the EoIP ping.
Recommended Actions	None.

WLAN_ALL_ANCHORS_TRAP_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAllAnchorsOnWlanDown.
Alarm Condition	WLAN all anchors down.
NCS Message	Controller "{0}." All anchors of WLAN "{1}" are down.
Symptoms	Successive EoIP ping attempts to all the anchors on WLAN is occurring.
Severity	Critical.
Category	Controller
Probable Causes	Anchors are not reachable by the EoIP ping.
Recommended Actions	None.

MESH_AUTHORIZATIONFAILURE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshAuthorizationFailure.
Alarm Condition	Mesh authorization failure.
NCS Message	MESH "{0}" fails to authenticate with controller because "{1}"
Symptoms	A mesh access point failed to join the mesh network because its MAC address is not listed in the MAC filter list. The alarm includes the MAC address of the mesh access point that failed to join.
Severity	Minor.
Category	Mesh
Probable Causes	The mesh node MAC address is not in the MAC filter list, or a security failure from the authorization server occurred.
Recommended Actions	None.

MESH_CHILDEXCLUDEDPARENT

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshChildExcludedParent.
Alarm Condition	Mesh child exclude parent.
NCS Message	Parent AP being excluded by child AP due to failed authentication, AP current parent MAC address "{0}," previous parent MAC address "{1}."
Symptoms	This notification is sent by the agent when the child access point marks a parent access point for exclusion. When the child fails to authenticate at the controller after a fixed number of times, the child marks the parent for exclusion. The child remembers the excluded MAC address and informs the controller when it joins the network. The child access point marks the MAC address and excludes it for the time determined by MAP node so that it does not try to join this excluded node. The child MAC address is sent as part of the index.
Severity	Informational
Category	Mesh
Probable Causes	The child access point failed to authenticate to the controller after a fixed number of times.
Recommended Actions	None.

MESH_PARENTCHANGE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshParentChange.
Alarm Condition	Mesh parent change.
NCS Message	MESH "{0}" changed its parent. AP current parent MAC address "{1}," previous parent MAC address "{2}."
Symptoms	This notification is sent by the agent when a child moves to another parent. The alarm includes the MAC addresses of the former and current parents.
Severity	Informational
Category	Mesh
Probable Causes	The child access point has changed its parent.
Recommended Actions	None.

MESH_PARENTEXCLUDECHILD

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshParentExcludedChild
Alarm Condition	NA
NCS Message	MESH "{0}" being excluded by parent AP due to failed authentication. AP neighbor type "{1}".

Symptoms	This notification is sent by the agent when the parent AP marks a child to be excluded. When child keeps failing authentication at controller, parent can mark child to be excluded for configured value for 'clMeshExclusionTimeout', so that child does not associate again with the parent.
Severity	Informational
Category	Mesh
Probable Causes	Child keeps failing authentication at controller.
Recommended Actions	None.

MESH_CHILDMOVED

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshChildMoved.
Alarm Condition	Mesh child removed.
NCS Message	Parent AP "{0}" lost connection to AP "{1}". AP neighbor type is "{2}".
Symptoms	This notification is sent by the agent when the parent access point loses connection with its child.
Severity	Informational.
Category	Mesh
Probable Causes	The parent access point lost connection with its child.
Recommended Actions	None.

MESH_EXCESSIVEASSOCIATIONFAILURE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshExcessiveAssociationFailure
Alarm Condition	Mesh excessive association failure.
NCS Message	MESH "{0}" has excessive association failures.
Symptoms	This notification is sent by the agent when the cumulative association failures of child APs exceeds value configured in 'clMeshExcessiveAssociationFailure'
Severity	Major
Category	Mesh
Probable Causes	This can happen when the cumulative association failure of child APs exceeds value configured in 'clMeshExcessiveAssociationFailure'.
Recommended Actions	None.

MESH_EXCESSIVEPARENTCHANGE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshExcessiveParentChange.
Alarm Condition	Mesh excessive parent change.
NCS Message	MESH "{0}" changes parent frequently.
Symptoms	This notification is sent by the agent if the number of parent changes for a given mesh access point exceeds the threshold. Each access point keeps count of the number of parent changes within a fixed time. If the count exceeds the threshold defined by c1MeshExcessiveParentChangeThreshold, then the child access point informs the controller.
Severity	Major.
Category	Mesh
Probable Causes	The child access point has frequently changed its parent.
Recommended Actions	None.

MESH_POORSNR

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshPoorSNR.
Alarm Condition	Mesh Poor SNR.
NCS Message	MESH "{0}" has SNR on backhaul link as "{1}" which is lower then predefined threshold.
Symptoms	This notification is sent by the agent when the child access point detects a signal-to-noise ratio below 12dB the backhaul link. The alarm includes the SNR value and the MAC addresses of the parent and child.
Severity	Major.
Category	Mesh
Probable Causes	SNR is lower then the threshold defined by c1MeshSNRThreshold.
Recommended Actions	None.

MESH_POORSNRCLEAR

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshPoorSNRClear.
Alarm Condition	Mesh Poor SNR clear.
NCS Message	MESH "{0}" has SNR on backhaul link as "{1}" which is normal now.
Symptoms	This notification is sent by the agent to clear ciscoLwappMeshPoorSNR when the child access point detects SNR on the backhaul link that is higher than the threshold defined by c1MeshSNRThreshold.
Severity	Informational
Category	Mesh

Probable Causes	SNR on the backhaul link is higher than the threshold defined by c1MeshSNRThreshold.
Recommended Actions	None.

MESH_CONSOLELOGIN

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshConsoleLogin.
Alarm Condition	Mesh console login.
NCS Message	MESH "{0}" has console logged in with status "{1}".
Symptoms	This notification is sent by the agent when login on the MAP console is successful or when a failure occurred after three attempts.
Severity	Critical.
Category	Mesh
Probable Causes	Login on the MAP console was successful, or a failure occurred after three attempts.
Recommended Actions	None.

LRADIF_REGULATORY_DOMAIN

MIB Name	ciscoLwappApIfRegulatoryDomainMismatchNotif
Alarm Condition	Radio interface regulatory domain mismatch.
NCS Message	Access Point "{0}" is unable to associate. The Regulatory Domain "{1}" configured on interface "{2}" does not match the controller "{3}" regulatory domain "{4}."
Symptoms	The system generates this trap when the regulatory domain configured on the access point radios does not match the country code configured on the controller.
Severity	Critical.
Category	Access Point.
Probable Causes	If the controller's country code configuration is changed, and some access points support a different country code, then these access points fail to associate. An access point on the controller's network sends join requests to the controller, but the regulatory domain is outside the domain in which the controller is operating.
Recommended Actions	Either remove the access points that are not meant for inclusion in the controller's domain or correct the controller's country code setting.

LRAD_CRASH

MIB Name	ciscoLwappApCrash
Alarm Condition	Access point crash.
NCS Message	Access Point "{0}" crashed and has a core dump on controller "{1}."
Symptoms	An access point has crashed.
Severity	Informational.
Category	Access Point.
Probable Causes	Access point failure.
Recommended Actions	Capture the core dump file using the controller's CLI and send it to TAC support.

LRAD_UNSUPPORTED

MIB Name	ciscoLwappApUnsupported
Alarm Condition	Access point not supported.
NCS Message	Access Point "{0}" tried to join controller "{1}" and failed. Associate failure reason "{2}."
Symptoms	An access point tried to associate to a controller to which it is not supported.
Severity	Informational.
Category	Access Point.
Probable Causes	The access point is not supported by the controller.
Recommended Actions	None.

Traps Added or Updated in Release 4.2

The following traps were added to WCS Release 4.2:

- GUEST_USER_ADDED, page 13-59
- GUEST_USER_AUTHENTICATED, page 13-59
- IOSAP_LINK_UP, page 13-59
- LRAD_POE_STATUS, page 13-60
- ROGUE_AP_NOT_ON_NETWORK, page 13-60
- IOSAP_UP, page 13-60

GUEST_USER_ADDED

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserAdded
Alarm Condition	Guest user added.
NCS Message	Guest user "{0}" created on the controller “{1}.”
Symptoms	This notification is sent by the agent when the GuestUser account is created successfully.
Severity	Informational.
Category	NCS
Probable Causes	The guest user account was created on the agent by either CLI, Web UI, or NCS.
Recommended Actions	None.

GUEST_USER_AUTHENTICATED

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserLogged
Alarm Condition	Guest user authenticated.
NCS Message	Guest user "{1}" logged into controller "{0}."
Symptoms	This notification is sent by the agent when the GuestUser logged into the network through webauth successfully.
Severity	Informational.
Category	Controller
Probable Causes	The guest user was successful with webauth authentication.
Recommended Actions	None.

IOSAP_LINK_UP

MIB Name	linkUp
Alarm Condition	Autonomous AP Link Up.
NCS Message	Autonomous AP “{0},” Interface “{1}” is {2} up.
Symptoms	The physical link is up on an autonomous access point radio port.
Severity	Clear.
Category	Access Point.
Probable Causes	A physical link has been restored to the autonomous access point.
Recommended Actions	None.

LRAD_POE_STATUS

MIB Name	ciscoLwappApPower
Alarm Condition	POE Status.
NCS Message	Access point “{0}” draws low power from Ethernet. Failure reason: “{1}”
Symptoms	This notification is generated when the access point draws low power from the Ethernet connection.
Severity	Critical.
Category	Access Point.
Probable Causes	The access point receives low power from the Ethernet connection.
Recommended Actions	Check the power status of the access point and the device connected to the access point.

ROGUE_AP_NOT_ON_NETWORK

MIB Name	bsnRogueAPDetectedOnWiredNetwork (bsnRogueAPOnWiredNetwork is set to false).
Alarm Condition	ROGUE_AP_NOT_ON_NETWORK
NCS Message	Rogue AP or ad hoc rogue "{0}" is not able to connect to the wired network.
Symptoms	A rogue access point is no longer on the wired network.
Severity	Informational.
Category	Rogue AP
Probable Causes	The rogue access point is no longer reachable on the wired network.
Recommended Actions	None.

IOSAP_UP

MIB Name	None.
Alarm Condition	Autonomous AP Up.
NCS Message	The autonomous AP “{0}” is reachable.
Symptoms	The autonomous AP is SNMP reachable.
Severity	Clear.
Category	Access Point.
Probable Causes	The autonomous access point starts to respond to SNMP queries.
Recommended Actions	None.

Traps Added or Updated in Release 5.0

The following traps were added for WCS Release 5.0:

- GUEST_USER_LOGOFF, page 13-61
- STATION_ASSOCIATE_DIAG_WLAN, page 13-61

GUEST_USER_LOGOFF

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserLoggedOut
Alarm Condition	Guest user logged off.
NCS Message	Guest user "{1}" logged out from the controller "{0}."
Symptoms	This notification is sent by the agent when a GuestUser who was previously logged into the network logs out.
Severity	Informational.
Category	Controller
Probable Causes	The GuestUser logs off from the network.
Recommended Actions	None.

STATION_ASSOCIATE_DIAG_WLAN

MIB Name	CISCO-LWAPP-DOT11-CCX-CLIENT-MIB.cldccDiagClientAssociatedToDiagWlan
Alarm Condition	Client Associated to Diagnostic Channel.
NCS Message	Client "{0}" is associated to diagnostic WLAN with reason "{1}."
Symptoms	This notification is sent by the agent when a v5 client associates to a diagnostic channel.
Severity	Informational.
Probable Causes	When a CCXv5 client gets associated to the diagnostic channel WLAN on WLC, this trap is raised.
Category	Clients
Recommended Actions	If you wish to automatically perform client troubleshooting, you must enable Client Troubleshooting in Administration > Settings > client. After it is enabled, the series of V5 tests are carried out on the client upon trap arrival, and the client is updated with the test status via pop-up messages. The report is placed in the logs directory. The log filename is shown in the Client Details page in the Automated Troubleshooting Report section. You can export all automated troubleshooting logs.

Traps Added or Updated in Release 5.2

The following traps were added for WCS Release 5.2:

- LRAD_REBOOTREASON, page 13-62
- WIPS_TRAPS, page 13-62

LRAD_REBOOTREASON

MIB Name	ciscoLwappApAssociated
Alarm Condition	AP reboot reason.
NCS Message	Access Point ''{0}'' associated to controller ''{2}'' on port number ''{1}''. Reason for association ''{3}''.
Symptoms	
Severity	Informational
Category	Access Point.
Probable Causes	None.
Recommended Actions	None.

WIPS_TRAPS

MIB Name	ciscoLwappIpsMIBNotif
Alarm Condition	wIPS Traps.
NCS Message	Dynamically generated per alarm.
Symptoms	Refer to wIPS alarm encyclopedia under WCS>Configuration>wIPS Profiles.
Severity	Critical
Category	Security
Probable Causes	Possible security attacks.
Recommended Actions	None.

Alarm Names

- DoS: Association flood
- DoS: Association table overflow
- DoS: Authentication flood
- DoS: EAPOL-Start attack
- DoS: PS-Poll flood
- DoS: Unauthenticated association
- DoS: CTS flood
- DoS: Queensland University of Technology Exploit
- DoS: RF jamming
- DoS: RTS flood
- DoS: Virtual Carrier attack
- DoS: Authentication-failure attack
- DoS: De-Auth broadcast flood
- DoS: De-Auth flood
- DoS: Dis-Assoc broadcast flood
- DoS: Dis-Assoc flood
- DoS: EAPOL-Logoff attack
- DoS: FATA-Jack tool
- DoS: Premature EAP-Failure
- DoS: Premature EAP-Success
- ASLEAP tool detected
- Airsnarf attack
- ChopChop attack
- Day-Zero attack by WLAN security anomaly
- Day-Zero attack by device security anomaly
- Device probing for APs
- Dictionary attack on EAP methods
- Fake APs detected
- Fake DHCP server detected
- Fast WEP crack tool detected
- Fragmentation attack
- Honeypot AP detected
- Hotspotter tool detected
- Hotspotter tool detected
- Malformed 802.11 packets detected
- Man in the middle attack

- NetStumbler detected
- Netstumbler victim detected
- PSPF violation detected
- Soft AP or host AP detected
- Spoofed MAC address detected
- Suspicious after-hours traffic detected
- Unauthorized association by vendor list
- Unauthorized association detected
- Wellenreiter detected

Traps Added or Updated in Release 6.0

The following traps were added for WCS Release 6.0:

- MSE_EVAL_LICENSE, page 13-64
- MSE_LICENSING_ELEMENT_LIMIT, page 13-65
- STATION_AUTHENTICATED, page 13-65
- WLC_LICENSE_NOT_ENFORCED, page 13-65
- WLC_LICENSE_COUNT_EXCEEDED, page 13-66
- VOIP_CALL_FAILURE, page 13-66

MSE_EVAL_LICENSE

MIB Name	None
Alarm Condition	MSE Evaluation license expired.
NCS Message	Evaluation license for {0} is expired.
Symptoms	The tracking for clients or tags stops, or service does not come up.
Severity	Critical.
Category	MSE
Probable Causes	The evaluation period for the service has expired.
Recommended Actions	Add a permanent license for the service using License Center or the appropriate third-party vendor application.

MSE_LICENSING_ELEMENT_LIMIT

MIB Name	None
Alarm Condition	MSE Licensing element limit reached.
NCS Message	{0} limit for {1} is reached or exceeded.
Symptoms	Elements are not tracked beyond a certain limit.
Severity	Critical.
Category	MSE
Probable Causes	Limit for the specified service has been reached.
Recommended Actions	Add a license with higher licensed capacity for the particular service.

STATION_AUTHENTICATED

MIB Name	ciscoLwappDot11ClientMovedToRunState
Alarm Condition	Client Authentication failure.
NCS Message	Client "{0}" is authenticated with interface "{2}" of AP "{1}."
Symptoms	A client has completed a security policy and has moved to Run state. It can start to send or receive data.
Severity	Informational.
Category	Wired Clients.
Probable Causes	A client has completed security policy and moved to Run state.
Recommended Actions	None.

WLC_LICENSE_NOT_ENFORCED

MIB Name	clmgmtLicenseNotEnforced
Alarm Condition	Attempt to use an unlicensed Controller feature.
NCS Message	Controller {0} has AP with unlicensed feature {1} version {2} attempting to join.
Symptoms	An access point with a licensed feature is trying to join a controller without the proper license.
Severity	Critical.
Category	Controller
Probable Causes	An access point with a WPLUS feature like indoor mesh or OfficeExtend AP is trying to join a controller without a WPLUS license.
Recommended Actions	You must add a WPLUS license to the controller or fix the primary, secondary, or tertiary controller configuration to have controllers with WPLUS licenses.

WLC_LICENSE_COUNT_EXCEEDED

MIB Name	clmgmtLicenseUsageCountExceeded
Alarm Condition	AP attempted to join Controller with licensed AP count exceeded.
NCS Message	Controller {0} with license {1} version {2} and counted feature {4} with limit {3} has been exceeded {5}.
Symptoms	The access point cannot join a controller.
Severity	Critical.
Category	Controller
Probable Causes	The controller has reached the maximum licensed access point capacity.
Recommended Actions	Add a license capacity to the controller or move the access point to a controller with more capacity.

VOIP_CALL_FAILURE

MIB Name	ciscoLwappVoipCallfailureNotif
Alarm Condition	VoIP Call failed.
NCS Message	VoIP Call failure of {4} (Error Code {3}) occurred on Client {0} with phone number {5} calling {6} which was associated with AP {1} on interface {2}.
Symptoms	VoIP snooping is enabled on a WLAN.
Severity	Informational.
Category	Clients
Probable Causes	A SIP error is detected by an access point.
Recommended Actions	The actions depend on the type of error that is being reported. Errors can range from “dialed number does not exist,” “busy,” “service unavailable,” to “service timeout.”

Traps Added or Updated in Release 7.0

SI_AQ_TRAPS

MIB Name	ciscoLwappSiAqLow
Alarm Condition	Air Quality Traps
NCS Message	Air Quality Index on Channel {0} is {1} (Threshold: {2}).
Symptoms	Air Quality fall below the set Threshold.
Severity	Minor.
Category	Performance.

Probable Causes	Threshold is set via the configuration->controller->CleanAir. When the Air Quality Index computed by the AP falls below the set threshold this is triggered.
Recommended Actions	Detect Source of Interference and remove it from the environment or enable RRM so that AP can move to another clean channel.

SI_SECURITY_TRAPS

MIB Name	ciscoLwappSiIdrDevice
Alarm Condition	Interferer Security Traps.
NCS Message	Set: Security-Risk Interferer {0} is detected. Clear: Security-risk Interferer "{0}" is no longer detected.
Symptoms	Raised when Interferer marked as a security threat is detected by the network.
Severity	Critical.
Category	Security
Probable Causes	Interferer marked as a security threat is detected by the network. Interferers have to configured to as Security threat and it can be done via the configuration->controller->CleanAir section.
Recommended Actions	Detect Source of Interference and remove it from the environment.

SI_SENSOR_CRASH_TRAPS

MIB Name	ciscoLwappSiSensorCrash
Alarm Condition	Sensor Crash Traps
NCS Message	CleanAir Sensor Status: {0} Error Code: {1}.
Symptoms	CleanAir Sensor Software stopped working.
Severity	Critical.
Category	Access Point.
Probable Causes	General SensorD crashes.
Recommended Actions	Reboot the AP.

Traps Added or Updated in Release 7.0.1

The following traps were added to WCS Release 7.0.1:

- FAN_MONITOR, page 13-68
- FUTURE_RESTART_DAY_MSG, page 13-68
- LOCATION_CALCULATOR, page 13-69
- RAID_MONITOR, page 13-73
- POWER_MONITOR, page 13-73
- SI_AQ_BUFFER_UNAVAILABLE_TRAPS, page 13-74

- NCS_NOTIFICATION_ALARM, page 13-75
- NMSP, page 13-76
- MSE_DOWN, page 13-76

FAN_MONITOR

MIB Name	None.
Alarm Condition	Fan Monitor on MSE
Category	Mobility Services
Symptoms	A system cooling fan gone bad.
Severity	Critical
NCS Message	Cooling fan failure [applies to MSE-3355 only]. One of the CPU cooling fans on $HOST [$IP] has failed.
Probable Causes	Failure of a fan.
Recommended Actions	Customer should contact Cisco TAC to arrange for replacing the system. This failure cannot be fixed in the field (fan is not replaceable).

FUTURE_RESTART_DAY_MSG

MIB Name	None.
Alarm Condition	MSE Restart
Category	Mobility Service
Symptom	None.
Severity	Major
NCS Message	The MSE {0} will be restarted on {date} at {time} am/pm..
Probable Causes	Planned restart for password refresh to prevent Oracle db locking.
Recommended Actions	None.

MIB Name	None.
Alarm Condition	MSE Restart
Category	Mobility Service
Symptom	NCS reported lost connectivity or MSE became unreachable momentarily.
Severity	Major
NCS Message	The MSE {0} was restarted on {date}.

Probable Causes	Planned restart for password refresh to prevent Oracle db locking.
Recommended Actions	None.

LOCATION_CALCULATOR

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Failed to complete the heatmap calculation processs.
Symptoms	Missing device locations. Inaccurate device location.
Severity	Major
Category	Mobility Service
Probable Causes	Matlab process crash.
Recommended Actions	None. System tries to correct itself every 2 hours. If needed resync the floors to the MSE.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Recovered from Matlab crash and completed the heatmap calculation process.
Symptoms	Devices start showing up or location is more accurate.
Severity	Clear
Category	Mobility Service
Probable Causes	Matlab process crash.
Recommended Actions	System recovered from a previous crash.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR The data set in the calibration is not initialized properly for Calibration Model (Name, id): {0} , {1}.
Symptoms	Poor location accuracy.
Severity	Major
Category	Mobility Service

Probable Causes	Calibration data pushed from NCS to MSE not good.
Recommended Actions	Reapply calibration model to the floor and resync to the MSE. Worst case, redo calibration.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Recovered from calibration error for model (Name, Id): {0}, {1}.
Symptoms	Improved location accuracy.
Severity	Clear
Category	Mobility Service
Probable Causes	System recovered from a previous calibration error due to resync.
Recommended Actions	None.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Failed to calculate Heatmap for AP Interface {0}. Falling back to using default heatmap.
Symptoms	No location for device or poor location accuracy..
Severity	Major
Category	Mobility Service
Probable Causes	Bad AP Data like antenna type, antenna pattern etc.
Recommended Actions	Correct AP antenna type/pattern of the AP Interface and resync the floor with the error AP to MSE. Enable Default Heatmaps Calculation from Context Aware Service -> Location Parameters page and resync the floor with the error AP to MSE..

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Successful heatmap computation for AP Key {0}.
Symptoms	Devices start showing up or location is more accurate.
Severity	Clear
Category	Mobility Service

Probable Causes	System recovered from a previous heatmap calculation error.
Recommended Actions	None.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR No Rails and Regions input specified for AP interface for floor (name, id): {0}, {1}.
Symptoms	Device show outside or inside unexpected areas on the maps.
Severity	Informational
Category	Mobility Service
Probable Causes	Default inclusion region was deleted from floor map.
Recommended Actions	Recreate the inclusion area on the floor map.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Rails and Regions added back to floor (name, id): {0}, {1}.
Symptoms	Devices locations are always constrained within the floor map inclusion region boundary.
Severity	Clear
Category	Mobility Service
Probable Causes	Inclusion region was added back to the floor map.
Recommended Actions	None.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Heatmap generated for AP Interface: {0} is not a location heatmap.
Symptoms	Devices not showing up.
Severity	Minor
Category	Mobility Service
Probable Causes	Mostly system error.
Recommended Actions	None. System tries to auto correct itself after 2 hours.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Successful heatmap computation of AP Key: {0}.
Symptoms	Devices start showing up.
Severity	Clear
Category	Mobility Service
Probable Causes	System recovered from a previous heatmap calculation error.
Recommended Actions	None.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Skipping default heatmap creation for AP Interface {0}.
Symptoms	No location for device or poor location accuracy.
Severity	Major
Category	Mobility Service
Probable Causes	Use of unknown Antenna pattern or non cisco antennas and use of default heatmaps is disabled.
Recommended Actions	Enable default heatmap calculation from Context Aware Service-> Location parameters page.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Floor (name): {0} was deleted.
Symptoms	No location for device.
Severity	Clear
Category	Mobility Service
Probable Causes	Floor with heatmap calculation error was deleted.
Recommended Actions	None.

RAID_MONITOR

MIB Name	None.
Alarm Condition	RAID Monitor on MSE.
Category	Mobility Services
Symptoms	One of the disks in a RAID array has failed, as reported by the RAID controller.
Severity	Critical
NCS Message	A Hard Disk in a RAID set has failed. This applies to all three [3310, 3350, 3355] platforms. One of the hard drives on $HOST [$IP] has failed and must be be replaced. Contact Cisco Customer Support immediately for assistance.
Probable Causes	Failure of a disk drive.
Recommended Actions	Replace the failed drive (if 3350, 3355) with a new hard drive, or setup an RMA with Cisco (for 3310). The new drive is automatically rebuilt (3355, 3350) by the RAID controller. For 3310, field replacement of the drive is NOT supported.

POWER_MONITOR

MIB Name	None.
Alarm Condition	Power Monitor on MSE.
NCS Message	No power supply redundancy [applies to MSE-3355 only]. One of the power supplies on $HOST [$IP] is not connected to a power source.
Symptoms	System has two power supplies but only one of them is connected to a power source.
Severity	Critical
Category	Mobility Services
Probable Causes	None.
Recommended Actions	Customer should connect the power supply to a good power source.

MIB Name	None.
Alarm Condition	Power Monitor on MSE.
NCS Message	Power supply missing or failed [applies to MSE-3355 only] Message Detail: One of the power supplies on $HOST [$IP] has failed or is missing." >.
Symptoms	System has two power supplies but one of them has failed or one of them has been physically removed.

Severity	Critical
Category	Mobility Service
Probable Causes	Bad or missing power supply.
Recommended Actions	Customer should check the power supplies and if it has failed, then replace it with a good one. Power supplies are spare items than can be ordered by customers. If the power supply is missing, then do the obvious.

SI_AQ_BUFFER_UNAVAILABLE_TRAPS

MIB Name	ciscoLwappSiAqBufferUnavailable
Alarm Condition	AQ Buffer unavailable on controller.
NCS Message	NCS MESSAGE (RAISE): AQ data for AP "{0}" interface "{1}" is not available as AQ buffer allocation limit ("{2}") on controller has reached or AQ data allocation failed. NCS MESSAGE (CLEAR): Allocation for AQ buffer successful, AQ data is now available for AP "{0}" interface "{1}".
Symptoms	This notification is generated if Air Quality buffer is unavailable.
Severity	Warning.
Category	Controller
Probable Causes	Controller Resource limitation.
Recommended Actions	None.

NCS_NOTIFICATION_ALARM

MIB Name	ciscoWirelessMOStatusNotification
Alarm Condition	NCS notification alarm.
NCS Message	NCS Message varies depending on the different HM sub category of the trap.
Symptoms	Health Monitor uses this trap to send notification to NCS to indicate the Health Monitor alarm during various operation phases. • HM_DATABASE • HM_DATABASE_CRITICAL • HM_FAILBACK • HM_FAILOVER • HM_REACHABILITY • HM_REGISTRATION
Severity	• HM_DATABASE—Major • HM_DATABASE_CRITICAL—Critical • HM_FAILBACK—Major • HM_FAILOVER-Major • HM_REACHABILITY—Major • HM_REGISTRATION—Major
Category	High Availability
Probable Causes	• HM_DATABASE_CRITICAL—The database is down and cannot be started by HM. • HM_DATABASE—At the Database level, the connection between primary and secondary is lost. • HM_FAILBACK—Failback attempt failed. • HM_ FAILOVER -Failover attempt failed. • HM_REACHABILITY—Primary and Secondary cannot reach each other. • HM_REGISTRATION—Failed HA registration due to invalid authentication parameters.
Recommended Actions	• HM_DATABASE_CRITICAL—Check the database and NCS log files for more information. • HM_DATABASE—Check the database and NCS log files for more information. • HM_FAILBACK—Check the NCS log file for more information. • HM_ FAILOVER—Check the NCS log file for more information. • HM_REACHABILITY—Ensure that network connectivity is functioning. • HM_REGISTRATION—Ensure that the authentication key, version number, OS platform are all correct.

NMSP

MIB Name	None.
Alarm Condition	NMSP Connection Status.
NCS Message	NMSP Connection Status: INACTIVE, Controller IP: {0}.
Symptoms	Devices associated with this controller are not located by MSE.
Severity	Critical.
Category	Mobility Services
Probable Causes	Controller not reachable from MSE, Controller in read only mode on WCS, Controller and MSE are not NTP time synched.
Recommended Actions	Check NMSP Connection Status troubleshooting wizard for suggestions to fix the problem. Click on the Tools link next to an inactive connection to open the wizard.

MIB Name	None.
Alarm Condition	NMSP Connection Status.
NCS Message	NMSP Connection Status: INACTIVE, Controller IP: {0}.
Symptoms	Device from Controller associated with the MSE show up.
Severity	Clear.
Category	Mobility Services
Probable Causes	NMSP Connection was reestablished between the MSE and the Controller or Switch.
Recommended Actions	None.

MSE_DOWN

MIB Name	None.
Alarm Condition	MSE down
NCS Message	MSE <Name> with IP Address <IPAddress> on port <port number> is unreachable.
Symptoms	Communication with MSE is not happening.
Severity	Major.
Category	Mobility Services
Probable Causes	This alarm is generated when the MSE or the LBS is unreachable from the NCS.
Recommended Actions	Ensure that the MSE Service is network reachable from NCS and services on MSE are running correctly.

Traps Added in NCS Release 1.0

The following traps were added in NCS 1.0:

- VOICE_COVERAGE_HOLE_ALARM, page 13-90
- WLC_SCHEDULED_RESET, page 13-91

AP_FUNCTIONALITY_LICENSE_EXPIRED

MIB Name	bsnAPFunctionalityDisabled
Alarm Condition	AP functionality license expired.
NCS Message	AP functionality has been disabled for key ‘’{0}’’ reason being ‘’{1}’’ for feature-set ‘’{2}’’.
Symptoms	None.
Severity	Critical
Category	Controller
Probable Causes	None.
Recommended Actions	None.

AP_IP_FALLBACK

MIB Name	bsnAPIPAddressFallback
Alarm Condition	AP IP fallback.
NCS Message	AP "{0}" with static-ip configured as "{2}" has fallen back to the working DHCP address "{1}".
Symptoms	None.
Severity	Minor
Category	Access Point.
Probable Causes	None.
Recommended Actions	None.

COUNTRY_CODE_CHANGED

MIB Name	countryChangeTrap
Alarm Condition	Country code changes.
NCS Message	None.
Symptoms	None.
Severity	Information
Category	Controller

Probable Causes	None.
Recommended Actions	None.

CPU_RX_MULTICAST_QUEUE_FULL

MIB Name	bsnRxMulticastQueueFull
Alarm Condition	CPU RX Multicast queue full.
NCS Message	CPU Receive Multicast Queue is full on Controller ‘’{0}’’.
Symptoms	None.
Severity	Critical
Category	Controller
Probable Causes	None.
Recommended Actions	None.

FAN_FAILURE

MIB Name	fanFailureTrap
Alarm Condition	Fan failure.
NCS Message	Fan failure. Controller ‘’{0}’’.
Symptoms	None.
Severity	Critical
Category	Controller
Probable Causes	None.
Recommended Actions	None.

GUEST_USER_REMOVED

MIB Name	cLWAGuestUserRemoved
Alarm Condition	Guest user removed.
NCS Message	Guest user ‘’{1}’’ deleted on Controller ‘’{0}’’.
Symptoms	This notification is generated when the lifetime of the guest-user {1} expires and the guest-user's accounts are removed from Controller "{0}".
Severity	Informational
Category	Controller

Probable Causes	None.
Recommended Actions	None.

HEART_BEAT_LOSS

MIB Name	heartbeatLossTrap
Alarm Condition	Heart beat loss
NCS Message	Keepalive messages are lost between Master and Controller''{0}''.
Symptoms	None.
Severity	Major
Category	Controller
Probable Causes	None.
Recommended Actions	None.

IPSEC_ESP_AUTH_FAILURE

MIB Name	bsnIpsecEspAuthFailureTrap
Alarm Condition	IPsec ESP auth failure.
NCS Message	IPsec ESP Authentication failure from remote IP address ''{0}''. Error Count is ''{1}''.
Symptoms	None.
Severity	Minor
Category	Security
Probable Causes	None.
Recommended Actions	None.

IPSEC_ESP_INVALID_SPI

MIB Name	bsnIpsecEspInvalidSpiTrap
Alarm Condition	IPsec ESP invalid SPI
NCS Message	IPsec ESP Invalid SPI from remote IP address ''{0}''. IPsec SPI is ''{1}''.
Symptom	None.
Severity	Minor
Category	Security

Probable Causes	None.
Recommended Actions	None.

IPSEC_ESP_REPLAY_FAILURE

MIB Name	bsnIpsecEspReplayFailureTrap
Alarm Condition	IPsec ESP replay failure.
NCS Message	IPsec ESP Replay failure from remote IP address ''{0}''. Error Count is ''{1}''.
Symptoms	None.
Severity	Minor
Category	Security
Probable Causes	None.
Recommended Actions	None.

IPSEC_SUITE_NEG_FAILURE

MIB Name	bsnIpsecSuiteNegFailure
Alarm Condition	IPsec suite negotiation failure.
NCS Message	IPsec Suite Negotiation failure from remote IP address ''{0}''.
Symptoms	None.
Severity	Minor
Category	Security
Probable Causes	None.
Recommended Actions	None.

INVALID_RADIO

MIB Name	invalidRadioTrap
Alarm Condition	Invalid radio
NCS Message	Radio ''{0}'' with protocol ''{1}'' on controller ''{2}'' has invalid interface. ''{3}''
Symptoms	When the controller detects that a Cisco AP that has joined has unsupported radios, controller generates a trap and it gets propagated as an alert in NCS.
Severity	Critical

Category	Access Point.
Probable Causes	None.
Recommended Actions	None.

LINK_FAILURE

MIB Name	linkFailureTrap
Alarm Condition	Link failure
NCS Message	Link failure. Controller ''{0}''.
Symptoms	None.
Severity	Critical
Category	Controller
Probable Causes	None.
Recommended Actions	None.

MESH_BATTERY

MIB Name	ciscoLwappMeshBatteryAlarm
Alarm Condition	Mesh Battery
NCS Message	MESH ''{0}'' battery status ''{1}''
Symptoms	None.
Severity	Critical
Category	Mesh Links
Probable Causes	None.
Recommended Actions	None.

MESH_DEFAULTBRIDGEGROUPNAME

MIB Name	ciscoLwappMeshDefaultBridgeGroupName
Alarm Condition	Mesh Default Bridge Group Name
NCS Message	MESH ''{0}'' has joined ''{1}'' with default bridge group name
Symptoms	None.
Severity	Major
Category	Mesh Links

Probable Causes	None.
Recommended Actions	None.

MESH_EXCESSIVECHILDREN

MIB Name	ciscoLwappMeshExcessiveChildren
Alarm Condition	Mesh Excessive Children
NCS Message	MESH ''{0}'' has exceeded child count of ''{1}'' for Mesh type ''{2}''.
Symptoms	
Severity	Major
Category	Mesh Links
Probable Causes	None.
Recommended Actions	None.

MESH_EXCESSIVEHOPCOUNT

MIB Name	ciscoLwappMeshExcessiveHopCount
Alarm Condition	Mesh Excessive Hop Count
NCS Message	MESH ''{0}'' number of hops from the MAP node to the RAP exceeds the threshold of ''{1}''
Symptoms	
Severity	Major
Category	Mesh Links
Probable Causes	None.
Recommended Actions	None.

MESH_QUEUEOVERFLOW

MIB Name	ciscoLwappMeshQueueOverflow
NCS Message	MESH ''{0}'' queue overflow peak packets ''{1}'' and packets dropped ''{2}''.
Symptoms	None.
Alarm Condition	Mesh Queue Pkt overflow
Severity	Critical
Category	Mesh Links

Probable Causes	None.
Recommended Actions	None.

MESH_SECBACKHAULCHANGE

MIB Name	ciscoLwappMeshSecBackhaulChange
Alarm Condition	Mesh Secondary Backhaul Change
NCS Message	MESH ''{0}'' changed backhaul from primary to secondary with ''{1}'' and backhaul is ''{2}'' with count ''{3}''.
Symptoms	None.
Severity	Major
Category	Mesh Links
Probable Causes	None.
Recommended Actions	None.

MSTREAM_CLIENT_DLIST

MIB Name	ciscoLwappMediaMCStreamDelistNotif
Alarm Condition	None.
NCS Message	Client ''{0}'' disconnected from the Media Stream with Reason code ''{1}''.
Symptoms	
Severity	Informational
Category	Clients
Probable Causes	None.
Recommended Actions	None.

MSTREAM_CLIENT_FAILURE

MIB Name	ciscoLwappMediaMCStreamFailureNotif
Alarm Condition	None.
NCS Message	Client ''{0}'' failed to get Media Stream with Reason code ''{1}''.
Symptoms	None.
Severity	Information
Category	Clients

Probable Causes	None.
Recommended Actions	None.

MSTREAM_CLIENT_ADMIT

MIB Name	ciscoLwappMediaMCStreamAdmitNotif
Alarm Condition	None.
NCS Message	Client ''{0}'' admitted to Media Stream.
Symptoms	None.
Severity	Informational
Category	Clients
Probable Causes	None.
Recommended Actions	None.

POWER_SUPPLY_CHANGE

MIB Name	powerSupplyStatusChangeTrap
Alarm Condition	Power supply change
Symptoms	None
Category	Controller
Severity	Critical
NCS Message	Power supply status changed. Controller ''{0}''.
Probable Causes	None.
Recommended Actions	None.

RADAR_CHANNEL_DETECTED

MIB Name	bsnRadarChannelDetected
Alarm Condition	Radar channel detected
Symptoms	None.
Category	AP
Severity	Informational
NCS Message	Radar has been detected on channel ''{1}'' by AP ''{0}'' on 5GHz Radio.

Probable Causes	None.
Recommended Actions	None.

RADIOCARD_FAILURE

MIB Name	bsnAPRadioCardRxFailure
Alarm Condition	Radiocard failure.
Symptoms	None.
Category	AP
Severity	Critical
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

RADIO_CURRENT_TXPOWER_CHANGED

MIB Name	bsnAPCurrentTxPowerChanged
Alarm Condition	Radio transmit power level changed.
Symptoms	None.
Category	RRM
Severity	Informational.
NCS Message	Transmit Power changed to ''{2}'' on ''{1}'' interface of AP ''{0}'' connected to Controller ''{3}''.
Probable Causes	None.
Recommended Actions	None.

RRM_GROUPING_DONE

MIB Name	ciscoLwappRrmRfGroupLeaderChange
Alarm Condition	RRM grouping done.
Symptoms	None.
Category	RRM
Severity	Information
NCS Message	RF Group Leader changed for the ''{0}'' network. New Group Leaders MAC address is ''{1}'' IP address is ''{2}'' Radio Type is ''{3}''

Probable Causes	None.
Recommended Actions	None.

SIGNATURE_ATTACK

MIB Name	bsnSignatureAttackDetected
Alarm Condition	Signature attack
Symptoms	None.
Category	Security
Severity	Critical
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

STATION_IOS_DEAUTHENTICATE

MIB Name	dot11Deauthenticate
Alarm Condition	Autonomous AP Client 802.1x authentication failure..
NCS Message	Client "{0}" is de-authenticated from AP "{1}" with reason code "{2}({3})".
Symptoms	This notification is generated by the AP when 802.1x authentication of the client fails.
Severity	Minor & Information (If the error code of the trap is > 13, then the alarms in generated with 'Minor' severity and under 'Security' category. If the error code is <= 12, then the event is generated with 'Information' severity under 'Client' category.).
Category	Clients and Security

Probable Causes	802.1x authentication failure of the client. Error Codes: 0 Reserved 1 Unspecified reason 2 Previous authentication no longer valid 3 Deauthenticated because sending station is leaving (or has left) IBSS or ESS 4 Disassociated due to inactivity 5 Disassociated because AP is unable to handle all currently associated stations 6 Class 2 frame received from nonauthenticated station 7 Class 3 frame received from nonassociated station 8 Disassociated because sending station is leaving (or has left) BSS 9 Station requesting (re)association is not authenticated with respondin 11 Disassociated because the information in the Power Capability element is unacceptable 12 Disassociated because the information in the Supported Channels element is unacceptable 13 Invalid information element 14 MIC failure 15 4-Way Handshake timeout 16 Group Key Handshake timeout 17 Information element in 4-Way Handshake different from (Re)Association Request/Probe 18 Invalid group cipher 19 Invalid pairwise cipher 20 Invalid AKMP 21 Unsupported RSN information element version 22 Invalid RSN information element capabilities 23 IEEE 802.1X authentication failed 24 Cipher suite rejected per security policy
Recommended Actions	Check client configuration for configured keys or passwords.

STATION_IOS_AUTHENTICATION_FAIL

MIB Name	dot11AuthenticateFail
Alarm Condition	Autonomous AP Client 802.11 authentication failure.
NCS Message	Client "{0}" has failed authenticating with AP "{1}". The reason code is "{2}({3})".

Symptoms	This notification is generated by the AP when 802.11 authentication of the client fails.
Severity	Informational.
Category	Clients
Probable Causes	802.11 Authentication failure of the client.
Recommended Actions	Check client configuration for configured keys or passwords.

STATION_WIRED_CHANGED

MIB Name	cmnMacChangedNotifications
Alarm Condition	MAC Address table notification trap.
NCS Message	Wired Client {0} {1} from Switch {2}
Symptoms	A MAC address table change on the switch.
Severity	Informational
Category	Clients.
Probable Causes	Switch detected a change in MAC address table.
Recommended Actions	None.

STP_NEWROOT

MIB Name	stpInstanceNewRootTrap.
Alarm Condition	STP newroot.
NCS Message	Controller "{0}". Spanning Tree Protocol Instance Root changed for VLAN ID "{1}".
Symptoms	This notification is generated by the AP when 802.11 authentication of the client fails.
Severity	Informational.
Category	Controller
Probable Causes	Failed Client authentication.
Recommended Actions	Check client configuration for configured keys or passwords.

TEMP_MOBILITY_ANCHOR_CTRL_PATH_DOWN

MIB Name	ciscoTempLwappMobilityAnchorControlPathDown
Alarm Condition	Mobility anchor control path down.

NCS Message	Controller ''{0}''. Control path on anchor ''{1}'' is down.
Symptoms	None.
Severity	Major
Category	Controller
Probable Causes	None.
Recommended Actions	None.

TEMP_MOBILITY_ANCHOR_DATA_PATH_DOWN

MIB Name	ciscoTempLwappMobilityAnchorDataPathDown
Alarm Condition	Mobility anchor data path down
NCS Message	Controller ''{0}''. Data path on anchor ''{1}'' is down.
Symptoms	None.
Severity	Major
Category	Controller
Probable Causes	None.
Recommended Actions	None.

TEMP_WLAN_ALL_ANCHORS_TRAP_DOWN

MIB Name	ciscoTempLwappMobilityAllAnchorsOnWlanDown
Alarm Condition	Mobility anchors down (Temp).
NCS Message	Controller ''{0}''. Data path on anchor ''{1}'' is down.
Symptoms	None.
Severity	Major
Category	Controller
Probable Causes	None.
Recommended Actions	None.

VOICE_COVERAGE_HOLE_ALARM

MIB Name	ciscoLwappDot11ClientCoverageHolePreAlarm
Alarm Condition	Voice coverage hole detected.
Symptoms	None.

Category	Coverage Hole
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

WLC_SCHEDULED_RESET

MIB Name	ciscoLwappScheduledResetNotif
Alarm Condition	None.
Symptoms	None.
Category	Controller
Severity	Informational
NCS Message	Controller ‘’{0}’’ is going to be reboot in {1} seconds.The reboot has been triggered from WLC CLI or Web Interface.
Probable Causes	None.
Recommended Actions	None.

Switch Traps

The following are the Switch traps added in NCS 1.0:

COLD_START (FROM MIB-II STANDARD)

MIB Name	coldStart.
Alarm Condition	Cold start trap from controller.
NCS Message	Cold start. Switch "{0}."
Symptoms	The switch is reinitializing itself and that its configuration may have been altered.
Severity	Informational.
Category	Controller

Probable Causes	• The switch (controller) has power-cycled. • The switch (controller) went through a hard reset. • The switch (controller) went through a software restart.
Recommended Actions	Power recycled; Software reset.

LINK_DOWN (FROM MIB-II STANDARD)

MIB Name	linkDown.
Alarm Condition	Interface state change.
NCS Message	Port "{0}" is down on Switch "{1}."
Symptoms	The physical link on one of the switch (controller) ports is down.
Severity	Critical.
Category	Switch.
Probable Causes	A communication link to the port is disconnected.
Recommended Actions	None.

LINK_UP (FROM MIB-II STANDARD)

MIB Name	linkUp.
Alarm Condition	Interface state change.
NCS Message	Port "{0}" is up on Switch "{1}."
Symptoms	A previously down link on a switch port is up now.
Severity	Clear.
Category	Switch
Probable Causes	A communication link has been restored to the port.
Recommended Actions	None.

SWT_AUTH_FAIL

MIB Name	authenticationFailure
Alarm Condition	Authentication failed.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch ‘’{0}’’. Authentication failed.

Probable Causes	None.
Recommended Actions	None.

SWT_CAEM_TEMPERATURE

MIB Name	caemTemperatureNotification
Alarm Condition	Over temperature Alarm Condition is detected in the managed system.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Over temperature Alarm Condition is detected in the managed system.
Probable Causes	None.
Recommended Actions	None.

SWT_CAEM_VOLTAGE

MIB Name	caemVoltageNotification
Alarm Condition	Over voltage Alarm Condition is detected in the managed system.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch ''{0}''. Over voltage Alarm Condition is detected in the managed system.
Probable Causes	None.
Recommended Actions	None.

SWT_CDER_MON_EXCEPTION

MIB Name	cderMonitoredExceptionEvent
Alarm Condition	An exception is detected on the managed device.
Symptoms	None.
Category	Switch
Severity	Informational
NCS Message	Switch ''{0}''. An exception is detected on the managed device.

Probable Causes	None.
Recommended Actions	None.

SWT_CEFC_STATUS_CHANGE

MIB Name	cefcModuleStatusChange
Alarm Condition	CEFC Module status change.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	CEFC module state changed to ''{0}''. sysUpTime=''{1}''.
Probable Causes	None.
Recommended Actions	None.

SWT_CEV_FANONS15540_FAN_TRAY8

MIB Name	cevFanONS15540FanTray8
Alarm Condition	cevFanONS15540FanTray8 Notification.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. cevFanONS15540FanTray8 Notification
Probable Causes	None.
Recommended Actions	None.

SWT_CEV_PORT_TRANSPARENT

MIB Name	cevPortTransparent
Alarm Condition	cevPortTransparent Notification
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. cevPortTransparent Notification

Probable Causes	None.
Recommended Actions	None.

SWT_CEV_PORT_WAVE

MIB Name	cevPortWave
Alarm Condition	cevPortWave Notification
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. cevPortWave Notification
Probable Causes	None.
Recommended Actions	None.

SWT_CONFIG_MAN_EVENT

MIB Name	ciscoConfigManEvent
Alarm Condition	Configuration management event has been recorded in ccmHistoryEventTable.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Configuration management event has been recorded in ccmHistoryEventTable.
Probable Causes	None.
Recommended Actions	None.

SWT_CONTENT_ENGINE_OVERLOAD

MIB Name	ciscoContentEngineOverloadBypass
Alarm Condition	A high watermark of percentage of capacity for transparent requests redirect.
Symptoms	None.
Category	Switch
Severity	Major

NCS Message	Switch ''{0}''. A high watermark of percentage of capacity for transparent requests redirected to the Content Engine via WCCP (Web Cache Control Protocol) has been reached. Subsequent WCCP requests are rejected and forwarded to the Origin Server until the utilization falls below a low watermarker.
Probable Causes	None.
Recommended Actions	None.

SWT_CONTENT_ENGINE_WRITE_FAILED

MIB Name	ciscoContentEngineWriteTransFailed
Alarm Condition	Failed writing to working transaction log located in /local1/working.lo.
Symptoms	None.
Category	Switch
Severity	Critical
NCS Message	Switch ''{0}''. Failed writing to working transaction log located in /local1/working.lo
Probable Causes	None.
Recommended Actions	None.

SWT_CVPDN_SESSION

MIB Name	cvpdnNotifSession
Alarm Condition	L2X session with the indicated session ID and Xconnect VCID.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. L2X session with the indicated session ID and Xconnect VCID.
Probable Causes	None.
Recommended Actions	None.

SWT_DMD_NBRLAYER2_CHANGE

MIB Name	demandNbrLayer2Change
Alarm Condition	D-Channel interface status change.
Symptoms	None.

Category	Switch
Severity	Major
NCS Message	D-channel of interface ‘’{0}’’ state changed to ‘’{1}’’.
Probable Causes	None.
Recommended Actions	None.

SWT_ENV_MON_SHUTDOWN

MIB Name	ciscoEnvMonShutdownNotification
Alarm Condition	Environmental monitor detects a testpoint reaching a critical state.
NCS Message	Switch ‘’{0}’’. Environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown.
Symptoms	None.
Severity	Informational.
Category	Switch
Probable Causes	None.
Recommended Actions	None.

SWT_GROUP_CHANGE

MIB Name	rptrGroupChange
Alarm Condition	Group structure of repeater has changed.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ‘’{0}’’. Group structure of repeater has changed.
Probable Causes	None.
Recommended Actions	None.

SWT_IP_PERMIT_DENIED

MIB Name	ipPermitDeniedTrap
Alarm Condition	None.
NCS Message	Switch "{0}". IP permit denied access.
Symptoms	None.

Severity	Informational.
Category	Switch
Probable Causes	None.
Recommended Actions	None.

SWT_LER_ALARM_ON

MIB Name	lerAlarmOn
Alarm Condition	None.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch "{0}". LER has transitioned true state.
Probable Causes	None.
Recommended Actions	None.

SWT_LS1010_CHASSIS_CHANGE

MIB Name	ciscoLS1010ChassisChangeNotification
Alarm Condition	Cisco LS1010: Detected hot-swap component or changes in the chassis.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ‘’{0}’’. Cisco LS1010: Detected hot-swap component or changes in the chassis
Probable Causes	None.
Recommended Actions	None.

SWT_LS1010_CHASSIS_FAILURE

MIB Name	ciscoLS1010ChassisFailureNotification
Alarm Condition	Cisco LS1010: Change in the status of ps0 ps1 fan 12V line and/or chassis temperature.
Symptoms	None.
Category	Switch

Severity	Critical
NCS Message	Switch ‘’{0}’’. Cisco LS1010: Change in the status of ps0 ps1 fan 12V line and/or chassis temperature.
Probable Causes	None.
Recommended Actions	None.

SWT_MODULE_DOWN

MIB Name	CISCO-STACK-MIB moduleDown
Alarm Condition	None.
NCS Message	Module "{0}" is down on Switch "{1}".
Symptoms	The module is changing state from OK.
Severity	Critical
Category	Switch
Probable Causes	None.
Recommended Actions	None.

SWT_MODULE_UP

MIB Name	CISCO-STACK-MIB moduleUp
Alarm Condition	None.
NCS Message	Module "{0}" is down on Switch "{1}".
Symptoms	The module is changing state from OK.
Severity	Clear
Category	Switch
Probable Causes	None.
Recommended Actions	None.

SWT_PETH_POWER_USAGE_OFF

MIB Name	pethMainPowerUsageOffNotification
Alarm Condition	PSE Threshold usage indication is off the usage power is below the threshold
Symptoms	None.
Category	Switch
Severity	Major

NCS Message	Switch ''{0}''. PSE Threshold usage indication is off the usage power is below the threshold.
Probable Causes	None.
Recommended Actions	None.

SWT_PETH_POWER_USAGE_ON

MIB Name	pethMainPowerUsageOnNotification
Alarm Condition	PSE Threshold usage indication is on the usage power is above the threshold.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. PSE Threshold usage indication is on the usage power is above the threshold.
Probable Causes	None.
Recommended Actions	None.

SWT_PETH_PSE_PORT_STATUS

MIB Name	pethPsePortDetectionStatus
Alarm Condition	The operational status of the port PD has changed.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. The operational status of the port PD has changed.
Probable Causes	None.
Recommended Actions	None.

SWT_RESET_EVENT

MIB Name	rptrResetEvent
Alarm Condition	A repeater reset has completed.
Symptoms	None
Category	Switch
Severity	Information

NCS Message	Switch ''{0}''. A repeater reset has completed.
Probable Causes	None.
Recommended Actions	None.

SWT_RPTR_HEALTH

MIB Name	rptrHealth
Alarm Condition	Repeater (RPTR) status has changes or a non-disruptive test has completed
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch ''{0}''. Repeater (RPTR) status has changes or a non-disruptive test has completed.
Probable Causes	None.
Recommended Actions	None.

SWT_RTT_MON_CONN_CHANGE

MIB Name	rttMonConnectionChangeNotification
Alarm Condition	Connection to a target has either failed on establishment.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Connection to a target (not to a hop along the path to a target) has either failed on establishment or been lost and when reestablished.
Probable Causes	None.
Recommended Actions	None.

SWT_RTT_MON_NOTE

MIB Name	rttMonNotification
Alarm Condition	Threshold violation occurs during an operation to the target.
Symptoms	None.
Category	Switch
Severity	Major

NCS Message	Switch ''{0}''. Threshold violation occurs during an operation to the target and not to a hop along the path to the target.
Probable Causes	None.
Recommended Actions	None.

SWT_RTT_MON_THRESHOLD

MIB Name	rttMonThresholdNotification
Alarm Condition	Threshold violation for an RTT operation occurred and subsided.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. Threshold violation for an RTT operation occurred and subsided.
Probable Causes	None.
Recommended Actions	None.

SWT_RTT_MON_TIMEOUT

MIB Name	rttMonTimeoutNotification
Alarm Condition	Timeout for an RTT operation occurred and cleared.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Timeout for an RTT operation occurred and cleared.
Probable Causes	None.
Recommended Actions	None.

SWT_RTT_MON_VERIFY_ERROR

MIB Name	rttMonVerifyErrorNotification
Alarm Condition	Data corruption in an RTT operation has occurred.
Symptoms	None.
Category	Switch
Severity	Information

NCS Message	Switch ''{0}''. Data corruption in an RTT operation has occurred.
Probable Causes	None.
Recommended Actions	None.

SWT_STP_NEW_ROOT

MIB Name	STPnewRoot
Alarm Condition	Sending agent has become the new root of the Spanning Tree.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. Sending agent has become the new root of the Spanning Tree
Probable Causes	None.
Recommended Actions	None.

SWT_STP_TOPOLOGY_CHANGE

MIB Name	STPtopologyChange
Alarm Condition	A port transitions from Learning state to Forwarding state.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch ''{0}''. A port transitions from Learning state to Forwarding state or from Forwarding state to Blocking state.
Probable Causes	None.
Recommended Actions	None.

SWT_SWT_LER_ALARM_OFF

MIB Name	lerAlarmOff
Alarm Condition	None.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch "{0}". LER has transitioned false state.
Probable Causes	None.
Recommended Actions	None.

SWT_SYS_CONFIG_CHANGE

MIB Name	sysConfigChangeTrap
Alarm Condition	System configuration in NVRAM is changed.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ‘’{0}’’. System configuration in NVRAM is changed
Probable Causes	None.
Recommended Actions	None.

SWT_VLAN_TRAUNK_PORT_DYN_STATUS

MIB Name	vlanTrunkPortDynamicStatusChange
Alarm Condition	The value of vlanTrunkPortDynamicStatus object has been changed.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ‘’{0}’’. The value of vlanTrunkPortDynamicStatus object has been changed.
Probable Causes	None.
Recommended Actions	None.

SWT_VM_VMPS_CHANGE

MIB Name	vmVmpsChange
Alarm Condition	Current VMPS has changed since last system re-initialization
Symptoms	None
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. Current VMPS has changed since last system re-initialization. The current VMPS is changed whenever the VMPS fails to response after vmVmpsRetries of a VQP request.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_CONFIG_DIGEST_ERROR

MIB Name	vtpConfigDigestError
Alarm Condition	Configuration digest error occurred. The device received a VTP advertisement.
Symptoms	None
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Configuration digest error occurred. The device received a VTP advertisement.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_CONFIG_REV_NUMBER

MIB Name	vtpConfigRevNumberError
Alarm Condition	Configuration revision number error has occurred.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Configuration revision number error has occurred.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_MTU_TOO_BIG

MIB Name	vtpMtuTooBig
Alarm Condition	VLAN's MTU size is larger than can be supported trunk ports
Symptoms	None
Category	Switch
Severity	Minor
NCS Message	Switch ''{0}''. VLAN's MTU size is larger than can be supported trunk ports.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_SERVER_DIABLED

MIB Name	vtpServerDisabled
Alarm Condition	Local server is no longer able to function as a VTP Server.
Symptoms	None
Category	Switch
Severity	Minor
NCS Message	Switch ''{0}''. Local server is no longer able to function as a VTP Server. The number of defined VLANs is greater than vtpMaxVlanStorage.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_VER1_DEV_DETECTED

MIB Name	vtpVersioNone.DeviceDetected
Alarm Condition	VTP version one device detected.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. VTP version one device detected that a management domain has been put into version 2 mode and 15 minutes has passed.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_VLAN_RING_NUM_CONFLICT

MIB Name	vtpVlanRingNumberConflict
Alarm Condition	Conflict between the ring number and the VTP-obtained ring number.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch ‘’{0}’’. Conflict between the ring number and the VTP-obtained ring number.
Probable Causes	None.
Recommended Actions	None.

WARM_START

MIB Name	None.
Alarm Condition	Warm start trap from controller
NCS Message	Warm start. Switch "{0}".
Category	Switch
Symptoms	The switch is reinitializing itself such that its configuration is unaltered.
Severity	Informational
Probable Causes	Reboot was issued.
Recommended Actions	None.

Alarms Raised Through Polling

This section lists those traps that are raised through polling and contains the following topics:

AP_DETECTED_DUPLICATE_IP

MIB Name	bsnDuplicateIpAddressReported.
Alarm Condition	AP Detected Duplicate IP.
NCS Message	AP "{0}" on Switch "{3}" detected duplicate IP address "{2}" being used by machine with mac address "{1}."
Symptoms	The system detects a duplicate IP address in the network that matches that assigned to an access point.
Severity	Critical.
Category	Security
Probable Causes	Another device in the network is configured with the same IP address as an access point.
Recommended Actions	Correct the misconfiguration of IP addresses in the network.

AUTHMGR-5-SUCCESS

MIB Name	AUTHMGR-5-SUCCESS
Alarm Condition	Wired client authorization success.
NCS Message	Authorization succeeded for client (%s) on Interface %s AuditSessionID %s
Symptoms	Authorization was successful.
Severity	Informational.
Category	Clients.
Probable Causes	Authorization was successful.
Recommended Actions	None.

AUTHMGR-5-FAIL

Syslog Name	AUTHMGR-5-FAIL
Alarm Condition	Wired client authorization failure.
NCS Message	Authorization failed or unapplied for client (%s) on Interface %s AuditSessionID %s
Symptoms	Authorization was unsuccessful.
Severity	Informational.
Category	Clients
Probable Causes	Authorization was unsuccessful.
Recommended Actions	None.

AUTHMGR-5-SECURITY_VIOLATION

Alarm Condition	Security violation on an Interface.
NCS Message	Security violation on the interface %s new MAC address (%e) is seen.AuditSessionID %s.
Symptoms	Security violation on an interface.
Category	Clients
Severity	Minor
Probable Causes	A host on the specified interface is attempting to gain access into the network or is trying to authenticate in a host mode that does not support the number of hosts attached. This is treated as a security violation and the port has been error-disabled.
Recommended Actions	Ensure that the port is configured to support the number of hosts attached. Enter the shutdown command followed by no shutdown command to restart the port.

DOT1X-5-SUCCESS

MIB Name	None.
Alarm Condition	Wired client 802.1X authentication success.
NCS Message	802.1X:Authentication was successful for client %s on Interface %s.
Symptoms	Authentication was successful.
Severity	Informational
Category	Clients
Probable Causes	Authentication was successful.
Recommended Actions	None.

DOT1X-5-FAIL

Alarm Condition	Wired client 802.1X authentication failure.
NCS Message	802.1X:Authentication failed for client %s on Interface %s.
Symptoms	Authentication was unsuccessful.
Severity	Informational
Category	Clients
Probable Causes	Authentication was unsuccessful.
Recommended Actions	None.

AP_DISASSOCIATED_MAINTENANCE

MIB Name	None.
Alarm Condition	None.
Category	Access Point.
Severity	Minor
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

CPM_UNREACHABLE

MIB Name	None.
Alarm Condition	Identity Services Engine down.
NCS Message	Identity Services Engine "{0}" is unreachable.
Symptoms	Identity Services Engine is not reachable by NCS.
Severity	Major
Category	ISE
Probable Causes	Identity Services Engine is down or there is a network issue.
Recommended Actions	Check the status of Identity Services Engine.

IOSAP_ADMIN_DOWN

MIB Name	None.
Alarm Condition	Autonomous AP Admin Status Down

Category	Access Point.
Severity	Major
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

IOSAP_DOWN

MIB Name	None.
Alarm Condition	Autonomous AP Oper Status Down.
NCS Message	Autonomous AP "{0}" is unreachable.
Symptoms	The autonomous AP is SNMP unreachable.
Severity	Critical.
Category	Access Point.
Probable Causes	• Network connectivity to the autonomous access point is broken. • Ethernet port of the autonomous access point is down. • SNMP agent is not running in the autonomous access point. • SNMP credentials on the NCS do not match the SNMP credentials configured on the autonomous access point. • SNMP version on the NCS does not match the SNMP version configured on the autonomous access point.
Recommended Actions	First, check the IP connectivity to the access point. Next, check the port status of the access point. Finally, check SNMP credentials on both the NCS and the access point.

NCS_VERY_LOW_DISK_SPACE

MIB Name	None.
Alarm Condition	NCS very low memory.
NCS Message	NCS have very low disk space.
Symptoms	NCS disk space meets requirement.
Severity	Critical.
Category	NCS
Probable Causes	Not enough disk space left on NCS server.
Recommended Actions	Free some disk space.

NCS_LOW_MEMORY

MIB Name	None.
Alarm Condition	NCS low memory.
NCS Message	NCS has low memory.
Symptoms	NCS server performance might be degrading.
Severity	Major.
Category	NCS
Probable Causes	NCS has low memory.
Recommended Actions	Free up memory if possible.

NCS_CLIENT_TRAP_DISABLED

MIB Name	None.
Alarm Condition	Client Traps are disabled on controllers.
NCS Message	Client traps are disabled on controller(s) {0}.
Symptoms	This notification is generated by NCS when required client traps are disabled in one or more controllers. These traps are needed for NCS to detect client sessions in a timely and efficient manner. The required traps are: • 802.11 Association • 802.11 Disassociation • 802.11 Authentication • 802.11 Deauthentication • 802.11 Failed Association • 802.11 Failed Authentication
Severity	Minor.
Category	NCS
Probable Causes	When a controller is added to NCS, NCS enables the required client traps. If NCS does not have the correct SNMP read-write community, it could fail. The trap controls can also be changed by pushing the SNMP trap control template or using controller GUI/CLI.
Recommended Actions	Use the NCS template to enable the required client traps on the controller list.

AUTHMGR-5-START

MIB Name	None.
Alarm Condition	Start of wired client authentication.
NCS Message	Starting ‘%s’ for client (%s) on Interface %s AuditSessionID %s
Symptoms	Starting an authentication method.

Severity	Informational.
Category	Clients.
Probable Causes	Starting an authentication method.
Recommended Actions	None.

AUTHMGR-5-FAIL

MIB Name	None.
Alarm Condition	Wired client authorization failure.
Category	Clients
Severity	Informational
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

AUTHMGR-5-SECURITY_VIOLATION

MIB Name	None.
Alarm Condition	Security violation on an Interface.
Category	Clients
Severity	Minor
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

AUTHMGR-5-START

MIB Name	None.
Alarm Condition	Start of wired client authentication.
Category	Clients
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

AUTHMGR-5-SUCCESS

MIB Name	None.
Alarm Condition	Wired client authorization success.
Category	Clients
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

AUTHMGR-SP-5-VLANASSIGN

MIB Name	None.
Alarm Condition	Wired Client critical VLAN assigned. Wired Client auth fail VLAN assigned. Vlan assignment as authorization policy. Wired Client guest VLAN assigned.
NCS Message	VLAN XXX assigned to Interface GiX/Y
Symptoms	VLAN assigned to an interface.
Severity	Informational
Category	Wired Clients
Probable Causes	VLAN assigned to an interface.
Recommended Actions	None.

APPLIANCE_FAN_BACK_TO_NORMAL

MIB Name	None.
Alarm Condition	Appliance fan error has cleared.
NCS Message	Fan is back to normal
Symptoms	A failure is no longer detected in the appliance fans.
Severity	Clear.
Category	NCS
Probable Causes	None.
Recommended Actions	None.

APPLIANCE_FAN_BAD_OR_MISSING

MIB Name	None.
Alarm Condition	A failure has been detected in the appliance fans.
NCS Message	Fan is either bad or missing.
Symptoms	A failure has been detected in the appliance fans.
Severity	Major.
Category	NCS
Probable Causes	A fan has failed.
Recommended Actions	Contact Technical Support.

APPLIANCE_POWER_SUPPLY_BACK_TO_NORMAL

MIB Name	None.
Alarm Condition	None.
NCS Message	Power supply is back to normal.
Symptoms	Power supply is back to normal.
Severity	Clear
Category	NCS
Probable Causes	None.
Recommended Actions	None.

APPLIANCE_POWER_SUPPLY_BAD_OR_MISSING

MIB Name	None.
Alarm Condition	None.
NCS Message	Power supply is is either bad or missing.
Symptoms	Power supply is either bad or missing.
Severity	Major
Category	NCS
Probable Causes	Power supply is is either bad or missing.
Recommended Actions	Replace bad or missing power supply.

APPLIANCE_RAID_BACK_TO_NORMAL

MIB Name	None.
Alarm Condition	None.
Symptoms	None.
Severity	Clear
NCS Message	RAID array in good health.
Category	Switch
Probable Causes	None.
Recommended Actions	None.

APPLIANCE_RAID_BAD_OR_MISSING

MIB Name	None.
Alarm Condition	None.
NCS Message	Drive "${0}" is missing or bad.
Symptoms	Disk or RAID failure.
Severity	Major
Category	NCS
Probable Causes	Disk or RAID failure.
Recommended Actions	Contact Technical Support. Replace failed drive.

APPLIANCE_TEMP_BACK_TO_NORMAL

MIB Name	None.
Alarm Condition	None.
NCS Message	Both CPU temperatures are OK.
Symptoms	None.
Severity	Clear
Category	Switch
Probable Causes	None.
Recommended Actions	None.

APPLIANCE_TEMP_EXCEED_UPPER_LIMIT

MIB Name	None.
Alarm Condition	None.
NCS Message	Appliance temperature exceeds upper limit.
Symptoms	None.
Severity	Major
Category	NCS
Probable Causes	None.
Recommended Actions	Contact Technical Support.

AUDIT_STATUS_DIFFERENCE

MIB Name	None.
Alarm Condition	Audit status difference.
NCS Message	Switch "{0}" Audit done at "(1)." Config differences found between NCS and controller.
Symptoms	This notification is generated by NCS when audit differences are detected while auditing a controller during a network audit background task or per controller audit.
Severity	Minor.
Category	NCS
Probable Causes	The NCS and controller configuration are not synchronized.
Recommended Actions	Refresh the configuration from the controller so that it synchronizes with the controller configuration on NCS.

CONFIG_BACKUP_FAILED

MIB Name	None.
Alarm Condition	Configuration backup failed.
Category	Controller
Severity	Warning
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

CONFIG_BACKUP_SUCCEEDED

MIB Name	None.
Alarm Condition	Configuration backup succeeded.
Category	Controller
Severity	Informational
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

COLD_START (FROM MIB-II STANDARD)

MIB Name	coldStart.
Alarm Condition	Cold start trap from controller.
NCS Message	Switch "{0}." Cold start.
Symptoms	The switch (controller) went through a reboot.
Severity	Informational.
Category	Controller
Probable Causes	• The switch (controller) has power-cycled. • The switch (controller) went through a hard reset. • The switch (controller) went through a software restart.
Recommended Actions	Power recycled; Software reset.

CONFIGAUDITSET_ENFORCEMENT_FAIL

MIB Name	None.
Alarm Condition	Enforcement on config group failed.
NCS Message	Failed to enforce Config Group “0” on controllers “1.”
Symptoms	This notification is generated by NCS during network audit when some failures are encountered during enforcement of the templates from the config groups (which as opted to be enforced).
Severity	Critical.
Category	NCS
Probable Causes	The config group (which are opted to be enforced) templates are not in sync with the device values.
Recommended Actions	Look at the controller audit report for the list of enforced values and for the failed enforcements. An alarm is cleared upon successful enforcements during the next network audit cycle.

CONFIGAUDITSET_ENFORCEMENT_SUCCESS

MIB Name	None.
Alarm Condition	Enforcement on config group succeeded.
NCS Message	Successfully enforced Config Group “0” on controllers “1.”
Symptoms	This notification is generated by NCS during network audit when all the templates from the config group (which are opted to be enforced) are successfully enforced.
Severity	Minor.
Category	NCS
Probable Causes	The config group (which are opted to be enforced) templates are not in sync with the device values.
Recommended Actions	Look at the controller audit report for the list of enforced values. An alarm is cleared when no enforcements are found during the next network audit cycle.

CONFIG_SAVED

MIB Name	bsnConfigSaved.
Alarm Condition	Configuration saved.
NCS Message	Switch "{0}.” Configuration saved in flash.
Symptoms	A configuration save to flash is performed on the switch (controller).
Severity	Informational.
Category	Controller.
Probable Causes	The switch (controller) saves the configuration to the flash via a CLI command or entry via the controller GUI or NCS.
Recommended Actions	If you change the configuration using the controller CLI or controller GUI, you may need to refresh the configuration.

CPM_REACHABLE

MIB Name	None.
Alarm Condition	Identity Services Engine reachable
NCS Message	Identity Services Engine "{0}" is reachable.
Symptoms	Identity Services Engine is reachable by NCS.
Severity	Clear.
Category	ISE
Probable Causes	Clear alarm for CPM_UNREACHABLE.
Recommended Actions	None.

DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND

MIB Name	None.
Alarm Condition	Authorization vlan not found on switch.
NCS Message	Attempt to assign non-existent or shutdown VLAN %s to 802.1x port %s AuditSessionID %s
Symptoms	”An attempt was made to assign a VLAN to an 802.1x port but the VLAN was not found in the VTP database.”.
Severity	Informational
Category	Clients
Probable Causes	”An attempt was made to assign a VLAN to an 802.1x port but the VLAN was not found in the VTP database.”
Recommended Actions	Make sure the VLAN exists and is not shut-down or use another VLAN.

DOT1X-5-FAIL

MIB Name	None.
Alarm Condition	Wired client 802.1X authentication failure.
Category	Clients
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

DOT1X-5-SUCCESS

MIB Name	None.
Alarm Condition	Wired client 802.1X authentication success.
Category	Clients
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

DBADMIN_PASSWORD_RESET

MIB Name	None.
Alarm Condition	None.
NCS Message	DBAdmin password has been changed.
Symptoms	DBAdmin password has been changed.
Severity	Informational
Category	NCS
Probable Causes	Clear alarm for DBADMIN_PASSWORD_RESET_FAILED_ALERT.
Recommended Actions	None.

DBADMIN_PASSWORD_RESET_FAILED

MIB Name	None.
Alarm Condition	DBAdmin password reset failed.
NCS Message	DBAdmin password reset has failed.
Symptoms	DBAdmin password could not be reset.
Severity	Major
Category	NCS
Probable Causes	There is probably some issues with the database.
Recommended Actions	None.

DBADMIN_PASSWORD_RESET_FAILED_ALERTi

MIB Name	None.
Alarm Condition	None..
NCS Message	DBAdmin password reset failed.
Symptoms	DBAdmin password could not be reset.
Severity	Major
Category	NCS
Probable Causes	There is probably some issues with the database.
Recommended Actions	Contact system administrator.

EPM-4-POLICY_APP_FAILURE

MIB Name	None.
Alarm Condition	Failure in applying security policy for a wired client.
NCS Message	IP=%i| MAC=%e| AUDITSESID=%s| AUTHTYPE=%s| POLICY_TYPE=%s| POLICY_NAME=%s| RESULT=FAILURE| REASON=%s
Symptoms	The displayed policy for the client could not be applied by the policy enforcement module (PEM) for the reason indicated in the message.
Severity	Informational
Category	Clients
Probable Causes	The displayed policy for the client could not be applied by the Policy Enforcement Module (EPM) for the reason indicated in the message.
Recommended Actions	Take appropriate action based the failure reason indicated in the message.

EPM-6-POLICY_APP_SUCCESS

MIB Name	None.
Alarm Condition	Success in applying security policy for a wired client.
NCS Message	IP=%i| MAC=%e| AUDITSESID=%s| AUTHTYPE=%s| POLICY_TYPE=%s| POLICY_NAME=%s| RESULT=SUCCESS
Symptoms	The displayed policy for the client has been applied successfully by the EPM.
Severity	Informational/Clear
Category	Clients
Probable Causes	The displayed policy for the client has been applied successfully by the EPM.
Recommended Actions	None.

HM_CONFIGURATION

MIB Name	None.
Alarm Condition	NCS failed HA configuration.
NCS Message	NCS failed HA configuration.
Symptoms	NCS failed on HA configuration.
Severity	Major
Category	NCS
Probable Causes	HA setup might be wrong.
Recommended Actions	Check HA setup.

HM_DATABASE_CRITICAL

MIB Name	ciscoWirelessMOStatusNotification
Alarm Condition	NCS database is down.
NCS Message	Database is down, trying to restart.
Symptoms	NCS database is down.
Severity	Critical
Category	NCS
Probable Causes	The database is down and cannot be started by HM.
Recommended Actions	Check server.

HM_DATABASE

MIB Name	ciscoWirelessMOStatusNotification
Alarm Condition	NCS primary lost connection to the secondary.
NCS Message	NCS lost connection with the other server..
Symptoms	NCS lost connection with the other server..
Severity	Major
Category	NCS
Probable Causes	At the Database level, the connection between primary and secondary is lost. The server probably rebooted or shutdown.
Recommended Actions	Check server and network connections.

HM_FAILOVER

MIB Name	ciscoWirelessMOStatusNotification.
Alarm Condition	NCS failover attempted and failed.
NCS Message	NCS failover attempted and failed.
Symptoms	NCS could not perform failover.
Severity	Major
Category	NCS
Probable Causes	Unknown.
Recommended Actions	Check server and network connections.

HM_FAILBACK

MIB Name	ciscoWirelessMOStatusNotification
Alarm Condition	NCS failback attempted and failed.
NCS Message	NCS failback attempted and failed.
Symptoms	NCS could not perform failback.
Severity	Major
Category	NCS
Probable Causes	Unknown.
Recommended Actions	Check server and network connections.

HM_REACHABILITY

MIB Name	None.
Alarm Condition	NCS primary and Secondary cannot reach each other.
NCS Message	NCS servers cannot reach each other.
Symptoms	NCS servers cannot reach each other.
Severity	Major
Category	NCS
Probable Causes	HA setup/configuration might be wrong. Servers may have also rebooted or shutdown.
Recommended Actions	Check HA setup/configuration.

HM_REGISTRATION

MIB Name	None.
Alarm Condition	NCS failed HA registration.
NCS Message	NCS failed HA registration.
Symptoms	NCS failed on HA registration.
Severity	Major
Category	NCS
Probable Causes	HA configuration might be wrong.
Recommended Actions	Check HA configuration.

IOSAP_LINK_DOWN

MIB Name	linkDown
Alarm Condition	Autonomous AP Link Down.
NCS Message	Autonomous AP "{0}," Interface "{1}" is {2} down.
Symptoms	The physical link is down on an autonomous access point radio port.
Severity	Critical.
Category	Access Point.
Probable Causes	The radio port of an autonomous access point was disabled manually or a port failure occurred.
Recommended Actions	Check the administrative status of the port. If the port administrative status is not down, check other port settings.

IPSEC_ESP_POLICY_FAILURE

MIB Name	None.
Alarm Condition	IPsec ESP policy failure
Category	Security
Severity	Minor
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

IPSEC_OTHER_POLICY_FAILURE

MIB Name	None.
Alarm Condition	IPsec other policy failure
Category	Security
Severity	Minor
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

LICENSE_VIOLATION

MIB Name	None.
Alarm Condition	License violation
Category	NCS
Severity	Critical
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

LOC_SENSOR_UP

MIB Name	None.
Alarm Condition	None.
NCS Message	None.
Symptoms	
Severity	Minor
Category	None.
Probable Causes	None.
Recommended Actions	None.

LINK-3-UPDOWN

MIB Name	None.
Alarm Condition	Interface state change.
NCS Message	Interface %s, changed state to up/down.
Symptoms	None.
Severity	Informational
Category	Clients
Probable Causes	None.
Recommended Actions	None.

LOCATION_SENSOR_DOWN

MIB Name	None.
Alarm Condition	WiFi TDOA Receiver down
Category	Mobility Service
Symptoms	This alarm is generated when a TDOA Receiver is detected to be down by Aeroscout Engine running on MSE.
Severity	Minor
NCS Message	WiFi TDOA Receiver <MacAddress> <Name> is Down.
Probable Causes	TDOA Receiver is down.
Recommended Actions	Check if TDOA Receiver is physically down or contact Aeroscout support.

LOCATION_SERVER_DOWN

MIB Name	None.
Alarm Condition	MSE down
Category	Mobility Service
Severity	Critical
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

LOCATION_SERVER_LIMIT

MIB Name	None.
Alarm Condition	MSE limit reached
Category	Mobility Service
Severity	Major
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

LOCATION_SERVER_OUT_OF_SYNC

MIB Name	None.
Alarm Condition	Mobility Service out of sync.
Category	Mobility Service
Severity	Minor
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

LWAPP_AP_IF_DOWN_FC

MIB Name	None.
Alarm Condition	None.
Severity	Critical
NCS Message	None.
Category	Access Point.
Probable Causes	None.
Recommended Actions	None.

LWAPP_AP_IF_DOWN_RC

MIB Name	None.
Alarm Condition	None.
Severity	Informational.
NCS Message	None.
Category	Access Point.
Probable Causes	None.
Recommended Actions	None.

MSE_LICENSING

MIB Name	None.
Alarm Condition	MSE Licensing

Category	Mobility Service
Severity	Minor
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

MSE_NOTIFY

MIB Name	None.
Alarm Condition	MSE Notification
Category	Mobility Service
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

MSE_UPGRADE

MIB Name	None.
Alarm Condition	MSE was upgraded from lower version.
Severity	Major
NCS Message	None.
Category	Mobility Service
Probable Causes	None.
Recommended Actions	None.

MAB-5-FAIL

MIB Name	None.
Alarm Condition	Wired client MAC authentication failure.
NCS Message	Authentication failed for client (%s) on Interface %s AuditSessionID %s
Symptoms	Authentication was unsuccessful.
Severity	Informational
Category	Clients.

Probable Causes	Authentication was unsuccessful.
Recommended Actions	None.

MAB-5-SUCCESS

Alarm Condition	Wired client MAC authentication success.
NCS Message	Authentication successful for client (%s) on Interface %s AuditSessionID.
Symptoms	Authentication was successful.
Severity	Informational
Category	Clients.
Probable Causes	Authentication was successful.
Recommended Actions	None.

NB_OSS_UNREACHABLE

MIB Name	None.
Alarm Condition	Northbound OSS server unreachable.
NCS Message	Northbound notification server "{0}" is unreachable. NCS alarms will not be processed for this server till it is reachable.
Symptoms	NCS could not send notification through north bound.
Severity	Major
Category	Northbound
Probable Causes	Notification server might not be reachable.
Recommended Actions	Check the notification server.

NB_OSS_REACHABLE

MIB Name	None.
Alarm Condition	Northbound OSS server reachable.
NCS Message	Northbound notification server "{0}" is reachable.
Symptoms	NCS could not send notification through north bound.
Severity	Major
Category	Northbound
Probable Causes	Notification server might not be reachable.
Recommended Actions	Check the notification server.

NCS_ALARM_TABLE_SIZE_BASED_CLEANUP_DONE

MIB Name	None.
Alarm Condition	Alarm table auto cleanup done.
NCS Message	Alarm table exceeds size limit.
Symptoms	Alarm table pruned.
Severity	Informational.
Category	NCS
Probable Causes	Alarm table exceeds size limit, NCS performed a cleanup.
Recommended Actions	None.

NCS_DOWN

MIB Name	None.
Alarm Condition	NCS Down
Category	NCS
Severity	Critical
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

NCS_EMAIL_FAILURE

MIB Name	None.
Alarm Condition	NCS email failure.
NCS Message	NCS with IP Address “{0}” failed to send e-mail.
Symptoms	This notification is generated by NCS when it fails to send e-mails.
Severity	Major.
Category	NCS
Probable Causes	This can happen when SMTP server is either not configured or not reachable from NCS.
Recommended Actions	Check Administration > Settings > Mail Server settings. Send a test e-mail from the mail server settings to see if it is successful.

NCS_NOTIFICATION_FAILURE

MIB Name	None.
Alarm Condition	NCS notification failure.
NCS Message	NCS with IP Address "{0}" failed to send notification. Please check Administration->Settings->Notification Receiver settings.
Symptoms	NCS could not send notifications.
Severity	Major.
Category	NCS
Probable Causes	The notification destination not reachable.
Recommended Actions	Make Notification receiver configuration change.

NCS_LOW_DISK_SPACE

MIB Name	None.
Alarm Condition	NCS has low disk space
NCS Message	NCS “{0}” does not meet the minimum hardware requirements for disk space. Available: “{3}.” Minimum requirement: “{4}” Mb.
Symptoms	This notification is generated by NCS when the free disk space where NCS is installed does not meet minimum hardware requirements. This event is of major severity if minimum requirements are not met. This event is of critical severity when the available disk space is less than half of the minimum requirement.
Severity	Major/Critical.
Category	NCS
Probable Causes	This can happen when the disk is out of space.
Recommended Actions	Free up disk space.

NCS_OK_DISK_SPACE_BACKUP

MIB Name	None.
Alarm Condition	System has sufficient disk backup space.
NCS Message	NCS "{0}" has sufficient disk space in directory "{1}" for backup. Space needed: "{2}"GB, space free: "{3}"GB”.
Symptoms	NCS have enough disk space for backup.
Severity	Clear.
Category	NCS
Probable Causes	Clear alarm for NCS_LOW_DISK_SPACE_BACKUP.
Recommended Actions	None.

NCS_OK_DISK_SPACE

MIB Name	None.
Alarm Condition	System has enough disk space.
NCS Message	NCS "{0}" meets the minimum hardware requirements for disk space. Available: "{3}"GB. Minimum requirement: "{4}"GB.
Symptoms	NCS disk space meets requirement.
Severity	Clear.
Category	NCS
Probable Causes	Clear alarm for NCS_LOW_DISK_SPACE.
Recommended Actions	None.

NCS_LOW_DISK_SPACE_BACKUP

MIB Name	None.
Alarm Condition	NCS does not have enough disk space for backup.
NCS Message	NCS "{0}" does not have sufficient disk space in directory "{1}" for backup. Space needed: "{2}"GB, space free: "{3}"GB.
Symptoms	NCS does not have enough disk space.
Severity	Major.
Category	NCS
Probable Causes	Disk space is low.
Recommended Actions	Free up disk space.

PASSWORD_EXPIRY_ALARM

MIB Name	None.
Alarm Condition	Root password expiry on MSE.
Category	Mobility Service
Severity	Warning
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

RADIO_COVERAGE_PROFILE_FAILED

MIB Name	bsnAPCoverageProfileFailed.
Alarm Condition	Radio coverage threshold violation.

NCS Message	AP "{0}," interface "{1}." Coverage threshold of "{3}" is violated. Total no. of clients is "{5}" and no. failed clients is "{4}."
Symptoms	Number of clients experiencing suboptimal performance has crossed the configured threshold.
Severity	Minor.
Category	Performance
Probable Causes	Many clients are wandering to the remote parts of the coverage area of this radio interface with no handoff alternative.
Recommended Actions	• If the configured threshold is too low, you may need to readjust it to a more optimal value. • If the coverage profile occurs on a more frequent basis, you may need to provide additional radio coverage. • If the power level of this radio can be manually controlled, you may need to boost it to increase the coverage area.

RADIO_CURRENT_CHANNEL_CHANGED

MIB Name	bsnAPCurrentChannelChanged.
Alarm Condition	Radio current channel changed.
Symptoms	None.
Category	RRM
Severity	Informational
NCS Message	AP "{0}", interface "{1}". Channel changed to "{2}". Interference Energy before update was "{3}" and after update is "{4}".
Probable Causes	None.
Recommended Actions	None.

RADIO_INTERFERENCE_PROFILE_FAILED

MIB Name	None.
Alarm Condition	Radio interference threshold violation.
Severity	Minor
NCS Message	None.
Category	Access Point.
Probable Causes	None.
Recommended Actions	None.

RADIO_LOAD_PROFILE_FAILED

MIB Name	bsnAPLoadProfileFailed
Alarm Condition	Radio load threshold violation.
Symptoms	A radio interface of an Access point is reporting that the client load crossed a configured threshold.
Category	AP
Severity	Minor
NCS Message	AP "{0}", interface "{1}". Load threshold violated.
Probable Causes	There are too many clients associated with this radio interface.
Recommended Actions	• Verify the client count on this radio interface. If the threshold for this trap is too low, it may need to be readjusted • New capacity may need to be added to the physical location if the client count tends to be a frequent issue on this radio.

RADIO_NOISE_PROFILE_FAILED

MIB Name	bsnAPNoiseProfileFailed.
Alarm Condition	Radio noise threshold violation.
NCS Message	AP "{0}," interface "{1}." Noise threshold violated.
Symptoms	The monitored noise level on this radio has crossed the configured threshold.
Severity	Minor.
Category	Access Point.
Probable Causes	Noise sources that adversely affect the frequencies on which the radio interface operates.
Recommended Actions	• If the noise threshold is too low, you may need to readjust it to a more optimal value. • Investigate noise sources in the vicinity of the radio interface (for example, a microwave oven).

RADIO_SHUT_FAILED

MIB Name	None.
Alarm Condition	Radio shutdown failed.
NCS Message	Radio shutdown failed for AP “{0}” connected to controller “{1}.”
Symptoms	This notification is generated by NCS during a scheduled operation for a given list of access point radios. It notifies the user that the status for certain radios has failed to change.
Severity	Major.
Category	Access Point.

Probable Causes	The controllers for the selected access point are not reachable, or the radio configurations are changed on the controller.
Recommended Actions	Check the NCS logs at the time of event generation and verify that the access point is associated with the controller.

RADIO_SHUT_SUCCESS

MIB Name	None.
Alarm Condition	Radio successfully shutdown.
NCS Message	Radio successfully shutdown for AP "{0}" connected to controller "{1}."
Symptoms	This notification is generated by NCS during scheduled operation for a given list of access point radios. It notifies the user that the admin status has been successfully changed.
Severity	Informational.
Category	Access Point.
Probable Causes	None.
Recommended Actions	Verify the status of the specified radio on the controller.

RADIUS-4-RADIUS_ALIVE

Syslog Name	RADIUS-4-RADIUS_ALIVE
Alarm Condition	Radius server alive.
NCS Message	"RADIUS server [IP_address]:[int] [int] is being marked alive."
Symptoms	A RADIUS server that previously was not responding has responded to a new request or the deadtimer has expired.
Severity	Minor
Category	Switch
Probable Causes	A RADIUS server that previously was not responding has responded to a new request or the deadtimer has expired.
Recommended Actions	No action is required.

RADIUS-4-RADIUS_DEAD

MIB Name	None.
Alarm Condition	Radius server dead
Severity	Minor
NCS Message	RADIUS server %s is not responding.
Category	Switch

Probable Causes	Radius Server is not reachable from NCS.
Recommended Actions	Check that Radius Server is reachable from NCS.

ROGUE_ADHOC_DETECTED_ON_NETWORK

MIB Name	None.
Alarm Condition	Adhoc Rogue detected on network.
Category	Adhoc Rogue
Severity	Critical
NCS Message	Rogue AP "{0}" is on wired network.
Probable Causes	None.
Recommended Actions	None.

ROGUE_ADHOC_DETECTED_CONTAINED

MIB Name	None.
Alarm Condition	Adhoc Rogue detected contained.
Category	Adhoc Rogue
Severity	Minor
NCS Message	Rogue AP contained.
Probable Causes	Manual or auto containment action.
Recommended Actions	None.

ROGUE_AP_STATE_CHANGE

MIB Name	None.
Alarm Condition	Rogue detected.
Category	Rogue AP.
Severity	Minor
NCS Message	Rogue AP marked as {0} AP..
Probable Causes	User action.
Recommended Actions	None.

ROGUE_DETECTED

MIB Name	None.
Alarm Condition	Rogue detected.
NCS Message	:Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Severity	Minor
Category	Rogue AP
Probable Causes	None.
Recommended Actions	None.

ROGUE_DETECTED_CONTAINED

MIB Name	None.
Alarm Condition	Rogue detected contained.
Category	Rogue AP
Severity	Minor
NCS Message	Adhoc Rogue contained.
Probable Causes	Manual or auto cntainment action.
Recommended Actions	None.

ROGUE_DETECTED_ON_NETWORK

MIB Name	None.
Alarm Condition	Rogue detected on network.
Category	Rogue AP
Severity	Critical
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

ROGUE_AUTO_CONTAINED

MIB Name	None.
Alarm Condition	Rogue auto contained.
Category	Security
Severity	Major
NCS Message	Rogue AP "{0}" on Controller "{1}" was advertising our SSID and has been auto contained as per WPS policy.
Probable Causes	None.
Recommended Actions	None.

SWITCH_DOWN

MIB Name	This is a NCS-only event.
Alarm Condition	Controller down.
NCS Message	Switch "{0}" is unreachable.
Symptoms	A switch (controller) is unreachable from the management system.
Severity	Critical.
Category	Controller
Probable Causes	• The switch (controller) has encountered hardware or software failure. • There are network connectivity issues between the management station and the switch (controller). • The configured SNMP community strings on the management station or the switch (controller) are incorrect.
Recommended Actions	• Check if the switch (controller) is powered up and reachable through the web interface. • Ping the switch (controller) from the management station to verify if there is IP connectivity. • Check the community strings configured on the management station.

SWT_SWITCH_DOWN

MIB Name	None.
Alarm Condition	Switch down
Category	Switch
Severity	Critical
NCS Message	None.

Probable Causes	None.
Recommended Actions	None.

STATION_AUTHFAIL_VLAN_ASSIGNED

MIB Name	None.
Alarm Condition	Wired Client auth fail VLAN assigned
Category	Clients
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

STATION_CRITICAL_VLAN_ASSIGNED

MIB Name	None.
Alarm Condition	Wired Client critical VLAN assigned
Category	Clients
Severity	Information
NCS Message	Critical VLAN %s is assigned to Wired Client "%s".
Probable Causes	Radius Server is not reachable from the Access Switch.
Recommended Actions	Check that Radius Server is reachalble from Access Switch.

STATION_GUEST_VLAN_ASSIGNED

MIB Name	None.
Alarm Condition	Wired Client guest VLAN assigned
Category	Clients
Severity	Information
NCS Message	Guest VLAN %s is assigned to Wired Client '%s".
Probable Causes	Client is moved to Auth Fail VLAN because client failed authentication.
Recommended Actions	Check that client provided appropriate credentials.

TRACKED_CLIENT_DETECTION

MIB Name	None.
Alarm Condition	Tracked client detected on the network.
Category	Security
Severity	Major
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

USER_AUTHENTICATION_FAILURE

MIB Name	None.
Alarm Condition	User Authentication Failure.
Category	Security
Severity	Informational
NCS Message	"%s" "%s" failed authentication on Controller "%s".
Probable Causes	User failed to authenticate.
Recommended Actions	Check that user provides appropriate credentials.

WARM_START

MIB Name	None.
Alarm Condition	Warm start trap from controller
Category	Controller
Severity	Informational
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

Wireless Intrusion Protection Alarms

MIB Name	None.
Alarm Condition	wIPS engine on MSE.
NCS Message	Dynamically generated. Refer WCS Monitor>Alarms.
Symptoms	Refer to wIPS alarm encyclopedia under WCS>Configuration>wIPS Profiles.
Severity	Critical.
Category	Mobility Service
Probable Causes	Possible security attack.
Recommended Actions	None.

WLAN_SHUT_FAILED

MIB Name	None.
Alarm Condition	Client associated failure with AP.
NCS Message	Wlan "{0}" shutdown failed on controller "{1}."
Symptoms	This notification is generated by NCS during scheduled operations for a given WLAN Config object. It notifies the user that the WLAN status did not change at the scheduled time.
Severity	Major.
Category	NCS
Probable Causes	The controller for the selected WLAN is not reachable, or the WLAN object does not exist.
Recommended Actions	Check the NCS logs at the time of event generation and verify if the WLAN exists on the controller.

WLAN_SHUT_SUCCESS

MIB Name	None.
Alarm Condition	WLAN successfully shutdown.
NCS Message	Wlan "{0}" successfully shutdown on controller "{1}."
Symptoms	This notification is generated by NCS during scheduled operation for each given WLAN configuration object. It notifies the user that the admin status has been successfully completed.
Severity	Informational..
Category	NCS
Probable Causes	Verify the admin status for the displayed WLAN on the controller.
Recommended Actions	Remove the event from the event list page.

WLC_CANCEL_SCHEDULED_RESET

MIB Name	None.
Alarm Condition	None.
Category	Controller
Severity	Informational
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

WLC_SCHEDULED_RESET_FAILED

MIB Name	None.
Alarm Condition	None.
Category	Controller
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

Unsupported Traps

- BROADCAST_STORM_START: broadcastStormStartTrap
- FAN_FAILURE: fanFailureTrap
- POWER_SUPPLY_STATUS_CHANGE: powerSupplyStatusChangeTrap
- BROADCAST_STORM_END: broadcastStormEndTrap
- VLAN_REQUEST_FAILURE: vlanRequestFailureTrap
- VLAN_DELETE_LAST: vlanDeleteLastTrap
- VLAN_DEFAULT_CFG_FAILURE: vlanDefaultCfgFailureTrap
- VLAN_RESTORE_FAILURE_TRAP: vlanRestoreFailureTrap
- IPSEC_ESP_REPLAY_FAILURE: bsnIpsecEspReplayFailureTrap
- IPSEC_ESP_INVALID_SPI: bsnIpsecEspInvalidSpiTrap
- LRAD_UP: bsnAPUp
- LRAD_DOWN: bsnAPDown
- STP_NEWROOT: stpInstanceNewRootTrap
- STP_TOPOLOGY_CHANGE: stpInstanceTopologyChangeTrap
- BSN_DOT11_ESS_CREATED: bsnDot11EssCreated
- BSN_DOT11_ESS_DELETED BSNDOT11ESSDELETED
- LRADIF_RTS_THRESHOLD_CHANGED
- LRADIF_ED_THRESHOLD_CHANGED
- LRADIF_FRAGMENTATION_THRESHOLD_CHANGED
- LINK_FAILURE: linkFailureTrap