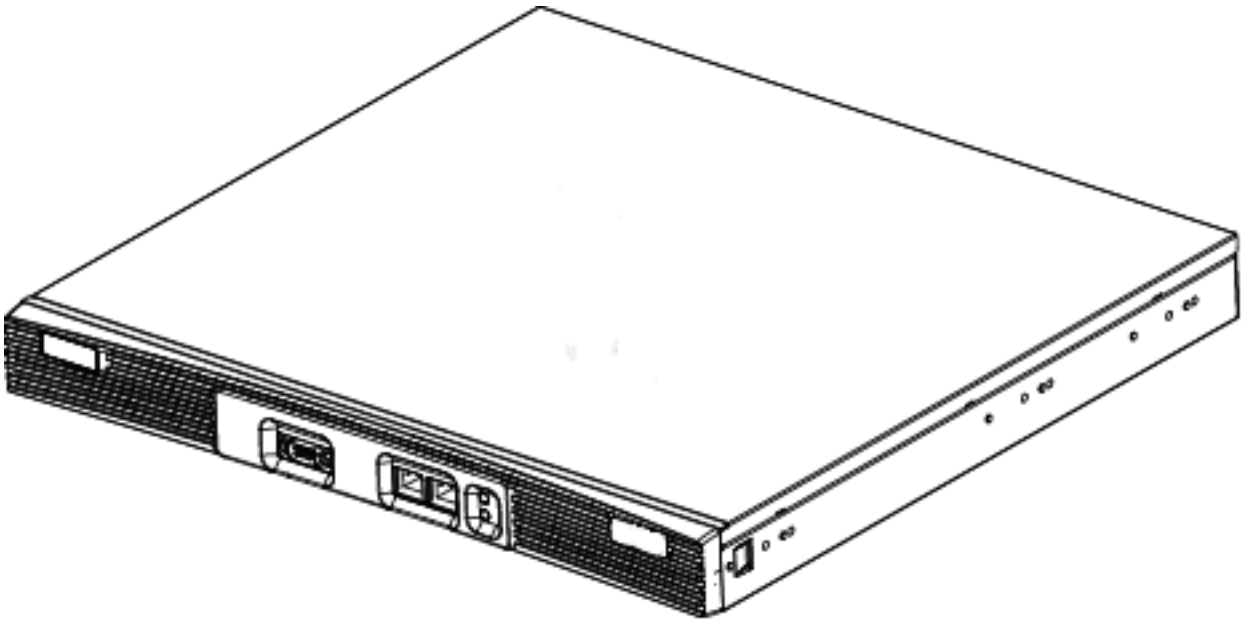
MOTOROLA

WS5100 Series Switch

Troubleshooting Guide



Contents

About This Guide

Introduction

This guide provides information for troubleshooting issues on the WS 5100 Series Switch.

NOTE: Screens and windows pictured in this guide are samples and can differ from actual screens.

Documentation Set

The documentation set for the WS5100 Series Switch is partitioned into the following guides to provide information for specific user needs.

- **WS5100 System Reference** - describes WS5100 Series Switch Web UI configuration activities and the resulting network behavior.
- **WS5100 Installation Guide** - describes the basic setup and configuration required to transition to more advanced configuration of the switch.
- **WS5100 CLI Reference** - describes the *Command Line Interface* (CLI) and *Management Information Base* (MIB) commands used to configure the WS5100 Series Switch.
- **WS5100 Migration Guide** - provides upgrade instructions and new feature descriptions for legacy users of the WS5100 Series Switch.

Document Conventions

NOTE: Indicate tips or special requirements.

CAUTION: Indicates conditions that can cause equipment damage or data loss.

WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

Notational Conventions

The following additional notational conventions are used in this document:

- *Italics* are used to highlight the following:
  - Chapters and sections in this and related documents
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Icons on a screen.
- **GUI** text is used to highlight the following:
  - Screen names
  - Menu items
  - Button names on a screen.
- bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

1

Overview

This chapter describes common system issues and what to look for while diagnosing the cause of a problem. Wherever possible, it includes possible suggestions or solutions to resolve the issues.

The following sections are included:

1.1 Wireless Switch Issues

This section describes various issues that may occur when working with the switch. Possible issues include

1.1.1 Switch Does Not Boot Up

The switch does not boot up to a username prompt via CLI console or Telnet.

Table 1.1 provides suggestions to troubleshoot this issue.

Table 1.1 Switch Does Not Boot Up Troubleshooting Notes

Possible Problem	***Suggestions to Correct***
Switch has no power	• Verify power cables, fuses, UPS power. The front panel LED lights up when power is applied to the switch. • Verify the power switch on the back of the switch is in the **I** (on) position. • Have a qualified electrician check the power source to which the switch is connected.
Chassis fans and/or CPU fan not rotating	• Visually inspect the fans located inside the switch chassis. • If one or more of the CPU fans are not running, contact the Motorola Support center for further instructions.
All else...	Contact Motorola Support.

1.1.2 Switch Takes a Long Time to Start Up

Until DHCP is enabled (and if static IP addresses are not being used), startup can be extremely slow. This is normal.

1.1.3 Switch Does Not Obtain an IP Address through DHCP

The switch requires a routable IP address for the administrator to manage it via Telnet, SSH or a Web browser. By default, the switch boots up with a non-routable static IP address.

Table 1.2 provides suggestions to troubleshoot this issue.

Table 1.2 Switch Does Not Obtain an IP Address through DHCP Troubleshooting Notes

Possible Issue	***Suggestions to Correct***
DHCP is not configured, or not available on same network as the switch	• Verify the configuration for the switch has DHCP enabled. By default, Ethernet NIC 2 is DHCP enabled. Otherwise, refer to the CLI reference for instructions on enabling the Ethernet interfaces. • Ensure the WS5100 is on the same network as the DHCP server and verify the server is providing DHCP services. • Connect another host configured for DHCP and verify it is getting a DHCP address
DHCP is not enabled on NIC 2 (that is, the Ethernet port that is not managing the RF network)	• Enable DHCP, use the CLI command or the GUI to enable DHCP on the Ethernet port connected to your network. • Verify DHCP packets are being sent to NIC 2 using a sniffer tool • If DHCP packets are seen, check to ensure that the switch is not configured for a static IP on NIC 2.
All else..	Contact Motorola Support.

1.1.4 Switch is Stuck in a Booting Loop

The switch continuously boots and does not change context to a user name prompt.

Table 1.3 provides suggestions to troubleshoot this issue.

Table 1.3 Switch is Stuck in a Booting Loop Troubleshooting Notes

Possible Issue	***Suggestions to Correct***
Bad flash memory module	Remove the flash memory and install it in a different switch.
Switch not getting enough ventilation	Verify the CPU fan is operating properly.
All else...	Contact Motorola Support.

1.1.5 Unable to Connect to the Switch using Telnet or SSH

The switch is physically connected to the network, but connecting to the switch using SSH or Telnet does not work.

Table 1.4 provides suggestions to troubleshoot this issue.

Table 1.4 Unable to Connect to the Switch using Telnet or SSH Troubleshooting Notes

Possible Issue	***Suggestions to Correct***
Console is not on network	• Check all cabling and terminal emulation program settings to be sure they are correctly set. See *Console Port is Not Responding* issue, or the *WS5100 Series Switch System Reference Guide* for more details. • From a another system on the same network. attempt to ping the switch.
Telnet is not enabled and/or SSH is disabled	Verify Telnet or SSH are enabled using the CLI or GUI (By default, telnet is disabled.).
Max sessions have been reached	Maximum allowed sessions is 8 concurrent users connected to a switch. Verify that the threshold has not been reached. .
Primary LAN is not receiving Telnet traffic	Verify Telnet traffic is on the primary VLAN.
All else...	Contact Motorola Support.

1.1.6 Web UI is Sluggish, Does Not Refresh Properly, or Does Not Respond

When configuring the switch, it is easy to overlook the fact that the host computer is running the browser while the switch is providing the data to the browser. Occasionally, while using the Web UI (GUI) the switch does not respond or appears to be running very slow; this could be a symptom of the host computer or the network, and not the switch itself. Table 1.5 provides suggestions to troubleshoot this issue.

Table 1.5 Web UI is Sluggish, Does Not Refresh Properly, or Does Not Respond Troubleshooting Notes

Possible Issue	***Suggestions to Correct***
Bad connection between switch and console system	Verify the line between the switch and the host computer is functioning normally.
Slow transmission of data packets	Verify the data packets are being sent to and from the switch using a sniffer tool.
Access ports may try to adopt while country code is not set	Set the country name for the switch, which is set to “none” by default.

Table 1.5 Web UI is Sluggish, Does Not Refresh Properly, or Does Not Respond Troubleshooting Notes (Continued)

Possible Issue	***Suggestions to Correct***
Packet storm	Check Syslog for any type of a packet storm.
Overburdened with a large number of access ports	With large numbers of access ports, changing the configuration quickly may cause the switch to not refresh properly, at least immediately following configuration.
Java JRE is out of date	Be sure you are using Sun Java JRE 1.5 or later. To download the appropriate for your system go to: http://www.sun.com/java/
All else...	Contact Motorola Support.

1.1.7 Console Port is Not Responding

The switch console port is physically connected to the host computer's serial port, but pressing the [Enter] key gets no response from the switch.

Table 1.6 provides suggestions to troubleshoot this issue.

Table 1.6 Console Port is Not Responding Troubleshooting Notes

Possible Issue	***Suggestions to Correct***
Cabling issue	Ensure that a NULL-modem cable is connected from the WS5100 console port to the host computer's serial port.
Not using a terminal emulation program	Verify a serial terminal emulation program, such as HyperTerminal, is in use.
Settings in terminal emulation program are incorrectly set	Check the serial port settings in the serial terminal emulation program being used. The correct settings are: Terminal Type: VT-100 Port: COM 1-4 Terminal Settings: 19200 bps transfer rate, 8 data bits, no parity, 1 stop bit, no flow control
All else...	Contact Motorola Support.

1.1.8 Shutting Down the Switch

The CLI commands used to shutdown the switch have changed with the release of the 3.x version WS5100 Series Switch. Please refer to the following to differentiate between the `shutdown` command (1.4.x and 2.x) from the `halt` command (3.x).

1.1.8.1 Shutting Down the Switch Using the 1.4.x/2.x Shutdown Command

To gracefully shutdown the WS 5100, issue the `shutdown` command from the configure context in the CLI:

```
WS5000.(Cfg)> shutdown
This command will halt the system.
```

```
A manual power cycle will be required to re-start the switch.
Do you want to proceed (yes/no) : yes

System shut down might take a few mins....
Shutting down the switch...
Shutting down dhcp daemon.. done
Shutting down apache server in the OPEN mode...done.
Shutting down cell controller........ done
Shutting down snmpd agent...done.
Shutting down Postgres....done.
INIT: Sending processes the TERM signal
Shutting down PacketSwitch interface  .....
Shutting down dhcp daemon.. done
Shutting down apache server in the OPEN mode...done.
Cell controller not running.
i2c-core: Device or resource busy
Shutting down Postgres....done.
Stopping periodic command scheduler: cron.
Stopping internet superserver: inetd.
Saving random seed... done.
Stopping deferred execution scheduler: atd.
Stopping kernel log daemon: klogd.
Stopping system log daemon: syslogd.
flushing ide devices: hda
System halted.
```

As directed, wait 10 seconds and turn off the device by toggling the power switch.

1.1.8.2 Shutting Down the Switch Using the Halt Command

To shut down the WS 5100 from the CLI, issue a **`halt`** command, as the halt command is now used to shut down the switch with the release of the 3.x version WS5100 baseline:

```
WS5100#halt
Wireless switch will be halted, do you want to continue? (y/n):y
The system is going down NOW !!

% Connection is closed by administrator!
WIOS_SECURITYMGR[395]: DNSALG: Shutting down.
WIOS_SECURITYMGR[395]: FTPALG: Shutting down.
The system is halted.
```

NOTE: The WS5100 will power off after issuing a halt command through a software toggle of the power supply. Be sure to flip the power switch to the Off position. If the power cord is removed and reinstalled, or power is lost and restored, the switch will power back on.

1.2 Access Port Issues

This section describes various issues related to access ports within the switch network.

1.2.1 Access Ports are Not Adopted

Access ports are not being adopted. Table 1.7 provides suggestions to troubleshoot this issue.

Table 1.7 Access Ports are Not Adopted Troubleshooting Notes

Possible Issue	***Suggestions to Correct***
Access port is not configured	Verify the license key that is set in the switch.
Country code for switch is not set	Verify the country code is entered into the switch prior to adopting any access ports. The switch is not fully functional until a country code is set.
Access ports are off-network	Verify the access ports are connected to the network and powered on.
Switch is configured as Standby switch	Verify the switch is not configured as a Standby system prior to adopting any access ports. Even if a Standby switch is not in use, the Primary switch must be in an active state in order for it to adopt access ports. The state is automatically determined by the failover system. From the CLI or Web UI check the standby state to see if the switch is either *Primary* or *Standby*
Access ports are restricted in configuration	Verify the switch is not configured with an access control list that does not allow access port adoption; verify that access port adoption is not set to "deny". Ensure that the access port adoption policy is added with a WLAN.
Access Port is on Exclude List	Verify the ACL adoption list does not include the access ports that are not being adopted.
Miscellaneous other issues	• Check the access port LEDs for "Loadme" message on start-up. • With a packet sniffer, look for 8375 (broadcast) packets • Reset the switch. If the switch is hung, it may begin to adopt access ports properly once it has been reset.
All else...	Contact Motorola Support.

1.3 Mobile Unit Issues

This section describes various issues that may occur when working with the Mobile Units associated with the wireless switch or associated Access Ports. Possible issues include:

- *Access Port Adopted, but MU is Not Being Associated*
- *MUs Cannot Associate and/or Authenticate with Access Ports*
- *Poor Voice Quality Issues*

1.3.1 Access Port Adopted, but MU is Not Being Associated

Access port associated with an MU is not yet being adopted. The following table provides suggestions to troubleshoot this issue.

Table 1.8 Troubleshooting When Access Port Is Not Yet Adopted

Possible Issue	***Suggestions to Correct***
Unadopted access port	Verify the switch has adopted the access port with which the MU is trying to associate.
Incorrect ESSID applied to the MU	Verify on the MU the correct ESSID has been applied to the MU.
Ethernet port configuration issues	Verify the Ethernet port connected to thenetwork and has a valid configuration. If DHCP is used, verify that the Ethernet cable is connected to the same NIC upon which DHCP services are enabled.
Incorrect security settings	Verify the correct security settings are applied to a WLAN in which the MU is tryng to associate.
All else...	Contact Motorola Support.

1.3.2 MUs Cannot Associate and/or Authenticate with Access Ports

MUs cannot associate and/or authenticate with access ports. The following table provides suggestions to troubleshoot this issue.

Possible Issue	***Suggestions to Correct***
Preamble differences	Verify the Preamble matches between switch and MUs. Try a different setting.
Device key issues	Verify in Syslog that there is not a high rate of decryption error messages. This could indicate that a device key is incorrect.
MU is not in Adopt List	Verify the device is not in the “do not adopt ACL”.
Keyguard not set on client	Verify Keyguard is set on the client if the Security/WLAN Policy calls for Keygaurd.

1.3.3 Poor Voice Quality Issues

VOIP MUs, BroadCast MultiCast and SpectraLink phones have poor voice quality issues. The following table provides suggestions to troubleshoot this issue.

Possible Issue	***Suggestions to Correct***
Traffic congestion with data traffic	• Maintain voice and data traffic on separate WLANs. • Use a QoS Classifier to provide dedicated bandwidth if data and voice traffic are running on the same WLAN.
Long preamble not used on Spectralink phones	Verify that a long preamble is used with Spectralink phones.

1.4 Failover Issues

This section describes various issues related to the failover capabilitie of the switch. Possible issues include:

- *Switch is Not Failing Over*

1.4.1 Switch is Not Failing Over

Switch is not failing over (Hot Standby) as appropriate.

The following table provides suggestions to troubleshoot this issue.

Possible Issues	***Suggestions to Correct***
Primary and Standby switches are not both enabled	Verify the Primary and Secondary switches are Standby enabled and have the correct MAC address configured for the correct Primary/Secondary switch.
Primary and Standby switches have mismatched software versions	Mismatch configurations are not allowed. Verify that the Primary and Secondary switches have the same software versions running.
Primary and Standby switches cannot communicate with each other	Verify the Primary and Secondary switch are configured properly and attempt to ping each switch (using the *ping* command) from each switch.
Other problems, as listed in switch logs	Review the local logs on the Standby switch.
MAC address configuration issues	Review the Syslog. The correct MAC address should be seen when checking the Syslog heartbeat messages.
Conflicting addressing on same network	If more than one Primary switch exists on the same network, then use MAC addresses to configure.
All else...	Contact Motorola Support.

1.4.2 Switch is Failing Over Too Frequently

Switch failing over too frequently (flapping).

The following table provides suggestions to troubleshoot this issue.

Possible Issues	***Suggestions to Correct***
One of the switches is crashing	Check the CPU usage using the CLI or Web UI Diagnostics information.
All else...	Contact Motorola Support.

1.5 Installation Issues

Before upgrading or downgrading any system, save a copy of the system configuration to an FTP or TFTP server.

1.5.1 After Upgrade, Version Number Has Not Changed

After upgrading the version number has not changed. The following table provides suggestions to troubleshoot this issue.

Possible Issues	***Suggestions to Correct***
Improper upgrade process	• Refer to the release notes and repeat the upgrade process exactly as stated in the release notes. • Verify the Syslog folder contents from the CLI Service Mode context. Repeat the upgrade process if necessary.
All else...	Contact Motorola Support.

1.6 Miscellaneous Issues

This section describes various miscellaneous issues related to the switch, and don't fall into any of the previously called out issue categories. Possible issues include:

- *Excessive Fragmented Data or Excessive Broadcast*
- *Excessive Memory Leak*

1.6.1 Excessive Fragmented Data or Excessive Broadcast

Excessive fragmented data or excessive broadcast.

The following table provides suggestions to troubleshoot this issue.

Possible Issues	***Suggestions to Correct***
Fragmentation	• Change the MTU size to avoid fragmentation on other ethernet devices. • Do not allow VoIP traffic when operating on a flat network (no routers or smart switches). • Move to a trunked Ethernet port. • Move to a different configuration.
All else...	Contact Motorola Support.

1.6.2 Excessive Memory Leak

Excessive memory leak. The following table provides suggestions to troubleshoot this issue.

Possible Issues	***Suggestions to Correct***
Memory leak	Using the CLI or Web UI's Diagnostics section to check the available virtual memory. If any one process displays an excessive amount of memory usage, that process could be one of the possible causes of the problem.
Too many concurrent Telnet or SSH sessions	Keep the maximum number of Telnet or SSH sessions low (6 or less), even though up to 8 sessions are allowed.
All else...	Contact Motorola Support.

1.7 System Logging Mechanism

The switch provides subsystem logging to a Syslog server. There are two Syslog systems, local and remote. Local Syslog records system information locally, on the switch. The remote Syslog sends messages to a remote host. All Syslog messages conform to the RFC 3164 message format.

2

Syslog Messages & MU Disassociation Codes

2.1 Syslog Messages

The following table provides information and descriptions of Syslog Messages.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
1.	AUTOUPCONFIG	4	Loaded new startup config	If checksum compares for new and running configurations are different – new config overwrites the running one. This may happen during auto-install.
2.	AUTONOUPCONFIG	4	Available config is same as last loaded - will not be reloaded	New and running configurations are the same. This may happen during auto-install.
3.	AUTOUPCLCONFIG	4	Loaded new cluster config	If checksum for new and running config are different – new config overwrites the running one. This may happen during auto-install.
4.	AUTOINSTCLCFGNOCOPY	3	Could not overwrite the cluster config file [str]	Copy temp to cluster-config failed. Overwriting running-config with cluster-config, wrong url path for files display this error.
5.	AUTOUPNOCLCONFIG	5	Available cluster config is same as last loaded - will not be reloaded	Config is the same.
6.	AUTOINSTCLCFGNOREAD	3	Could not read the cluster config file [str]	Cluster config copy to temp failed.
7.	AUTONOIMAGEUPODATE	5	Requested image matches running image - will not be loaded	New and installed image versions match.
8.	AUTOIMAGEUPODATE	5	Attempting to load requested image	Local image version does not match required image version.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
9.	AUTOINSTNODHCP	5	DHCP did not provide any configuration information - no autoinstall action taken	DHCP information got update but file cannot be opened.
10.	AUTOINSTTIMEDREBOOT	7	Autoinstall delayed reboot - shutting down system now	Auto-install rebooting the system.
11.	AUTOCLCONFDISAB	5	Autoinstall of cluster configuration is disabled	No autoinstall options were enabled.
12.	AUTOINSTNODHCP	5	Autoinstall of startup configuration is disabled	No autoinstall options were enabled.
13.	AUTOINSTSIGWCCP	7	Changed cluster config - signalling WCCP daemon pid [int]	Cluster config changed. Need to inform WCCP – Wireless Cluster Control protocol, which handles all cluster services.
14.	AUTOINSTSIGWCCPUNKONWN	7	Tried to signal wccpd using pidof because pid was not read	Failed to open wccpd UID file, trying plan B. By plan B we mean that we using alternative method to find and kill the process.
15.	AUTOINSNOCLCFGCHANGE	7	Autoinstall did not change cluster config - not signalling wccpd	No cluster config changes
16.	AUTOIMAGEDISAB	5	Autoinstall of image upgrade is disabled	Image upgrade is not set – upgrade will not run
17.	AUTOINSTSTART	6	Autoinstall triggered	DHCP triggered auto-install to start
18.	AUTOINSTSCHEDULED	7	Autoinstall starting	DHCP should have written the config to the file, if we can read the config and assemble the URLs then – start auto-install.
19.	AUTOINSTTOOLATE	6	Too late for DHCP triggered autoinstall	If uptime is over 10 minutes – auto-install will not run.
20.	TKIPCNTRMEASEND	4	TKIP countermeasures ended on WLAN [uint]	End of the countermeasures timer.
21.	TKIPCNTRMEASSTART	4	TKIP countermeasures started on WLAN [uint]	Two MIC failure within pre-defined period of time – countermeasures are starting – WLAN will be disabled.
22.	DOT11ISUCCESS	6	Station [mac] completed dot11i (tkip/ccmp) handshake on WLAN [uint]	If this is a hotspot or a mac-authentication MU, then there is authentication work needed, else we are done. Mark the MU as successfully completed 802.11i authentication.
23.	DOT11IFAILURE	6	Station [mac] failed dot11i (tkip/ccmp) handshake on WLAN [uint]	Failure could occur due to 4-way handshake timeout; or unknown state of authentication (HOW?); or too many retries; or IE element is different than during association; or key routine returned error.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
24.	TKIPMICFAILRPT	4	Station [mac] reported a TKIP message integrity check fail on WLAN [uint]	MU reported MIC failure.
25.	DOT11IKEYROTN	6	Rotating dot11i (tkip/ccmp) keys on WLAN [uint]	Broadcast key rotation starting on WLAN.
26.	STATIONUNASSOC	6	Station [mac] un-associated from radio [uint]	MU is disassociated due to AP being gone for some reason; or received de-authentication request from MU; or switch sends de-authentication message because of inactivity or non-valid authentication or WPA failure or MIC failure or AP is not found or there is no valid Radius server or IDS violation ; or received disassociation request from MU.
27.	TKIPMICCHECKFAIL	4	TKIP message integrity check failed in frame on WLAN [uint]	Switch reports MIC failure for MU
28.	COUNTRYCODE	5	config: setting country code to [str]	New country code is set. All APs will be reset.
29.	RADIOUNADOPTED	5	[str] radio on AP [mac] un-adopted	Due to country code change or heartbeats timed-out or switch issued reset command.
30.	MAXAPCAPACITY	4	Max APs capacity reached: [int]	Cluster max AP capacity reached.
31.	DISKFULL	4	"Flash Disk Full, file cannot be created	File creation failed due to no memory.
32.	DFSNOVALIDHANNEL	6	"Radio [uint] unable to get a valid channel, configuration deferred	DFS is unable to find a valid channel.
33.	DFSMOVECHANNEL	6	Radio [uint] move to channel [uint] - [uint] MHz	DFS is changing the radio channel.
34.	RADIORADARDETECT	4	802.11a radio on AP [mac] found radar on channel [uint]	Radar detection notice. Channel will be changed if possible.
35.	RADIODFSEND	6	Radio [uint] has completed a DFS scan on channel [uint]	Radar scan complete.
36.	RADIODFSSTART	6	Radio [uint] starting a DFS scan on channel [uint] - [uint] MHz	Starting DFS scan.
37.	STATIONDENIEDAUTH	4	Station [mac] denied authentication : unsupported authentication method	Radius authentication timed-out, MU timed-out or authentication is not supported.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
38.	WEBAUTHSUCCESS	6	Station [mac] web authentication success on WLAN [uint]	Hotspot/Web authentication success.
39.	WEBAUTHDISC	6	Station [mac] has disconnected WLAN [uint]	Hotspot MU disconnected
40.	WEBAUTHFAILED	6	Station [mac] failed web authentication on WLAN [uint]	Hotspot/Web MU authentication failure due to wrong password.
41.	EXCESSAUTHSASSOCS EXCESSPROBES EXCESSDISASSOCS EXCESSAUTHFAILS EXCESS80211REPLAY EXCESSCRYPTOREPLAY EXCESSDECRYPTFAILS	"4	"MU [mac] tx [uint] in detect-window, filtering for [int] seconds	IDS Excessive number of disassociations or authentication failures, or excessive probes, or excessive disassociations or excessive replay or decrypt failures - MU will be disassociated.
42.	IDSNULLADDR IDSSAMEADDR IDSMCASTSRC IDSWEAKWEPIV IDSCNTRMEAS	"4	MU [mac]. Filtering for [int] seconds	IDS failure - MU will be disassociated.
43.	IDSEVENTRADIO	4	IDS event [str] detected at Radio [uint]	Events are: • probe-requests • association-requests • disassociations • authentication-fails • crypto-replay-fails • 80211-replay-fails • decryption-fails • unassoc-frames • eap-starts • null-destination • same-source-destination • multicast-source • weak-wep-iv • tkip-countermeasures • invalid-frame-length
44.	IDSEVENTSWITCH	4	IDS event [str] detected on switch	Events are same as above. Violations thresholds are user configurable on IDS.
45.	WLANKERBCFGCHG	6	WLAN [uint] de-authenticated, configuration changed	Set the WLAN as not authenticated.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
46.	WLANKERBTKTEXP	6	WLAN [uint] de-authenticated, ticket could not be renewed	Ticket couldn't be renewed due to WLAN not being authenticated.
47.	WLANKERBAUTH	6	WLAN [uint] authenticated with KDC [str], ticket valid for [uint] hr [uint] min [uint] sec	WLAN successfully authenticated with KDC.
48.	STATIONKERBAUTH	6	"Station [mac] authenticated, ticket valid for [uint] hr [uint] min [uint] sec	MU successfully authenticated with KDC.
49.	STATIONKERBTKTEXP	6	"Station [mac] de-authenticated, session ticket expired	KDC ticket expired.
50.	STATIONKERBIDCHG	6	"Station [mac] de-authenticated, station identity changed	Different user failed to provide adequate authentication credentials.
51.	STATIONTOTALLIMIT	4	Station [mac] denied authentication : max supported stations limit reached	MAX MU limit of 4096 has been reached.
52.	STATIONAUTHSEQINVAL	4	Station [mac] denied authentication : invalid auth sequence number	Incorrect sequence number in authentication request.
53.	STATIONCAPERR	4	Station [mac] denied association to radio [uint] : 802.11 capability field unsupported	Bad ESS, IBSS or WEP settings provided.
54.	STATIONSHORTPREAM	4	Station [mac] denied association to radio [uint] : Station does not support short preamble	No short preamble support on this MU.
55.	STATIONSPECMISSING	4	Station [mac] denied association to radio [uint] : Station missing spectrum management capability	Missing spectrum management capability element.
56.	STATIONLENGTHERR	4	"Station [mac] denied association to radio [uint] : Malformed request, element length exceeds packet size	Element length in assocication request exceeds packet size.
57.	STATIONSSIDERR	4	Station [mac] denied association to radio [uint] : [str]	ESSID length is invalid or ESSID not supported on radio.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
58.	STATIONNOTINACL	4	Station [mac] denied association due to ACL/ MAC-Auth-Local to radio [uint]	MU denied association due to ACL violation.
59.	STATIONRADIOLIMIT	4	Station [mac] denied association to radio [uint] : maximum Stations per radio [uint] reached	Max MU limit per radio is reached.
60.	STATIONWLANERR	4	Station [mac] denied association to radio [uint] : WLAN not specified by station	WLAN is not specified by MU.
61.	STATIONTXRATES	4	Station [mac] denied association to radio [uint] : TX rates specified by MU are not supported	Bad TX rates for MU.
62.	STATION11IMISSING	4	Station [mac] denied association to radio [uint] : Security (Keyguard/WPA/ WPA2) info element in association request was missing/invalid	WPA/WPA2 element absent in association request from MU.
63.	STATIONASSOC	6	Station [mac] associated to radio [uint] WLAN [uint]	MU successfully associated to radio.
64.	RADIUSVLANUPDATE	6	Assigning Radius Server specified VLAN [uint] to station [mac] on WLAN [uint]	Raduis assigned new VLAN to MU.
65.	RADIUSPOLICYFAIL	4	Unable to apply Radius server specified parameters to Station [mac] on WLAN [uint]	Radius Server received ACCESS-ACCEPT, but unable to apply the attributes specified.
66.	EAPAUTHSUCCESS	6	Station [mac] eap (802.1x) authentication success on WLAN [uint]	Successful 802.1x authentication.
67.	MACAUTHSUCCESS	6	Station [mac] MAC authentication success on WLAN [uint]	Successful MAC authentication.
68.	EAPAUTHFAILED	6	Station [mac] failed eap (802.1x) authentication on WLAN [uint]	Received access-reject from Radius Server.
69.	MACAUTHFAILED	6	Station [mac] failed Radius MAC authentication on WLAN [uint]	MAC authentication failure
70.	RADIUSDISCREQ	6	Received Radius Disconnect Request from [ip]	Received Radius server disconnect request. What are the reasons for this request?

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
71.	RADIUSRXCOAREQ	6	Received Radius Change-Of-Authorization Request from [ip]	Got Change of Authorization from Radius Server
72.	RADIUSDISCACK	6	Sending Radius Disconnect ACK to [ip]	All went well, user was removed - msg sent to server"
73.	RADIUSDISCNACK	6	Sending Radius Disconnect NACK to [ip]	Didn't like the request - couldn't find the MU - msg sent to server.
74.	RADIUSTXCOAACK	6	Sending Radius Change-Of-Authorization ACK to [ip]	Request for Change of Authorization succeeded - msg sent to server
75.	RADIUSTXCOANACK	6	Sending Radius Change-Of-Authorization NACK to [ip]	Didn't like the request - couldn't find the MU - msg sent to server.
76.	RADIOACSSTART	6	Radio [uint] starting auto channel selection scan	ACS is started. Called by WISP if the on radio configuration if it's set for ACS
77.	RADIOACSEND	6	Radio [uint] has completed an auto channel selection scan. Channel selected: [uint]	ACS is done. New channel is selected.
78.	RADIOADOPTED	5	[str] radio on AP [mac] adopted	Radio adoption message.
79.	UNAPPROVEDAPDETECT	4	AP [uint] detected Unapproved AP : [mac]	Rogue AP detected
80.	UNAPPROVEDAPREMOVE	4	Removing Unapproved AP [mac] : Last detected detected by AP [uint] with signal strength [int] dBm	Rogue AP is being removed from rogue AP table because: • Rogue AP detection has been disabled. • AP is not a rogue anymore • Entry aged out.
81.	SHEALRADIODOWN	4	Radio [uint] was detected down.	Radio has been detected as being down by its neighbors.
82.	SHEALACTIONTAKEN	5	Radio [uint] took self healing action to cover for down neighbor	Self healing has been activated.
83.	SHEALACTIONTAKEN	5	Radio [uint] has returned to normal operation	Radio resumed active work mode
84.	SHEALACSRERUN	5	Auto Channel Select was re-run for radio [uint] due to retry threshold being crossed	Happens if we exceeded the configured avg number or retries
85.	STATSSTATION	4	Threshold reached, [str] is [str] [str] for MU# [mac]	One of the threshold values set for the MU has been exceeded. Each threshold value has its own unique thrshold setting defined by the user.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
86.	STATSRADIO	4	Threshold reached, [str] is [str] [str] for radio# [str]	One of the threshold values set for the radio has been exceeded. Each threshold value has its own unique thrshold setting defined by the user.
87.	STATSMODULE	4	Threshold reached, [str] is [str] [str]	One of the threshold values set for the switch has been exceeded. Each threshold value has its own unique thrshold setting defined by the user.
88.	STATSWLAN	4	Threshold reached, [str] is [str] [str] for WLAN# [str]	One of the threshold values set for the WLAN has been exceeded. Each WLAN threshold value has its own unique thrshold setting defined by the user.
89.	DELETETRUSTPOINT	6	Trustpoint [str] is deleted	Certificate trustpoint is deleted due to user request or certificate expired.
90.	DELETERSAKEY	6	Rsakey [str] is deleted	Keypair is being deleted.
91.	CERTSELFSIGNEDGEN	6	Selfsigned certificate generated for the trustpoint [str]	Self-signed certificate has been generated successfully.
92.	CERTREQUESTGEN	6	Certificate request generated for the trustpoint [str]	Certificate request has been generated.
93.	RSAKEYGEN	6	Rsa key [str] generated	Keypair generated successfully. The switch can maintain different key pairs for each certificate generated. These keys can be manually or automatically generated.
94.	CERTEXPIRED	5	Server/Ca Certificate of trustpoint [str] is expired	Certificate expiration notice
95.	INVALIDCERTKEY	5	Private key imported for trustpoint [str] is not valid	Each trustpoint is associated with a certificate and RSA key. If RSA key specified is not a valid RSA key type (PEM or DER) this message displays.
96.	INVALIDSERVCERT	5	Server Certificate imported for the trustpoint [str] is invalid	If Server Certificate imported/ specified for Trustpoint is not of PEM/ DER formatted.
97.	INVALIDCACERT	5	CA Certificate imported for the trustpoint [str] is invalid	If CA Certificate imported/specified for Trustpoint is not of PEM/DER formatted.
98.	INVALIDCERTCRL	5	Certificate Crl Imported for trustpoint [str] is invalid	CRL is Certificate Revocation List, issued for revoked Certificate from a root CA authority. Wrong format of imported CRL displays this message.
99.	CERTIMPORTED	6	Server/Ca/CRL Certificate imported for the trustpoint [str]	A certificate has been imported.

Number	***Mnemonic***	***Severity***	***Syslog Message***	***Meaning / Cause***
100.	CERTKEYIMPORTED	6	Private key imported for the trustpoint [str]	Key is successfully imported for specified trust point.
101.	INVALIDRSAKEY	5	Rsakey imported with the name [str] is invalid	RSA Key imported is not of valid PEM/DER format.
102.	KEYDECRYPTFAILE	4	Rsakey cannot be decrypted with the password provided	If private key is generated using a pass phrase, while importing it we need to specify it. The wrong password can display this error.
103.	ERROR	5	CERTMGR_NO_ TRUSTPOINT: No tustpoint is configured with the specified name.	A trustpoint cound not be generated using the requested name. Ensure the name meets required naming conventions for the trustpoint.
104.	ERROR	5	CERTMGR_FILE_OP_ ERROR: Performing file operation.	This internal error is triggered when any error occurs during write/read to certifcate file.
105.	ERROR	5	CERTMGR_DIR_OP_ ERROR: Performing directory operation.	This error is triggered when any eror occurs during directory operations.
106.	ERROR	5	CERTMGR_MEM_ALLOC_ ERROR: Memory allocation error.	This eror is triggered when the switch runs out of memory and memory allocation fails.
107.	ERROR	5	CERTMGR_INVALID_PKEY _FORMAT: Invalid private key format. PEM and DER formatted keys are supported. Please check the format and try again.	This eror is triggered when the private key imported is not in either PEM or DER formats.
108.	ERROR	5	CERTMGR_INVALID_CERT _FORMAT: Invalid certificate format. PEM and DER formatted certificates are supported. Please check the format and try again.	This eror is triggered when the certificate imported is not in either PEM or DER formats.
109.	ERROR	5	CERTMGR_INVALID_TIME: Certificate imported is either not yet valid or is expired with respect to switch time. Please check the switch time and try again.	This eror is triggered when a certificate imported is either not yet valid or is expired with respect to switch time.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
110.	ERROR	5	CERTMGR_INVALID_ SERVER_CERT: Server certificate does not match corresponding private key. Please import the valid certificate and try again.	This eror is triggered when a server certificate imported does not match corresponding private key.
111.	ERROR	5	CERTMGR_NO_PARAMS: Mandatory parameters are not set for the trustpoint. Please set the subject-name in the trustpoint context and try again.	This error is triggered when subject name is not set for a trustpoint before generatoing a self-signed certificate or certificate request.
112.	ERROR	5	CERTMGR_SELF_CERT_ ERROR: Failed to generate selfsigned certificate.	An error took place during the generation process.
113.	ERROR	5	CERTMGR_CERT_REQ_ ERROR: Failed to generate certificate request.	An error took place during the certificate request.
114.	ERROR	5	CERTMGR_TRUSTPOINT_ ENROLLED: Specified trustpoint is already enrolled.	This error is triggered when the user attempts to generate a self-signed certificate or certificate request to a trust point to which a self signed certificate or certificate request exists.
115.	ERROR	5	CERTMGR_NO_KEYPAIR: No keypair exists with the specified name.	This erorr is triggered when the user attempts to delete a keypair that does not exists.
116.	ERROR	5	CERTMGR_KEY_PAIR_ ERROR: Failed to generate RSA key.	This error is triggered when the RSA key generation fails.
117.	ERROR	5	CERTMGR_KEY_ENC_ ERROR: Failed to encrypt the key.	This error is triggered when the key fails to get encrypted during the key export.
118.	ERROR	5	CERTMGR_KEY_DEC_ ERROR: Failed to decrypt the key.	This error is triggered when the key fails to get decrypted during the key import.
119.	ERROR	5	CERTMGR_MAX_ TRUSTPOINTS: Maximum number of trustpoints already configured.	This error is triggered when the user tries to configure a trustpoint when there are already maximum numbers of truspoints configured.

Number	*Mnemonic*	*Severity*	*Syslog Message*	*Meaning / Cause*
120.	ERROR	5	CERTMGR_MAX_ KEYPAIRS: Maximum number of keypairs already configured.	This error is triggered when the user tries to configure a keypair when there are already maximum numbers of keypair configured.
121.	ERROR	5	CERTMGR_LIST_ADD_ ERROR: Failed to add the trustpoint/ key.	This error is triggered when adding a trustpoint/ key to a link list.
122.	ERROR	5	CERTMGR_KEYPAIR_TRUS TPOINT_EXISTS: Specified keypair has been associated to one/more trustpoints. Please delete the associated trustpoint and then delete the key.	This error is triggered when a specified keypair has been associated to one/more trustpoints.
123.	ERROR	5	CERTMGR_KEYPAIR_ EXISTS: Key with the specified name already exists.	This error is triggered when a key with the specified name already exists.
124.	ERROR	5	CERTMGR_TRUSTPOINT_ EXISTS: Trustpoint with the specified name already exists.	This error is triggered when a trustpoint with the specified name already exists.
125.	ERROR	5	CERTMGR_CA_EXISTS: CA certificate already exists for the specified trustpoint.	This error is triggered when the user attempts to import a CA certificate for a trustpoint to which CA certifcate already exists.
126.	ERROR	5	CERTMGR_SERVER_ EXISTS: Server certificate already exists for the specified trustpoint.	This error is triggered when the user attempts to import a Server Certificate for a trustpoint to which Server Certificate already exists.
127.	ERROR	5	CERTMGR_SAVE_ ERROR: Failed to save the certificate.	This error is thorwn when the certificate fails to get stored to certificate storage.
128.	ERROR	5	CERTMGR_ENROLL_ ERROR: Trustpoint specified is not enrolled.	This error is triggered when user tries to import a certificate for which a request is not generated.
129.	ERROR	5	CERTMGR_NO_CA: CA certificate does not exists for the specified trustpoint.	This error is triggered when user attempts to delete a CA certificate for a trust point for which CA cettifictae does not exist.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
130.	ERROR	5	CERTMGR_NO_SERVER: Server certificate does not exists for the specified trustpoint.	This error is triggered when user attempts to delete a Server certificate for a trust point for which Server cettifictae does not exist.
131.	ERROR	5	CERTMGR_INVALID_PRIV_ KEY: Private key imported is not valid.	This error is triggered when the user imports invalid private key.
132.	ERROR	5	CERTMGR_DEFAULT_ TRUSTPOINT_ERROR: Default trustpoint can not be deleted.	This error is triggered when the user attempts to delete the default trustpoint. The default trustpoint cannot be deleted.
133.	ERROR	5	CERTMGR_DEFAULT_ RSAKEY_ERROR: Default keypair can not be deleted.	This error is triggered when the user attempts to delete the default keypair. The default keypair cannot be deleted.
134.	ERROR	5	CERTMGR_INVALID_CERT _CRL: CRL imported is not valid.	This error is triggered when the user attempts to import invalid CRL.
135.	ERROR	5	CERTMGR_CA_CRL_ EXISTS: CRL exists for the trustpoint. Please delete the CRL before deleting the CA Certificate.	This error is triggered when the user attempts to delete the CRL for a trustpoint for which the CA cetificate exists.
136.	ERROR	5	CERTMGR_NO_CA_CRL: CRL does not exist for the specified trustpoint.	This error is triggered when the user attempts to delete the CRL for a trustpoint for which the CRL cetificate exists.
137.	ERROR	5	CERTMGR_CERT_INFO_ ERROR: Failed to show certificate details.	This error is triggered when the system fails to generate the certificate information when the user attempts to see the information in the trustpoint certificate.
138.	ERROR	5	CERTMGR_CERT_MAX_ SIZE: File size exceeded maximum size(10240 bytes).	THis eror is triggered when the user imports certificate or key of size more than 10240 bytes.
139.	ERROR	5	CERTMGR_NO_KEY_ PASSWORD: Imported key file is encrypted. Please provide the pass phrase and try again.	This error is triggered when the user imports encrypted key file without entering the password.

Number	*Mnemonic*	*Severity*	*Syslog Message*	*Meaning / Cause*
140.	ERROR	5	CERTMGR_DEFAULT_ SERVCERT_DEL_ERROR: Server certificate of default trustpoint can not be deleted.	This error is triggered when the user attempts to delete the server certificate of the default trustpoint. Server certificate of default trustpoint cannot be deleted.
141.	ERROR	5	CERTMGR_SENDTO_ ERROR: Failed to notify rtificate/key events.	This error is triggered when the event bus notification of the certificate manager events fails.
153.	NO INFORMATION: NEED MNEMONIC FROM ENGINEERING	5	Include range is not configured for pool [str]	Generated when trying to remove a DHCP IP range not configured for the specified pool.
154.	PANIC	5	Last reboot was caused by a panic	The panic message is used to indicate a switch restart due to a kernel crash. Panic files are created when the switch comes up in flash/crashinfo. These files are visible in GUI under *Diagnostics > Panic Snapshot*s and through the CLI using command service show crash-info.
155.	TRUSTPOINTDELETED	4	Trustpoint [str] associated with https is deleted so https is restarted with default trustpoint	HTTPS is configured to work with a trustpoint other than the default trustpoint, and that trustpoint is deleted. Specify a different trustpoint.
156.	KEYDELETED	4	Rsakey [str] associated with ssh is deleted so ssh is restarted with default rsa key	SSHD can be configured to use the RSA key generated by user. If this key is deleted, SSHD goes back to the default key displaying this message.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
157.	NEWLEDSTATE	6	LED state message ID [uint] from module [str]	Event IDs are: WIOS_LED_POWER_OFF = 0 WIOS_LED_POWER_ON_SELF_TEST =1 WIOS_LED_POST_FAILED = 2 WIOS_LED_POST_SUCCEEDED = 3 /* PM Responsibe to set the following */ WIOS_LED_SOFTWARE_FAILED = 4 WIOS_LED_SOFTWARE_SUCCEEDED = 5 /* CC responsible to set the following */ WIOS_LED_NO_COUNTRY_CODE_SET = 6 WIOS_LED_COUNTRY_CODE_SET = 7 WIOS_LED_PORT_NOT_ADOPTED = 8 WIOS_LED_PORT_ADOPTED = 9 /* Cluster responsible to set the following */ WIOS_LED_ACTIVE_ADOPTING = 10 WIOS_LED_NO_LICENSE_TO_ADOPT = 11 WIOS_LED_ACTIVE_FAILEDOVER = 12 WIOS_LED_ACTIVE_NOTFAILEDOVER = 13 /* When the following event occurs, LED lib should set the LED state to * WIOS_LED_POST_SUCCEEDED provided no other prioritized events * in the queue */ WIOS_LED_CLUSTER_DISABLED = 14 Module names are WCCP or CC or LICENSEMGR. Those modules will set LED state.
158.	FANUNDERSPEED	4	Fan [str] under speed: [uint] RPM is under limit [uint] RPM	Diagnostic message: Fan speed is too slow.
159.	UNDERVOLTAGE	4	Voltage [dec2]V under low limit [dec2]V	Diagnostic message: Voltage reading is under low limit.
160.	OVERVOLTAGE	4	Voltage [dec2]V over high limit [dec2]V	Diagnostic message: Voltage reading is over high limit.
161.	LOWTEMP	6	Temp sensor [str] [dec2]C under low limit [dec2]C	Diagnostic message: Temperature reading is under low limit.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
162.	HIGHTEMP	4	Temp sensor [str] [dec2]C over high limit [dec2]C	Diagnostic message: Temperature reading is over high limit.
163.	OVERTEMP	0	Temp sensor [str] [dec2]C over maximum limit [dec2]C. Shutdown switch!	Diagnostic message: Temperature reading is over high limit – switch is shutting down. Ensure problem is diagnosed before powering back up the switch.
164.	CPULOAD	4	"One/Five/Fifteen minute average load limit exceeded, value is [dec2]% limit is [dec2]% (top process [str] [dec2]%)	When checking processor load every 1, 5 and 15 minute, alarms are over limit conditions. Error exists when average CPU load at 1, 5 and 15 minute intervals are more than maximum limit (99.9 % , 98 % and 95% respectively).
165.	BUFUSAGE	6	"[uint] byte buffer usage gter than expected, [uint] used, warning level [uint]real	Kernel buffer usage more than predefined maximums. Maximum limits for kernel buffer can be seen by "service show diag limit" command and current status can be seen by the "service show diag stats" command.
166.	HEADCACHEUSAGE	6	"socket buffer head cache usage is greater than expected, usage [uint], warning level [uint]	The packet buffer head cache usage is more than the maximum limit of 11000 bytes. Reduce cache to rectify.
167.	IPDESTUSAGE	6	"IP destination cache usage is greater than expected, usage [uint], warning level [uint]	The number if IP destinations the switch sees. This is informative does not constitute any alert condition
168.	FREERAM	6	"Free RAM, [dec2]% is less than limit [dec2]%	This may happen if there is a memory leak in any of the applicationsrunning on switch. Memory consumption can be seen by the "service show diag top" command. Killing the process will free the memory required to run at preferred limits and stop the message.
169.	RAMUSAGE	6	"[str], pid [uint], has exceeded ram usage limit [uint].[uint]%, now using [uint].[uint]%	Displays if a particular process increases beyond maximum memory allocations per process (i.e. 50% of the total RAM memory). Could be from a memory leak or a process hang. Restarting the process will resolve the issue.
170.	FDCOUNT	4	FD Usage [uint] is over limit [uint]	Displays when running out of space on the flash disk. Results when file descriptors exceed the maximum limit of 2500.
171.	NEWLICENSE	6	Licensed AP count changed to [uint]	Displays when the user enters a new license.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
172.	OPERUP	6	Mobility is Operationally UP	An informational message displaying when Layer 3 Mobility is Enabled.
173.	OPERDOWN	6	Mobility is Operationally DOWN	An informational message displaying when Layer 3 mobility is disabled.
174.	MUADD	6	Station [mac]: Added to Mobility Database	An informational message displaying when a new MU is added to the mobility database.
175.	MUDEL	6	Station [mac]: Deleted from Mobility Database	Occurs when a MU is deleted from the mobility database. Can occur when a MU is disconnected.
176.	MUJOIN	6	Station [mac]: JOIN received from peer [ip]	A join request from a peer is received.
177.	MUL3ROAM	6	Station [mac]: L3-ROAM received from peer [ip]	Is originated by a new CS (current switch on a different L3 network) when a MU roams to it. The home switch does not change for the MU. The MU roams to same the SSID on different switch.
178.	MUREHOME	6	Station [mac]: REHOME received from peer [ip]	Originated by a new CS (current switch on the same L3 network) when a MU roams to it. The peer switch is new home wwitch for the MU.
179.	MULEAVE	6	Station [mac]: LEAVE received from peer [ip]	The current switch originates a message and sends it to the home switch after confirming a MU has left its mobility domain.
180.	MUCONFLICT	4	Station [mac]: Conflict in Database state	MU mobility database conflict. The MU will be de-authenticated and re-associated to refresh the database of all peers.
181.	PEERUP	4	Peer [ip] is UP	The mobility peer is up. The mobility peer is the switch specified in the L3 mobility service list.
182.	PEERDOWN	5	Peer [ip] is DOWN	The mobility peer is down. Possible causes could include: • Connection broken with peer • Mobility disabled on peer • Connection close received from peer • Error message received from peer.
183.	PROCNORESP	4	"Process ""[str]"" is not responding	Process monitor is not getting heartbeat from process. The switch restarts the process after the timeout interval.

Number	***Mnemonic***	***Severity***	***Syslog Message***	***Meaning / Cause***
184.	PROCID	5	"Process ""[str]"" changed its PID from [int] to [int]	The process has changed its PID. Informational only.
185.	PROCSTART	6	"Starting process ""[str]	The process is started. Informational only.
186.	PROCRSTRT	3	"Process ""[str]"" is not responding. Restarting process	Unresponsive process detected. Process will be restarted and a core dump will be saved to the switch.
187.	PROCMAXRSTRT	1	"Process ""[str]"" reached its maximum number of allowed restarts	Too many restarts of the same process. The maximum number of process restarts has been reached but the system-restart is disabled or reached maximum the number of system restarts Default number of process restarts is 4.
188.	PROCSYSRSTRT	0	"Process ""[str]"" reached its maximum number of allowed restarts. Rebooting the system !	The maximum number of process restarts has been reached. The switch is going to reboot.
189.	PROCSTOP	5	"Process ""[str]"" has been stopped	The switch is killing the process from the start-shell using a kill command.
190.	STARTUPCOMPLETE	5	System startup complete	The switch was started.
191.	ADOPTEXCEED	4	"Total APs adoption exceeded redundancy group authorization level in group [uint], adoption count: [uint], group authorization level: [uint]	The adoption level on am AP has exceeded the cluster adoption license. Some APs will have to be removed. Should not happen unless there are unlicensed APs on the network.
192.	PEERACTIVEUP	5	"Heartbeats getting exchanged with peer [ip], group ID [uint] in active mode	The primary peer is observable.
193.	PEERSTAUP	5	"Heartbeats getting exchanged with peer [ip], group ID [uint] in standby mode	The standby peer is observable.
194.	PEERACTIVEDOWN	4	"Peer [ip], with group ID [uint] in active mode is down	Error in the update message from the peer. The connection will come down. Re-establish the connection.
195.	PEERSTADOWN	4	"Peer [ip], with group ID [uint] in standby mode is down	Error in the update message from the peer. The connection will come down. Re-establish the connection.
196.	PEERACTIVEINVLCONF	1	"Peer [ip], with group ID [uint] in active mode has detected with invalid configuration	The redundancy configuration has to be identical across the entire cluster. Consequently, a misconfiguration has been detected.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
197.	PEERSTAINVLCONF	1	"Peer [ip], with group ID [uint] in standby mode has detected with invalid configuration	The redundancy configuration has to be identical across the entire cluster. Consequently, a misconfiguration has been detected.
198.	PEERACTIVEOPER	5	"Peer [ip], with group ID [uint] in active mode is fully operational	The primary peer is fully operational.
199.	PEERSTAOPER	5	"Peer [ip], with group ID [uint] in standby mode is fully operational	The standby peer is fully operational.
200.	STATEDISABLED	6	The wireless module has changed its redundancy state to disabled	Redundancy needs to be disabled by users to be consistent with switch redundancy state.
201.	STATESTARTUP	6	The wireless module has changed its redundancy state to startup	Redundancy needs to be enabled by users to be consistent with switch redundancy state.
202.	STATEDISCOVERY	6	The wireless module has started discovering other members in the redundancy group	Discovery process has started for the cluster group.
203.	STATEONLINE	6	The wireless module has started adopting radio ports actively	Discovery is conmpleted and a connection to peer is established.
204.	REDUNDANCYDISABLED	5	Redundancy protocol disabled	Redundancy is disabled
205.	REDUNDANCYENABLED	5	Redundancy protocol enabled	Redundancy is enabled.
206.	AUTHORIZATIONCHNGD	1	Redundancy group authorization level changed to [uint]	The License level changed. Required support levels have either been increased or decreased.
207.	BADCMD	4	"Command Execution Failed, Invalid Command: <[str]>	Invalid command used in the startup config. If needed, troubleshoot startup config.
208.	AMBIGUOUSCMD	4	"Command Execution Failed, Ambiguous Command: <[str]>	Ambiguous command in startup config. If needed, troubleshoot startup config.
209.	INCOMPLETECMD	4	"Command Execution Failed, Incomplete Command: <[str]>	Incomplete command in startup config. If needed, troubleshoot startup config.
210.	USERAUTHSUCCESS	5	User '[str]' logged in with role of '[str]' from auth source '[str]	The user has successfully logged in.
211.	USERUPDATE	6	User '[str]' updated with use roles of '[str]' and allowed access from '[str]	A new or existing user now has a new set or user access permissions.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
212.	USERDELETE	5	User '[str]' deleted	An existing user has been deleted and removed from the list available for switch resources.
213.	AUTHNOTIFY	5	Radius server secret not configured or server not reachable. Hence trying next auth method	User access denied. Now trying next auth method since the Radius server is not reachable or properly configured.
214.	DIAGSHELL	6	Diag shell started with parameter [int] [str]	Possible reasons include: • Testing entry from imi shell • Normal exit from imi shell • LINE_CODE_ERROR reading line • readn returned <= 0, error or null length • Bad header length read" • No line body after reading header info
215.	USERAUTHFAIL	3	User '[str]' can not be authenticated	Bad password used in authetnication attempt. Attempt authentication again using correct passowrd.
216.	IFUP	6	Interface [str] is up	Ethernet interface is up.
217.	IFDOWN	4	Interface [str] is down	Ethernet interface is down
218.	DHCPIP	6	Interface [str] acquired IP address [ip]/[uint] via DHCP	Interface has aquired an IP address using DHCP.
219.	DHCPDEFRT	6	Default route with gateway [ip] learnt via DHCP	Default route for gateway has been acquired through DHCP.
220.	DHCPIPCHG	5	"Interface [str] changed DHCP IP - old IP: [ip]/[uint], new IP: [ip]/[uint]	The IP address provided by the DHCP server is different from previous lease.
221.	DHCPNODEFRT	5	Interface [str] lost its DHCP default route	Interface is disabled for DHCP and therefore leaving its default route to gateway.
222.	FREEFLASHDISK	6	"Free [str] file system space, [str]% is less than limit	The current file system space is less than the minimum limit of 10%. Could result when files are saved on the switch. Delete files when required to create the necessary space.
223.	KERNEL-4-WARNING	4	"Queue to user space full, packet throttled=%d	Queue for user space full and a warning has been generated.
224.	KERNEL-4-WARNING	4	crypt: enabling countermeasures on WLAN %	

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
225.	KERNEL-4-WARNING	4	"tkip: station replay counters out of sync for ""MACSTR"". deauthing	TKIP authentication failed, as counters are out of sync in TKIP request. Validate TKIP credentials and re-attempt.
226.	KERNEL-4-WARNING	4	"aes: station replay counters out of sync for ""MACSTR"". deauthing	AES authentication failed, as counters are out of sync in TKIP request. Validate AES credentials and re-attempt.
227.	KERNEL-4-WARNING	4	PS_Decrypt:line Unknown bcast/ucast encryption type: %d	Unknown encryption information within the broadcast/unicast data.
228.	KERNEL-4-WARNING	4	"mic check failure ""MACSTR"". got: ""MACSTR"" calc: ""MACSTR	
229.	KERNEL-4-WARNING	4	Get_Udp_Ptr: wrong IP version	BAD IP packet received. If necessary, check IP versus expected address.
230.	KERNEL-4-WARNING	4	"flowctl: bad tx_res, retries=%d, rate=%d	BAD flow control warning.
231.	KERNEL-4-WARNING	4	"fc:mu removed before fc ack on prtl ""MACSTR	An MU has been removed before a flow control ACK. If required, re-associate MU.
232.	KERNEL-4-WARNING	4	"fc:dropped assoc resp pkt to ""MACSTR	An association response packet has been dropped. Validate the success of the association attempt, and (if needed) try again.
233.	KERNEL-4-WARNING	4	"fc:mu removed before fc tx on prtl ""MACSTR	An MU has been removed before a transmission attempt could be initiated.
234.	KERNEL-4-WARNING	4	"fc:prevent tx to unreachable mu ""MACSTR	Transmissions to an unreachable MU have been prevented. If required, re-initiate connection attempt to MU.
235.	KERNEL-4-WARNING	4	"mismatch(roam?): dest=""MACSTR	
236.	KERNEL-4-WARNING	4	std: pkt sent % not in ack queue	Packet sent information is not within the ACK queue.
237.	KERNEL-4-WARNING	4	mgmt fc: send failed seq %d not in ack queue	
238.	KERNEL-4-WARNING	4	"MACSTR"" ack q is null for seq:0x%08x	The ACK queue is null for this attempt.
239.	KERNEL-4-WARNING	4	"MACSTR"" lost seq: %d, res:%x	

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
240.	KERNEL-4-WARNING	4	Update_MU_State : wrong IP version	Wrong IP address information within an update MU state request. Validate IP address information (if necesary) and re-attempt request.
241.	KERNEL-4-WARNING	4	"PAL_ESS_Data : de-auth ""MACSTR"" tx'ing on wrong radio:""MACSTR"" should be on""MACSTR	De-authentication was the result of a transmission on a wrong (undefined) radio.
242.	KERNEL-4-WARNING	4	"pshandle:de-authing ""MACSTR"". unknown src-addr in ctl frame	Unknown address in a control frame results in deauthentication.
243.	KERNEL-4-WARNING	4	received unconfigured VLAN id %d	A unconfigured VLAN ID was received. Interoperations with this VLAN requires the correct ID.
244.	KERNEL-4-WARNING	4	pal: Send_2_CC call failed for a deauth-req	
245.	KERNEL-4-WARNING	4	pal: Send_2_CC call failed for mu-remove-req	An MU association removal request has failed. Attempt to remove the MU again.
246.	KERNEL-4-WARNING	4	warning: rx data from unknown portal	Data has been received from an unknown portal location. This is an informational warning and should be checked periodically to ensure its not repeated and the source represents a viable threat.
247.	KERNEL-4-WARNING	4	Unreal dt(tx_pkt) @ rate %d: 0x%08lx - 0x%08lx = 0x%08lx\	
248.	KERNEL-4-WARNING	4	Unreal dt(retry) @ %d: 0x%08lx - 0x%08lx = 0x%08lx	
249.	KERNEL-4-WARNING	4	Unreal delta tx-fail: 0x%08lx - 0x%08lx = 0x%08lx	
250.	KERNEL-4-WARNING	4	"capwap skb length underrun: received %d, expected %d	
251.	KERNEL-4-WARNING	4	"radio ""MACSTR"" lost first frag of seq %04x till %04x	
252.	KERNEL-4-WARNING	4	"radio ""MACSTR"" lost seq %u to %u	
253.	KERNEL-4-WARNING	4	warning: unable to queue skb	

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
254.	KERNEL-4-WARNING	4	warning: rx wisp data from unknown portal	WISP data has been received from an unknown portal location. This is an informational warning and should be checked periodically to ensure its not repeated and the source represents a viable threat.
255.	KERNEL-4-WARNING	4	"psp_tx_unicast dropping skb to unreachable mu ""MACSTR	Unreachable MU. Ensure target MU is a viable MU in the wireless network.
256.	KERNEL-4-WARNING	4	"psp:dropped %d bytes unicast to ""MACSTR	
257.	KERNEL-4-WARNING	4	"psp:deauthing ""MACSTR"" due to max-tx-fails	Station being de-authenticated due to the maximum permitted transmission failures being exceeded.
258.	KERNEL-4-WARNING	4	Update_WHS_State: wrong IP version	Wrong IP version creating compatibility issues.
259.	KERNEL-3-ERROR	3	WLAN Index is not supported	For hotspot feature. Error is seen when destination IP is check in the WHITE IP list and WLAN index is bad.
260.	KERNEL-3-ERROR	3	CCdev_read: bug in circular index computation rd %d wr %d" "tot_entry %d to_read %d rcc %d	Index not being correctly defined and an index computation loop has been created.
261.	KERNEL-3-ERROR	3	1. dev_read copy error rcc %d ccdev : Mob CCdev_Read copy_to_user error	Read copy error encountered.
262.	KERNEL-3-ERROR	3	2. dev_read copy error rcc %d ccdev : Mob CCdev_Read copy_to_user error	Read copy error encountered.
263.	KERNEL-3-ERROR	3	ccdev : CCdev_Read copy_to_user error	Read copy error encountered.
264.	KERNEL-3-ERROR	3	ccdev : Handle_VLAN bad cmd->index %d	Read copy error encountered.
265.	KERNEL-3-ERROR	3	ccdev : Handle_VLAN no VLAN cfg for idx %d	No VLAN configuration defined for supplied ID.
266.	KERNEL-3-ERROR	3	ccdev : Handle_VLAN bad cmd id : %d	
267.	KERNEL-3-ERROR	3	CCdev_Ioctl : bad ioctl_num %d	
268.	KERNEL-3-ERROR	3	ccdev : CC server not up	Unreachable CC Server.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
269.	KERNEL-3-ERROR	3	Error registering ccdev	An error has been encountered registering ccdev.
270.	KERNEL-3-ERROR	3	Error unregistering ccdev	An error has been encountered unregistering ccdev.
271.	KERNEL-3-ERROR	3	invalid WLAN index: %d	Invalid WLAN index encountered. Verify correctness of WLAN index.
272.	KERNEL-3-ERROR	3	unknown bcast/ucast encryption type %d	Unknown or erroneous broadcast or unicast encryption scheme encountered.
273.	KERNEL-3-ERROR	3	DHCP_Get_Msg_Type : bad cookie	Bad cookie encountered with DHCP_Get_Msg_Type request.
274.	KERNEL-3-ERROR	3	pkt0 has not been created	Packet 0 has not been created.
275.	KERNEL-3-ERROR	3	device eth1/eth2 needs to be re-installed	Device using the switch Eth1 or Eth2 resources requires re-installation.
276.	KERNEL-3-ERROR	3	send from Linux no free skb	
277.	KERNEL-3-ERROR	3	Error initializing virtual device	A virtual device initialization error has been encountered.
278.	KERNEL-3-ERROR	3	"MACSTR"" prtl window wrap curr=%u, new=%u	
279.	KERNEL-3-ERROR	3	"MACSTR"" wisp seq %u != fc seq=%u setting to %u	
280.	KERNEL-3-ERROR	3	fc alloc:no memory for fc allocs	No memory exists currently for fc allocations.
281.	KERNEL-3-ERROR	3	"MACSTR"" fc ack timeout:curr %u,acktime=%u	FC ACK timeout threshold value has been exceeded.
282.	KERNEL-3-ERROR	3	"MACSTR"" fc no prtl traffic in last %d secs	No portal traffic detected over the last “N” number of seconds.
283.	KERNEL-3-ERROR	3	"flowctl : bad tx_ctl %x	
284.	KERNEL-3-ERROR	3	"MACSTR"" std queue: can't tx, fc blocked	Transmission error encountered. FC management currently blocked.
285.	KERNEL-3-ERROR	3	"MACSTR"" can't tx, fc mgmt blocked	Transmission error encountered. FC management currently blocked.
286.	KERNEL-3-ERROR	3	"Unknown fc_type = %d on ""MACSTR	Unknown fc type encountered.
287.	KERNEL-3-ERROR	3	"flowctl: num_pkts_on_portal = 0, ac_idx = %d can't dec	No packets detected over portal. Possible decoding error.
288.	KERNEL-3-ERROR	3	"%d not found in ack queue for ""MACSTR	For TX results – sequence no found.
289.	KERNEL-3-ERROR	3	Invalid Wisp cmd id: 0x%04X	Found bad WISP command ID when updating flow control results.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
290.	KERNEL-3-ERROR	3	psp update tim: alloc skb failed	Could not allocate buffer needed to send heartbeat message.
291.	KERNEL-3-ERROR	3	Hotspot: Netdevice does not exists for interface VLAN %d	Valid tunnel was not found for given IP and VLAN tag.
292.	KERNEL-3-ERROR	3	Hotspot: Device is null	
293.	KERNEL-3-ERROR	3	Mob_Sw_To_HS : skb2tun copy failed.	
294.	KERNEL-3-ERROR	3	Mob_Sw_BCMC_To_CS_Tunnels : skb2tun copy failed.	
295.	KERNEL-3-ERROR	3	PAL_ESS_Data: invalid data sub type %X	Invalid data sub type
296.	KERNEL-3-ERROR	3	PAL_Process_ESS : 802.11 data pkt too small (%d bytes)	Recieved 802.11 packet with bad length.
297.	KERNEL-3-ERROR	3	PAL_Process_ESS: unknown frame type %x	Unknown 802.11 frame type encountered. Not necessarily data, control or management.
298.	KERNEL-3-ERROR	3	PAL_Tx_BCMC_To_Bss : new_skb allocation failed	
299.	KERNEL-3-ERROR	3	VLAN id %d out of range	VLAN is bigger than 4128. Sent when trying to create broadcast for all BSSIDs.
300.	KERNEL-3-ERROR	3	"Multicast Flooding Detected, limiting the segments in broadcast domain to %d	To eliminate flooding, each broadcast should not be sent to more than 32 BSSIDs.
301.	KERNEL-3-ERROR	3	"PAL_Unicast_To_WLAN : MU ""MACSTR"" has a null prtl	There are no known APs for this MU.
302.	KERNEL-3-ERROR	3	Send_ARP_Resp: skb alloc failed	Cannot allocate memory required to send ARP response.
303.	KERNEL-3-ERROR	3	PC_Rx_From_CC : CC sending data pack to unknown MU	Upper layer send packet to unknown MU – for capwap path.
304.	KERNEL-3-ERROR	3	pshandle:failed to allocate roam skbuf	Cannot allocate packet required for roam notification.
305.	KERNEL-3-ERROR	3	PS_Wisp_Rx_From_CC : CC sending data pack to unknown MU	Upper layer send packet to unknown MU – for legacy WISP.
306.	KERNEL-3-ERROR	3	psp update tim: alloc skb failed	Cannot allocate buffer required to send Update TIM message to AP.
307.	KERNEL-3-ERROR	3	psp store: out of memory	Cannot store PSP packet.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
308.	KERNEL-3-ERROR	3	dtim poll: recvd bad bss index	Received bad BSS in DTIM_POLL message. This is for legacy WISP only.
309.	KERNEL-3-ERROR	3	Get_Lower_Rate : curr = %d allowed = %x	Cannot get lower rate.
310.	KERNEL-3-ERROR	3	Get_Higher_Rate : curr = %d allowed = %x	Cannot get higher rate.
311.	KERNEL-3-ERROR	3	ratescale : no highest rate = %x	Rate is set to 54 Mbps.
312.	KERNEL-3-ERROR	3	"ratescale : invalid attempts = %u, pkts = %u	
313.	KERNEL-3-ERROR	3	fragment too big to copy:%d bytes	Got bad fragment packet.
314.	KERNEL-3-ERROR	3	reassy:unknown cmd type	Bad command in WISP fragmented packet.
315.	KERNEL-3-ERROR	3	error:fragment too big to copy:%d bytes	WISP fragment is too big
316.	KERNEL-3-ERROR	3	PS_Frag_Send unable to alloc skb	If a packet is bigger than 1514, it will be fragmented. However, the buffer can't be allocated.
317.	KERNEL-3-ERROR	3	PS_BCMC_Frag_Send unable to alloc skb	Big BCMC packet, can't allocate memory for fragment.
318.	KERNEL-3-ERROR	3	"rssi : bad vals ap = %d, rd = %d, rssi = %d	If RSSI value is bigger than 255, or smaller than 0 (or unknown radio), when attempting to convert RSSI to DBM.
319.	KERNEL-3-ERROR	3	Tunnel Pre-Routing: skb linearize failed	
320.	KERNEL-3-ERROR	3	Tunnel Pre-Routing: No free skb	
321.	KERNEL-3-ERROR	3	Tunnel Post-Routing: No free skb	
322.	KERNEL-3-ERROR	3	Tunnel_Init: can't register Tunnel_Pre_Routing hook	Tunnel initialization error encountered. Cannot register tunnel pre-routing hook.
323.	KERNEL-3-ERROR	3	Tunnel_Init: can't register Tunnel_Post_Routing hook	Tunnel initialization error encountered. Cannot register tunnel pre-routing hook.
324.	KERNEL-3-ERROR	3	null device passed to get stats routine	Unavailable device has been forwarded for statistics gathering.
325.	KERNEL-3-ERROR	3	null priv pointer in get stats	Stats generation failure occured when collecting data.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
326.	KERNEL-3-ERROR	3	null device passed to probe routine	Unavailable device incorrectly forwarded to a probe routine.
327.	KERNEL-3-ERROR	3	null device passed to close routine	Unavailable device incorrectly forwarded to a probe routine.
328.	KERNEL-3-ERROR	3	null device passed to probe routine	Unavailable device incorrectly forwarded to a probe routine.
329.	KERNEL-3-ERROR	3	VLAN_Handle_Ingress unable to get VLAN config for %s	Packet received from a trunked interface with VLAN tag
330.	KERNEL-3-ERROR	3	"VLAN_Handle_Ingress untagged pkt on %s dropped, no untagged VLAN set	Got untagged packet on a VLAN interface.
331.	KERNEL-3-ERROR	3	VLAN_Handle_Egress: skb had no VLAN tag. dropping	Missing VLAN tag in the packet that we are sending. Should be set already.
332.	KERNEL-3-ERROR	3	PAL_Tx_BCMC_To_Wired : skb copy failed.	
333.	KERNEL-3-ERROR	3	PAL_Tx_BCMC_To_Ron : skb2ron copy failed.	
334.	KERNEL-3-ERROR	3	PAL_Tx_BCMC_To_Linux : skb2ron copy failed.	
335.	KERN-6-INFO	6	Add WTP at N	Adds a WTP entry to the table. WTP is a CAPWAP definition for AP.
336.	KERN-6-INFO	6	"Prtl <MAC>"" add @ N	Adds an AP entry to the table.
337.	KERN-6-INFO	6	Prtl <MAC> rem @ N	Deletes an AP entry from the table.
338.	KERN-6-INFO	6	mu <MAC> w/ aid N added to prtl <MAC>	Adds MU to an AP.
339.	KERN-6-INFO	6	mu <MAC> w/ aid N removed from prtl <MAC> - bss_idx N	Removes MU from an AP.
340.	KERN-6-INFO	6	crypt: disabling countermeasures on WLAN N	Disabling countermeasures.
341.	KERN-6-INFO	6	"WEP Decrypt Failed ""MU MAC	Failed to decrypt WEP encrypted packet.
342.	KERN-6-INFO	6	"Tkip/keyguard decrypt failure: ""MAC"" iv32 = 0xX iv16 = 0xX	Tkip.Keyguard decryption failed.
343.	KERN-6-INFO	6	"TKIP Replay check fail ""MAC"" got: X expecting X	Replay check failure.
344.	KERN-6-INFO	6	"ccmp decrypt failed ""MACSTR"" (%u bytes)	Decryption of packet that have been encrypted using AES-CCMP failed

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
345.	KERN-6-INFO	6	"aes replay check failed ""MAC"" got: X expected: X	Replay check failed for AES-CCMP packet
346.	KERN-6-INFO	6	qos admission control verification failed	WMM admission control check failed.
347.	KERN-6-INFO	6	"rx encrypted frame from ""MAC"" when policy is no encryption.	Encrypted packet received on non-encrypted WLAN.
348.	KERN-6-INFO	6	"dropping clear frame from ""MACSTR"". policy requires encryption	Received packet was expected to be encrypted.
349.	KERN-6-INFO	6	"EWEP bit in WEP hdr = 1, Expected 0 ""MAC"	For WEP64 and WEP128 traffic.
350.	KERN-6-INFO	6	"EWEP bit in WEP hdr = 0, Expected 1 ""MAC	For Keyguard and TKIP and CCMP traffic.
351.	KERN-6-INFO	6	"AES-CCMP encrypt failed ""MAC	Encryption failure occurred.
352.	KERN-6-INFO	6	qos admission control verification failed	Unicast packet did not pass WMM admission control.
353.	KERN-6-INFO	6	Driver - deliver to Linux VLAN N	Packet destined to VLAN.
354.	KERN-6-INFO	6	rx from Linux	Packet received from Linux source.
355.	KERN-6-INFO	6	flowctl: no stats update for dropped seq N	No stats available for target dropped sequence.
356.	KERN-6-INFO	6	"fc:dropped N consec pkts to ""MAC"	
357.	KERN-6-INFO	6	"fc:mu [""MAC""] in psp, dropped packet N	MU in PSP mode has dropped a packet.
358.	KERN-6-INFO	6	"MACSTR"" fc window wrap curr=N, new=Y	
359.	KERN-6-INFO	6	fc allocs:q full	
360.	KERN-6-INFO	6	fc:allocs back down to N	
361.	KERN-6-INFO	6	"fc freed ack q pkt seq N, tx time U, now Y	
362.	KERN-6-INFO	6	fc q extract:seq N not found in Y entries	Target sequence not found in target entries.
363.	KERN-6-INFO	6	""MAC"" fc send failure	
364.	KERN-6-INFO	6	"flowctl Q-Full WLAN %d, ac %d (%d/%d)	
365.	KERN-6-INFO	6	"MACSTR"" std queue:alloc failed, curr %d	
366.	KERN-6-INFO	6	"MACSTR"" std q:failed	

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
367.	KERN-6-INFO	6	"MACSTR"" fc mgmt q:alloc failed	
368.	KERN-6-INFO	6	"MACSTR"" fc mgmt q:failed	
369.	KERN-6-INFO	6	fc can't send	
370.	KERN-6-INFO	6	mgmt fc can't send	
371.	KERN-6-INFO	6	"MACSTR"" fc free queues	
372.	KERN-6-INFO	6	"MACSTR"" fc window wrap around curr = %d, new = %d	
373.	KERN-6-INFO	6	Update_MU_State: wrong arp prot %x	MU state updated, as the wrong ARP protocol has been used.
374.	KERN-6-INFO	6	"PAL_ESS_Data : de-authing unknown MU ""MACSTR"" on BSS ""MACSTR	Unknown MU has been deauthenticated.
375.	KERN-6-INFO	6	PAL_Rx_From_WLAN	
376.	KERN-6-INFO	6	proxy arp resp was sent	A proxy ARP response was sent.
377.	KERN-6-INFO	6	PD_Tx_To_Linux	
378.	KERN-6-INFO	6	PD_Tx_To_Wire	
379.	KERN-6-INFO	6	PAL_Defrag_ESS_Data	
380.	KERN-6-INFO	6	PAL_Unicast_To_WLAN	
381.	KERN-6-INFO	6	"Non-IP pkt, no DSCP bits. Default DSCP to 0x08	
382.	KERN-6-INFO	6	PAL_Unicast_From_LAN	
383.	KERN-6-INFO	6	from switch. Sending to wire	
384.	KERN-6-INFO	6	"dropping pkt src:""MACSTR"" dst:""MACSTR	Unknown destination
385.	KERN-6-INFO	6	"dropping wisp packets to another switch ""MACSTR	WISP packets to another switch have been dropped.
386.	KERN-6-INFO	6	"dropping L2 wisp packets in wrong direction, cmd=0x%04x	Each L2 WISP packet that was sent in the wrong direction has been dropped.
387.	KERN-6-INFO	6	wrong arp prot %x	
388.	KERN-6-INFO	6	gratuitous arp from ip=%u.%u.%u.%u	Gratuitous ARP received from target address.
389.	KERN-6-INFO	6	"arp resp: smac=""MACSTR "", sip=%u.%u.%u.%u dmac=""MACSTR	

Number	***Mnemonic***	***Severity***	***Syslog Message***	***Meaning / Cause***
390.	KERN-6-INFO	6	warning: rx data from unknown portal	Warning message stating data has been received from an unknown source (portal).
391.	KERN-6-INFO	6	"Rx inactive mu stats for unknown/inactive mu: "" MACSTR	No longer receiving stats for an inactive or unknown MU.
392.	KERN-6-INFO	6	"PC_Rx_From_CC (): packet failed encryption	Received packet was not able to correctly encrypt.
393.	KERN-6-INFO	6	no tail room to fix for runt packet	Runt packet fix could not be accomodated.
394.	KERN-6-INFO	6	"pshandle:mu ""MACSTR"" roamed	Target MU inadvertently roamed.
395.	KERN-6-INFO	6	warning: rx wisp data from unknown portal	Warning message stating WISP data has been received from an unknown source (portal).
396.	KERN-6-INFO	6	ps_rx_from_cc: no portal to queue to	Received packet has no portal to queue to.
397.	KERN-6-INFO	6	ps_rx_from_cc: packet failed encryption	Received packet was not able to correctly encrypt.
398.	KERN-6-INFO	6	"prtl ""MACSTR"" bss %d psp queue full with %d pkts	
399.	KERN-6-INFO	6	"psp:mu ""MACSTR"" authenticating	
400.	KERN-6-INFO	6	psp:free mu queue	
401.	KERN-6-INFO	6	psp:free portal queues	
402.	KERN-6-INFO	6	"MACSTR"" rate[%s to %s], [%d/%d], pct:%d	
403.	KERN-6-INFO	6	"Tunnel_Pre_Routing: BCAST: dip=%u.%u.%u.%u, VLAN=%d	
404.	KERN-6-INFO	6	"Tunnel_Pre_Routing: MCAST: dip=%u.%u.%u.%u, VLAN=%d	
405.	KERN-6-INFO	6	"Tunnel_Pre_Routing: SUBNET-BCAST: dip=%u.%u.%u.%u, VLAN=%d	
406.	KERN-6-INFO	6	"Tunnel_Pre_Routing: DHCP: MU=%u.%u.%u.%u, VLAN=%d	

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
407.	KERN-6-INFO	6	"Tunnel_Pre_Routing: MU=%u.%u.%u.%u not found, VLAN=%d	
408.	KERN-6-INFO	6	"Tunnel_Pre_Routing: UCAST: dip=%u.%u.%u.%u, VLAN=%d	
409.	KERN-6-INFO	6	Tunnel_Post_Routing: MU=%u.%u.%u.%u not found	
410.	KERN-6-INFO	6	Tunnel_Post_Routing: Sending packet to MU %u.%u.%u.%u	
411.	KERN-6-INFO	6	%s: Unknown tunnel=%s	Unknown tunnel attributes.
412.	KERN-6-INFO	6	"Tunnel_Send_Pkt: Sending out on %s, dmac=""MACSTR	
413.	KERN-6-INFO	6	wrong arp prot %x	Wrong ARP protocol used.
414.	KERN-6-INFO	6	Tunnel_Gw_Proxyarp: Not an ARP REQ	Tunnel gateway proxy ARP not an appropriate ARP request.
415.	KERN-6-INFO	6	"Tunnel_Gw_Proxyarp: ARP REQ from MU for IP=%u.%u.%u.%u, gw=%u.%u.%u.%u	
416.	KERN-6-INFO	6	Tunnel_Gw_Proxyarp: ARP req not for gw-ip	
417.	KERN-6-INFO	6	Tunnel_Deliver_To_Linux: Dropping non-IP pkt	Non IP packets dropped.
418.	KERN-6-INFO	6	"%s tagged pkt on %s dropped, port not tagged member of %d	
419.	KERN-6-INFO	6	W_Host_Idle_Timeout : wrong arp prot %x	The wrong ARP protocol resulted in a host idle timeout.
420.	KERN-6-INFO	6	"%s : session-timeout for Wired-host ""MACSTR	Session timeout for wired host.
421.	KERN-6-INFO	6	"W_Host_Idle_Timeout : idle-timeout for Wired-host ""MACSTR	Host idle timeout for wired host
422.	KERN-6-INFO	6	"create_wired_host : Wired-host ""MACSTR"" created!	Wired host has been created.
423.	AUTH-3-ERR: WIOS_SECURITYMGR	3	Malformed IKE identity `%s	Remote ID for aggressive mode IKE SA cannot be decoded.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
424.	AUTH-3-ERR: WIOS_SECURITYMGR	3	Malformed IKE secret	Pre-shared key for aggressive mode IKE SA cannot be decoded.
425.	AUTH-3-ERR: WIOS_SECURITYMGR	3	Could not force CA certificate as a point of trust	CA certificate could not be used as/ with trustpoint.
426.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Can not insert CA certificate into local database	The CA certificate will not insert into the local database. Either resolve issue with this certificate or use a different one.
427.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Message: Malformed IKE SA proposal	Error displayed when checking if IKE security association proposal matches.
428.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Reason: Invalid protocol ID %d, should be %d	Invalid protocol ID. The result is a malformed IKE security association proposal.
429.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Reason: Protocol %d given more that once	Protocol is specified multiple times in IKE security association proposal. The result is a malformed IKE proposal.
430.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Reason: Invalid transform identifier %d, "" ""should be %d	Transform identifier invalid. IKE security association proposal check will fail.
431.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Reason: No key-length proposed for "" ""variable key-length cipher %s	Variable key length cipher is specified in IKE SA proposal, but the key length attribute is missing.
432.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Neither pre-shared keys nor CA certificates are "" ""specified for a tunnel	There is no pre-shared key or certificates specified for tunnel. Ensure they are available for this request.
433.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""AES counter mode cannot be used without an "" ""authentication algorithm	A tunnel check has failed because of using an AES counter mode with the authentication algorithm.
434.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""AES counter mode cannot be used with manual keys	A tunnel check has failed because of using an AES counter mode with manual keys.
435.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Tunnel does not specify any keying method "" ""(IKE or manual)	A tunnel check has failed because of using no keying method (i.e. IKE or manual defined for tunnel).
436.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"Auto-start rule does not specify single IP address "" ""or domain name for its remote peer	The post auto-start rule check has failed. The user did not provide enough information to (remote IKE peer and IP address) establish the rule automatically.
437.	AUTH-3-ERR: WIOS_SECURITYMGR	3	Both REJECT and PASS defined for a rule	Both the reject and pass flags for a rule are on. Policy manager use these flag to reject or pass the rule.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
438.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"The AUTHENTICATION-ONLY can be specified only for "" ""PASS rules	Authentication flag must not be set for DENY rule.
439.	AUTH-3-ERR: WIOS_SECURITYMGR	3	To-tunnel specified for a REJECT rule	Cannot set rejetct rules on To-tunnel.
440.	AUTH-3-ERR: WIOS_SECURITYMGR	3	No from-tunnel specified for an AUTHENTICATION-ONLY rule	FROM-TUNNEL cannot be null if authentication-only flag is set.
441.	AUTH-3-ERR: WIOS_SECURITYMGR	3	To-tunnel specified for an AUTHENTICATION-ONLY rule	To-tunnel cannot be null if authentication-only flag is set.
442.	AUTH-3-ERR: WIOS_SECURITYMGR	3	The maximum number of policy rules reached	Max number of policy rule is 600 i.e. four times the number of maximum tunnels.
443.	AUTH-3-ERR: WIOS_SECURITYMGR	3	IP protocol not specified for this service element.	IP protocol not specified for this service element.
444.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"Cannot insert this rule, the forced NAT protocol"" "" type does not match rule protocol	The selected rule cannot be used, as the type does not match the rule protocol in effect.
445.	AUTH-3-ERR: WIOS_SECURITYMGR	3	Message: negotiation aborted	Following one message is reason for this message.
446.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Reason: AH can not be initiated with NAT-T	NAT traversal cannot be used with AH mode, as it has run hash on the IP addresses.
447.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Message: malformed IPSec SA proposal	There is a malformed IPSec SA proposal.
448.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Reason: Inconsistent encapsulation modes:" "current %d, new %d"	The current and new encapsulation mode is not same. Ensure they are consistent.
449.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Reason: unknown encapsulation mode %d proposed	The encapsulation mode specified for an IPSec security association is not recognized.
450.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Reason: Protocol %d given more than once	The encapsulation protocol is defined more than once in the security association proposal
451.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Message: malformed IPSec ESP proposal	There is a malformed IPSec ESP proposal.
452.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"Reason: No key-length proposed for "" "variable key-length cipher %s	A variable key length cipher is specified in IPSec ESP proposal, but the key length attribute is missing.
453.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Message: malformed IPSec AH proposal	Following two messages are reason for this message.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
454.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""Reason: AH authentication algorithm ID %s (%d) "" ""does not match AH transform %s (%d).	The AH authentication algorithm ID does not matchthe AH transform being used.
455.	AUTH-3-ERR: WIOS_SECURITYMGR	3	" Reason: No key-length proposed for " "variable key-length algorithm %s"	A variable key length cipher is specified in the IPSec AH proposal, but a key length attribute is missing.
456.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Could not select proposal for IPSec SA %d	A proposal could noty be selected for the IPSec security association.
457.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Message: Could not select policy rule	A policy rule could not be successfully selected for security policy. Try a different policy rule.
458.	AUTH-3-ERR: WIOS_SECURITYMGR	3	""" Message: Could not select SA from IPSec SA "" ""proposal	A security association could not be specified from the IPSec security association proposal.
459.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Tunnel is already specified to be manually keyed"")	The target tunnel for the authentication request is already defined to be manually keyed.
460.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""ESP tunnel is missing encryption and authentication "" ""algorithms	Supply an encryption algorithm for ESP tunnel. Supply a NULL attribute if not using encryption.
461.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""ESP tunnel is missing encryption algorithm "" ""(the NULL encryption algorithm must be specified "" ""if no encryption is required)	Supply an encryption algorithm for ESP tunnel. Supply a NULL attribute if not using encryption.
462.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""ESP NULL-NULL is proposed for this tunnel. "" ""This is forbidden by RFC 2406."")	Ensure ESP NULL-NULL is not specified for the tunnel to avoid a violation of RFC 2406.
463.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""AH tunnel is missing authentication algorithm	Ensure AH authentication algorithm is supplied with AH supported tunnel.
464.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""AH is not supported	If AH is not support, use a different authentication mechanism.
465.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""IPComp tunnel is missing compression algorithm	Add compression algorithm to IPComp tunnel.
466.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""IPComp is not supported	IPComp is not supported.
467.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Anti-replay detection must be enabled when using" ""64 bit sequence numbers."	If a 64-bit sequence is to be used, enable anti-replay detection.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
468.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""No IPSec transform (AH or ESP) specified for tunnel	Specify a AH or ESP transform for tunnel.
469.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""The `per-port' or `per-host' SA flags can not be "" ""specified for `auto-start' tunnels	Security association per-port and per-flag attributed could not be specified for an auto-start tuunel
470.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Both `auto-start' and `dont-initiate' specified "" ""for a tunnel	This error is generated when the user tries to configure both, Auto-start and dont- initate, for a tunnel at the same time.
471.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Out of memory. Could not allocate memory for "" ""tunnel name!	Tunnel name could not be accounted for due to memory constraints. Free up necessary memory.
472.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Malformed IKE identity `%s' for tunnel"", identity	The IKE secret identity used has corrupt characters. Create a new one with usable parameters.
473.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Malformed IKE secret for tunnel	The IKE secret password used has corrupt characters. Create a new secret with usable parameters.
474.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Extended (64 bit) "" ""sequence numbers are not supported for manually keyed "" “tunnels	Extended (64 bit) sequence numbers not supported for manually keyed tunnels. Do not use extended 64 bit.
475.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Invalid SPI values specified for ESP: in=%08x, out=%08x	Invalid SPI values specified for ESP authentication credentials.
476.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Invalid SPI values specified for AH: in=%08x, out=%08x"",	Invalid SPI values specified for AH authentication credentials.
477.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Invalid CPI values specified for IPComp: "" ""in=%04x, out=%04x	Invalid CPI values specified for IPComp.
478.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Tunnel is already specified to be IKE keyed	The requested tunnel is already specified to be IKE keyed.
479.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Manual key already configured	Manual key credentials have already been configured. Do not change their values or use a different key.
480.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Malformed manual key for tunnel	Manual key credentials are malformed and cannot be used.
481.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Manual key tunnel specifies ambiguous algorithms	Manual key tunnel specifies ambiguous algorithms. Use a different key or rectify ambiguous algorithms.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
482.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"Too little key material for manually keyed tunnel. " "Needs %u bytes but got only %u bytes"	Too little key material for manually keyed tunnel. Update the number of bytes used.
483.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"Too much key material for manually keyed tunnel. " "Needs only %u bytes but got %u bytes"	Byte limit exceeded for manual key. Ensure the key size is not too long.
484.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Invalid key sizes specified	Invalid key size specified. Ensure the key size is consistent with what is expected.
485.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Algorithm key sizes specified for unknown algorithm	Key sizes specified for unknown algorithm. Validate expected key size before continuing.
486.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""Key size limits specified for fixed key size "" ""cipher %s	A fixed key size must be used.
487.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""The maximum cipher key size %u is bigger than "" ""the built-in maximum %u	Maximum cipher key size too large for expected. Reduce key size or use a different key.
488.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""The maximum cipher key size %u is bigger than "" ""the built-in maximum %u	Maximum cipher key size too large for expected. Reduce key size or use a different key.
489.	AUTH-3-ERR: WIOS_SECURITYMGR	3	"""The maximum cipher key size %u is bigger than "" ""the built-in maximum %u	Maximum cipher key size too large for expected. Reduce key size or use a different key.
490.	AUTH-3-ERR: WIOS_SECURITYMGR	3	Remote IKE peer %@%@	Remote machine where the tunnel terminates.
491.	AUTH-3-ERR: WIOS_SECURITYMGR	3	Local IKE peer %@%@	Local machine which initiates the tunnel.
493.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""The maximum number of active Phase-1 SAs reached	The maximum number of active phase 1 security associations has been reached.
494.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""The maximum number of active Phase-1 negotiations "" ""reached	The maximum number of active phase 1 security associations has been reached.
495.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""The maximum number of active Quick-Mode negotiations "" ""reached. Quick-Mode not done.	Maximum number of active Quick-Mode negotiations reached before Quick-Mode was done.
496.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Cannot use binary formatting for syslog "" ""auditing.	Binary formatting for syslog audit is not permitted.
497.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Cannot create audit file context. Is '%s' a "" ""valid file name?	Audit file contect cannot be audited. Suspected reason is invalid filename.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
498.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Could not decode Certificate. """"The certificate may be corrupted or it was """"given in unrecognized format "" ""(file format may be wrong)	Certificate could be corrupted or in unrecognized (wrong) format. Check certificate attributes or use a different certificate.
499.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Could not decode Certificate. """"The certificate may be corrupted or it was ""given in unrecognized format "" ""(file format may be wrong)	Certificate could be corrupted or in unrecognized (wrong) format. Check certificate attributes or use a different certificate.
500.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Could not get subject name from a CA certificate. "" ""This certificate is not usable as an IPsec ""authenticator, and is not inserted into loal list of "" ""trusted CAs	Certificate cannot be used as an IPSec authenticator, as a subject name could not be extracted.
501.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Could not set CA certificate to non-CRL issuer. """"This may cause authentication errors if valid CRLs """"are not available	Could not set CA certificate to non-CRL issuer. This may cause authentication errors if valid CRLs are not available.
502.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Could not set the trusted set for a CA certificate	Trusted credentials could not be set for certificate. Review the attributes of the certificate or (if necessary) use a different certificate.
503.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Could not decode certificate. """"The certificate may be corrupted or it was ""given in unrecognized format """"(file format may be wrong)	Certificate could be corrupted or in unrecognized (wrong) format.
504.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Could not lock certificate in cache	Could not lock certificate in cache.
505.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Could not insert certificate into local database	Certificate could not be inserted into local database. Review the attributes of the certificate or (if necessary) use a different certificate.
506.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Could not decode CRL. The certificate may be """"corrupted or it was given in unrecognized format """"(file format may be wrong)	Certificate could be corrupted or in unrecognized (wrong) format.
507.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""NAT-T initial contact notification with IP """"identity %@	NAT-T initial contact notification.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
508.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""It is recommended to use non-IP identities with """"NAT-T to avoid ID collision	Use non-IP identities with NAT-T to avoid ID collision.
509.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"%s Phase-1 notification `%s' (%d) (size %d bytes) """"from %s%@ for protocol %s spi[0...%d[=%s"", encrypted ? ""Encrypted"" : ""Plain-text"",	Phase 1 notifications may have been encrypted in plain text. Verify to ensure data protection.
510.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""The maximum number of active Quick-Mode negotiations """"reached. Incoming Quick-Mode negotiation rejected	Maximum number of active Quick-Mode negotiations reached. Incoming Quick-Mode negotiation rejected.
511.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""%s Phase-2 notification `%s' (%d) (size %d bytes) "" ""from %s%@ for protocol %s spi[0...%d]=%s """"causes IKE SA deletion and QM abort	Problems in phase II negotiations result in IKA security association deletion and QM abort.
512.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""%s Phase-2 notification `%s' (%d) (size %d bytes) """"from %s%@ for protocol %s spi[0...%d]=%s	Phase 2 negotiation of protocol attributes taking palce.
513.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Suspicious outbound IPSec rule without any selectors: """"the rule might not work at all	Properties of outbound IPSec rule appear to be suspicious. The rule may nmot work.
514.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Type of the local ID %@ is not KEY-ID for "" ""the mamros-pskeyext negotiation. "" ""The negotiation might fail.	Properties of the key extension may not be supported. The negotiation and handshake of key credentials may fail.
515.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Tunnel end-point %@ is a link-local address, but "" ""tunnel local-ip is undefined. This is a """"configuration error!	Configuration error encountered. Tunnel local-ip is undefined.
516.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""% PFS group proposed for IPComp	*Perfect Forward Secrecy* (PFS) group has been proposed for IP Comp.
517.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Trigger for non-IP packet of protocol %d. "" ""Dropping request for policy	Request for policy dropped.
518.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""The rule is not in the active configuration. "" ""Dropping request for policy	A requested rule is not in active configuration, and can therefore not be supported.Request for policy is being dropped

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
519.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""The maximum number of active Quick-Mode negotiations "" ""reached. Dropping request for policy"")	The maximum number of active Quick-Mode negotiations has been reached. Request for policy is being dropped.
520.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Malformed packet for trigger. Dropping request for policy	A bad packet trigger was encountered, request for policy is being dropped.
521.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Malformed packet for trigger. Dropping request for policy	A bad packet trigger was encountered, request for policy is being dropped.
522.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Certificate contains bad IP address: length=%d	Certificate contains an invalid IP address. Validate the IP address and either correct certificate request or use a different certificate.
523.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Certificate contains bad IP address: length=%d	Certificate contains an invalid IP address. Validate the IP address and either correct certificate request or use a different certificate.
524.	AUTH-4-WARNING: WIOS_SECURITYMGR	4	"""Could not decode Certificate. "" ""The certificate may be corrupted or it was ""given in unrecognized format "" ""(file format may be wrong)	Certificate could not be properly decoded. It may be corrupt. Validate certificate credentials before trying again.
526.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""IKE SA [%s] negotiation completed:	IKE security association negotiation has been completed.
527.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" %s using %s (%s%s - %s)	This error message displays the stauts of IKE negotiaion that is carried out either in *main mode* or *aggressive mode*.
528.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""Diffie-Hellman group %u (%u bits)	IKE security association's DH group.
529.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""Lifetime: %u seconds"",	IKE security association in Lifetime (in seconds).
530.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: %s (%d)	Informational logs on the status of IKE security association negotiation.
531.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""IKE SA destroyed:	An IKE security association has been destroyed.
532.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: Could not select policy rule	Policy rule could not be properly selected during authentication attempt.
533.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Reason:	Reason for not selecting a policy rule.

Number	*Mnemonic*	*Severity*	*Syslog Message*	*Meaning / Cause*
534.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""Message: Could not select SA from IKE SA "" ""proposal	Security association could not be selected from IKE security association proposal.
535.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""IPSec SA negotiations: %u done, %u successful, %u failed	IPSec security associations completed. Percentages supplied for number of successful attempts out of total.
536.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""NGM [responder] between %@ and %@ rejected	
537.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: No attributes sent to client	Problem encountered during authentication attempt. No attributes sent to client.
538.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Reason: "" ""Could not register remote access client	Problem encountered during authentication attempt. Could not register remote access client.
539.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" IP address %@ assigned for client	An IP address has been assigned to the client.
540.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: No attributes sent to client	No attributes sent to client during authentication attempt.
541.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Reason: Could not encode attributes	Specific attributed could not encoded during authentication attempt.
542.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Reason: Could not encode attributes	Specific attributed could not encoded during authentication attempt.
543.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""XAUTH [Responder] exchange done	Authentication responder exchange completed.
544.	AUTH-6-INFO: WIOS_SECURITYMGR	6	" Authentication done	Authentication attempt completed for user.
545.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Authentication failed	Authentication attempt failed for user.
546.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: Could not store configuration "" ""parameters	Configuration parameters could not be stored during authentication attempt.
547.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Reason: Out of memory	Memory allocation problem encountered during authentication attempt.
548.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Configuration data received:	Configuration data received during authentication attempt.
549.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""QM notification `%s' (%d) (size %d bytes) "" ""from %s%@ for protocol %s spi[0...%d]=%s	Qucik Mode completion message.
550.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Result: %s	Quick mode result.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
551.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Error: %s	Quick mode completion error message.
552.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""IPSec SA [%s%s] negotiation completed:	IPSec security association negotiation has been completed.
553.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" PFS using Diffie-Hellman group %u (%u bits)"",	PDF using DH group for the above IP Sec security association.
554.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Local Proxy ID %@	Local proxy ID for IP Sec security association.
555.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Remote Proxy ID %@	Remote proxy ID for IP Sec security association.
556.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Inbound SPI: | Outbound SPI: | Algorithm:	Displays this message when the inbound/outbound SPI for the above IP Sec security association happens.
557.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" AH [%08x] | [%08x] | %s	Authentication algorithm for the above IP Sec security association.
558.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" ESP [%08x] | [%08x] | %s%s - %s	ESP algorithm for the above IP Sec.
559.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" IPComp [%04x] | [%04x] | %s	IP Comp algorithm for the above IPSec security association.
560.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""IPSec SA [Manual] completed:	IPSec security association completed.
561.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Local peer %@	Problem communicating with local peer during authentication attempt.
562.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Remote peer %@	Problem communicating with remote peer during authentication attempt.
563.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""Message: Could not verify remote peer's identity	Remote peer's identity could not be properly identified during authentication attempt.
	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" User-name: %.*s	User name could not be validated properly during authentication attempt.
564.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: PPP failure	PPP failure during authentication attempt.
565.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: Tunnel request rejected	Tunnel request rejected during authentication attempt.
566.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Reason: Out of resources	Ran out of resources during authentication request.
567.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: Tunnel request aborted	Tunnel request aborted during authentication request.
568.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: Could not start PPP"")	PPP session could not be properly started.

Number	***Mnemonic***	***Severity***	***Syslog Message***	***Meaning / Cause***
569.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: Could not start PPP	PPP session could not be properly started.
570.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: No LAC IP address negotiated	LAC IP address not properly negotiated during authentication attempt.
571.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: Could not create L2TP rule	Layer 2 rules could not be properly generated during authentication attempt.
572.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Message: Could not add ARP entry	ARP entry could not be added during authentication attempt.
573.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" PPP Authentication method:	PPP authentication method for SA.
574.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Virtual IP: %@	Virtual IP data insuffucient during authentication attempt.
575.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""Message: No IKE SA negotiations done	No IKE negotiation during authentication attempt.
576.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""Reason: The authentication credentials were not """"specified,	Authentication credentials not properly specified during handshake.
577.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" or private key was not available	Private key was not availabale during authentication attempt.
578.	AUTH-6-INFO: WIOS_SECURITYMGR	6	""" Attributes sent to client	Authentication attributes have been sent to the client.
579.	AUTH-6-INFO: WIOS_SECURITYMGR	6	"""XAUTH [Initiator] exchange done	Authentication initiator exchange completed.
580.	AUTH-6-INFO: WIOS_SECURITYMGR	6	No IPSec rules configured	Failed responder policy rule selection due to no IPSec rules being configured.
581.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Peer IP address mismatch	Failed responder policy rule selection due to a peer IP address mismatch.
582.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Local IP address mismatch	Failed responder policy rule selection due to a local IP address mismatch.
583.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Local IP address mismatch	Failed responder policy rule selection due to a local IP address mismatch.
584.	AUTH-6-INFO: WIOS_SECURITYMGR	6	CA not trusted	Failed responder policy rule selection due to a non-trusted CA.
585.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Access group mismatch	Failed responder policy rule selection due to access group mismatch.
586.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Quick-Mode local ID mismatch	Failed responder policy rule selection due to local ID mismatch.
587.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Quick-Mode remote ID mismatch	Failed responder policy rule selection due to remote ID mismatch.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
588.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Local IKE peer %s%@ ID %@	Local device which initiates IKE tunnel.
589.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Remote IKE peer %s%@ ID %@	Remote device where IKE tunnel terminates
590.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Initiator Cookie %@	Iniaitior cookie for IKE security association.
591.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Responder Cookie %@	Responder cookie for IKE security association.
592.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Invalid proposal	Security association selection failure. Failed responder security association selection due to invlaid proposal.
593.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Invalid protocol	Security association selection failure. Failed responder security association selection due to invalid protocol.
594.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Protocol given more than once	Security association selection failure. Failed responder security association selection due to protocol provided more than once.
595.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Invalid transform	Security association selection failure. Failed responder security association selection due to invlaid transform
596.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Invalid attribute	Security association selection failure. Failed responder security association selection due to invalid attribute.
597.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Mandatory attribute missing	Security association selection failure. Failed responder security association selection due to missing attribute.
598.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Protocol mismatch	Security association selection failure. Failed responder security association selection due to protocol mismatch.
599.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Protocol mismatch with NAT-T	Security association selection failure. Failed responder security association selection due to protocol mismatch.
600.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Attribute mismatch	Security association selection failure. Failed responder security association selection due to attribute mismatch.
601.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Algorithm did not match policy	Security association selection failure. Failed responder security association selection due to algorithm not matching policy.
602.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Unsupported algorithm	Security association selection failure. Failed responder security association selection due to unsupported algorithm.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
603.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Authentication method mismatch	Security association selection failure. Failed responder security association selection due to auth failure.
604.	NO INFORMATION: NEED MNEMONIC FROM ENGINEERING		Unsupported authentication method	Security association selection failure. Failed responder security association selection due to unsupported auth method.
605.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Diffie-Hellman group mismatch	Security association selection failure. Failed responder security association selection due to DH group mismatch.
606.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Unsupported Diffie-Hellman group	Security association selection failure. Failed responder security association selection due to supported DH group.
607.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Address %@	Print configuration information
608.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Valid %u seconds	Informational logs for config mode attributes.
609.	AUTH-6-INFO: WIOS_SECURITYMGR	6	DNS %@	Informational logs for config mode attributes
610.	AUTH-6-INFO: WIOS_SECURITYMGR	6	WINS %@	Informational logs for config mode attributes
611.	AUTH-6-INFO: WIOS_SECURITYMGR	6	DHCP %@	Informational logs for config mode attributes
612.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Subnet %@	Informational logs for config mode attributes
613.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Encapsulation mode mismatch	Security association selection failure. Failed responder security association selection.
614.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Key length mismatch	Security association selection failure. Failed responder security association selection.
615.	AUTH-6-INFO: WIOS_SECURITYMGR	6	ESP-none/none proposed	Security association selection failure. Failed responder security association selection.
616.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Out of memory	Security association selection failure. Failed responder security association selection.
617.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Rule not active (invalid interface selector?)	Security association selection failure. Failed responder security association selection.
618.	AUTH-6-INFO: WIOS_SECURITYMGR	6	Sequence number size mismatch	Security association selection failure. Failed responder security association selection.

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
619.	NO INFORMATION: NEED MNEMONIC FROM ENGINEERING	6	"L2TP [%s, incoming-call] negotiation %s:	
620.	NO INFORMATION: NEED MNEMONIC FROM ENGINEERING	6	"Local L2TP peer %s:%s	Device where L2TP tunnel is initiated.
621.	NO INFORMATION: NEED MNEMONIC FROM ENGINEERING	6	Remote L2TP peer %s:%s	Device where L2TP tunnel is terminated.
622.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""%s: Could not start application gateway: "" ""registration failed: %s.	Registration failed for any of these services cifs, dns, ftp, netbios, sip, socksify or wins.
623.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""%s: Could not create application gateway: """"out of memory.	Insufficient memory resulted in the failed creation of application gateway.
624.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""%s: Could not create application gateway: """"initialization failed.	Initialization failure resulted in the failed creation of application gateway session.
625.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""%s: Received broken configuration.	Broken configuration received. Ensure configuration is credible before sending over application gateway.
626.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"%s: Can't start application gateway: " "registration failed; reason %s.""	Application gateway could not be started due to failed registration.
627.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""%s: Can't create application gateway: no space.	Insufficeint space to create application gateway.
628.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""%s: Can't create application gateway: """"no space for connection container.	Application gateway session could not be created. Ensure enough space exists interoperation over gateway.
629.	NO INFORMATION: NEED MNEMONIC FROM ENGINEERING	3	"""%s: Could not decode configuration data """"for service %u	Configuration data could not be decoded. Validate the configuration and try again.
630.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""%s: Can't start application gateway: """"registration failed; reason %s.	Application gateway could noty be started.
631.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""Rejecting IPSec SA delete notification """"from %s%@ since it was or protocol %s	IPSec security association rejected.

Number	***Mnemonic***	***Severity***	***Syslog Message***	***Meaning / Cause***
632.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"Rejecting IPSec SA delete notification " "from %s%@ since the SPI size %d does not match ""the expected value 4"	Delete notification received for rejected security association. SPI size does not match expected value.
633.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""Invalid protocol %s received for selected SA """"when installing Phase-2 Quick-Mode SA	Non-compliant protocol received for when installing security association.
634.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""Could not export IKE SA	IKE information within a security association could not be exported.
635.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""Could not save IKE SA `%s	IKE information within a security association could not be saved.
636.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""Could not remove IKE SA `%s	IKE information within a security association could not be removed.
637.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""Could not open persistent SA directory `%s	Persistent security association directory could not be opened.
638.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	" ""Could not read IKE SA `%s'"	An IKE security association could not be read.
639.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""Could not import IKE SA `%s	An IKE security association could not be imported.
640.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""Could not allocate IKE SA `%s	An IKE security association could not be allocated.
641.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""Rule commit failed	User access rule could not be established. The rule could not be permitted.
642.	DAEMON-3-ERR: WIOS_SECURITYMGR	3	"""Removing of unused rules failed	Switch attemoted and failed to remove user access permissions that were not being used. Review user access policies and amend as needed.
643.	DAEMON-5-NOTICE: WIOS_SECURITYMGR	5	"""%s: Shutting down.	Switch shutting down.
644.	DAEMON-5-NOTICE: WIOS_SECURITYMGR	5	%s: Application gateway started.	Application gateway has started. Informational message only.
645.	DAEMON-5-NOTICE: WIOS_SECURITYMGR	5	Cannot set session identifier for background process. " "Operation (setsid) failed with error: %.100s	Session identifier ID could not be established..

Number	Mnemonic	Severity	Syslog Message	Meaning / Cause
647.	DAEMON-5-NOTICE: WIOS_SECURITYMGR	5	Remote L2TP implementation (Vendor Name `%.*s') is ""not standard-compliant: " "the Mandatory bit (%s) of the AVP `%s' (%d) " "does not match RFC 2661	Layer 2 error generated as a result of unknown vendor name not matching RFC 2661 standard.
648.	DAEMON-6-INFO: WIOS_SECURITYMGR	6	"""%s: Can't copy NetBIOS scope ID; reason: ""	NOT SUPPORTED.
649.	DAEMON-6-INFO: WIOS_SECURITYMGR	6	%s: Can't serve connection; reason: no space.	Existing space does not permit updates to configuration. Space must be freed to make requested update.
650.	DAEMON-6-INFO: WIOS_SECURITYMGR	6	Lifetime: %u kilobytes, %u seconds	Lifetime of the IP Sec SA in both kilobytes and seconds.
651.	DAEMON-6-INFO: WIOS_SECURITYMGR	6	Lifetime: %u seconds	Lifetime of the IP Sec SA in seconds
652.	DAEMON-6-INFO: WIOS_SECURITYMGR	6	Lifetime: %u kilobytes	Lifrtime of the IP Sec SA in kilobytes
654.	DAEMON-6-INFO: WIOS_SECURITYMGR	6	"The PPP implementation of the remote L2TP client "" ""(Vendor Name `%.*s') does not handle PPP "" ""authentication method negotiation correctly: "" disabling EAP	PPP support mis-match between switch and client. Ensure the selected switch authentication method is supported on client and try again.
655.	DAEMON-2-CRIT: WIOS_SECURITYMGR	2	"service %s: insufficient memory available, "" ""unable to apply new configuration	Existing memory space does not permit updates to configuration. Memory space must be freed to make requested update.
656.	DAEMON-2-CRIT: WIOS_SECURITYMGR	2	"service %s: internal error, could not "" ""unmarshal configuration!	This error message occurs when security manager encounters a failure while unmarshalling a configuration for application gateways.
657.	DAEMON-2-CRIT: WIOS_SECURITYMGR	2	"registering HTTP APPGW failed: %s	HTTP gateway failure. Re-establish HTTP connection.
658.	DAEMON-4-WARNING: WIOS_SECURITYMGR	4	"""No IKE logging enabled. The system has not "" ""been compiled with `--enable-debug'.	Login not enabled for IKE negotiation.

2.2 MU Dissasociation Codes

The following table provides reason codes for 802.11 mobile unit disassociation.

ID	***802.11 or Motorola/WPA Reason Code***	***Description***
0	REASON_CODE_80211_SUCCESS	Reserved internally to indicate success.
1	REASON_CODE_80211_UNSPECIFIED_ERROR	Unspecified reason.
3	DISASSOCIATION_REASON_CODE_STATION_LEAVING_ESS	Deauthenticated because sending station has left or is leaving IBSS or ESS.
4	DISASSOCIATION_REASON_CODE_INACTIVITY	Disassociated due to inactivity.
5	DISASSOCIATION_REASON_CODE_STATION_LIMIT_EXCEEDED	Disassociated because AP is unable to handle all currently associated stations.
6	DISASSOCIATION_REASON_CODE_CLASS_2_PKT_FROM_NON_AUTH	Class 2 frame received from non-authenticated station.
7	DISASSOCIATION_REASON_CODE_CLASS_3_PKT_FROM_NON_ASSOC	Class 3 frame received from non-associated station.
8	DISASSOCIATION_REASON_CODE_STATION_LEAVING_BSS	Disassociated because sending station has left or is leaving BSS.
9	DISASSOCIATION_REASON_CODE_STATION_NOT_AUTHENTICATED	Station requesting re-association is not authenticated with responding station.
13	DISASSOCIATION_REASON_CODE_INVALID_INFORMATION_ELEMENT	Invalid information element.
14	DISASSOCIATION_REASON_CODE_MIC_FAILURE	MIC failure.
15	DISASSOCIATION_REASON_CODE_4WAY_HANDSHAKE_TIMEOUT	4-way handshake timeout.
16	DISASSOCIATION_REASON_CODE_GROUP_KEY_UPDATE_TIMEOUT	Group key update timeout.
17	DISASSOCIATION_REASON_CODE_4WAY_IE_DIFFERENCE	Information element in 4-way handshake different from associated request/probe response/beacon.
18	DISASSOCIATION_REASON_CODE_MULTICAST_CIPHER_INVALID	Multicast cipher is not valid.
19	DISASSOCIATION_REASON_CODE_UNICAST_CIPHER_INVALID	Unicast cipher is not valid.
20	DISASSOCIATION_REASON_CODE_AKMP_NOT_VALID	AKMP is not valid.
21	DISASSOCIATION_REASON_CODE_UNSUPPORTED_RSNE_VERSION	Unsupported RSN IE version.
22	DISASSOCIATION_REASON_CODE_INVALID_RSNE_CAPABILITIES	Invalid RSN IE capabilities.
23	DISASSOCIATION_REASON_CODE_8021X_AUTHENTICATION_FAILED	IEEE 802.1X authentication failed.

ID	***802.11 or Motorola/WPA Reason Code***	***Description***
44	DISASSOCIATION_REASON_CODE_PSP_TX_PKT_BUFFER_EXCEEDED	Motorola defined (non-802.11 standard) code. The switch has exceeded its time limit in attempting to deliver buffered PSP frames to the mobile unit without receiving a single 802.11 PS poll or NULL data frame. The switch begins the timer when it sets the mobile unit's bit in the TIM section of the 802.11 beacon frame for the BSS. The time limit is at least 15 seconds. The mobile unit is probably gone (or may be faulty).
77	DISASSOCIATION_REASON_CODE_TRANSMIT_RETRIES_EXCEEDED	Motorola defined (non 802.11 standard) codes. The switch has exceeded its retry limit in attempting to deliver a 802.1x EAP message to the mobile unit without receiving a single 802.11 ACK. The retry limit varies according to traffic type but is at least 64 times. The mobile unit is either gone or has incorrect 802.1x EAP authentication settings.

3

Security Issues

This chapter describes the known troubleshooting techniques for the following data protection activities:

- *Switch Password Recovery*
- *RADIUS Authentication*
- *Rogue AP detection*
- *Firewall configuration*

3.1 Switch Password Recovery

If the switch Web UI password is lost, you cannot get passed the Web UI login screen for any viable switch configuration activity. Consequently, a password recovery login must be used that will default your switch back to its factory default configuration.

To access the switch using a password recovery username and password:

CAUTION Using this recovery procedure erases the switch's current configuration and data files from the switch /flash dir. Only the switch's license keys are retained. You should be able to log in using the default username and password (admin/superuser) and restore the switch's previous configuration (only if it has been exported to a secure location before the password recovery procedure was invoked).

1. Connect a terminal (or PC running terminal emulation software) to the serial port on the front of the switch.

   The switch login screen displays. Use the following CLI command for normal login process:

   ```
   WS5100 login: cli
   ```

2. Enter a password recovery username of **restore** and password recovery password of **restoreDefaultPassword**.

   ```
   User Access Verification


   Username: restore

   Password: restoreDefaultPasword


   WARNING: This will wipe out the configuration (except license key) and user
   data under "flash:/" and reboot the device

   Do you want to continue? (y/n):
   ```

3. Press **Y** to delete the current configuration and reset factory defaults.

   The switch will login into the Web UI with its reverted default configuration. If you had exported the switch's previous configuration to an external location, it now can be imported back to the switch.

3.2 RADIUS Troubleshooting

The issues defined in this section have the following troubleshooting workarounds:

Radius Server does not start upon enable

Ensure the following have been attempted:

- Import valid server and CA certificates
- Add a Radius client in AAA context
- Ensure that key password in AAA/EAP context is set to the key used to generate imported certificates
- DO NOT forget to SAVE!

Radius Server does not reply to my requests

Ensure the following have been attempted:

- Add a Radius client in AAA configuration with NIC1/NIC2 IP address
- Save the current configuration
- Ensure that Security Policy is configured for this RADIUS server.

Radius Server is rejecting the user

Ensure the following have been attempted:

1. Verify a SAVE was done after adding this user.
2. Is the user present in a group?
    - If yes, check if the WLAN being accessed is allowed on the group
    - Check if time of access restrictions permit the user.

Time of Restriction configured does not work

Ensure the following have been attempted:

- Ensure date on the system matches your time

Authentication fails at exchange of certificates

Ensure the following have been attempted:

- Verify that valid certificates were imported.
- If the Supplicant has "Validate Server Certificate" option set, then make sure that the right certificates are installed on the MU.

When using another WS5100 (switch 2) as RADIUS server, access is rejected

Ensure the following have been attempted:

- Make sure that the user, group and access policies are properly defined on switch 2.
- Add a AAA client on switch 2 with NIC2 IP address of switch 1
- Save the current configuration

Authentication using LDAP fails

Ensure the following have been attempted:

- Is LDAP server reachable?
- Have all LDAP attributes been configured properly?
- Dbtype must be set to LDAP in AAA configuration
- Save the current configuration

VPN Authentication using onboard RADIUS server fails

Ensure the following have been attempted:

- Ensure that the VPN user is present in AAA users
- This VPN user MUST NOT added to any group.
- Save the current configuration

Accounting does not work with external RADIUS Accounting server

Ensure that accounting is enabled.

- Ensure the RADIUS Accounting server is reachable
- Verify the port number being configured on accounting configuration matches that of external the RADIUS Accounting Server
- Verify the shared secret being configured on accounting configuration matches that of the external RADIUS Accounting Server

3.2.1 Troubleshooting RADIUS Accounting Issues

Use the following guidelines when configuring RADIUS Accounting:

1. The RADIUS Accounting records are supported only for clients performing 802.1X EAP based authentication.
2. The user name present in the accounting records, could be that of the name in the outer tunnel in authentication methods like: TTLS, PEAP.
3. If the switch crashes for whatever reason, and there were active EAP clients, then there would be no corresponding STOP accounting record.
4. If using the on-board RADIUS Accounting server, one can delete the accounting files, using the 'acct purge' command in the AAA context.
5. If using the on-board RADIUS Accounting server, the files would be logged under the: /usr/var/log/radius/radacct/<clientIP>

   In this case, the <clientIP> is the SRC IP used to send across the accounting packets in the CellController.

   Typically, this depends on the IP of the Radius Accounting Server, and the CC binds to the interface, over which the UDP packet would go out (based on the routing tables).

3.3 Rogue AP Detection Troubleshooting

Motorola recommends adhereing to the following guidelines when configuring Rogue AP detection:

1. Basic configuration required for running Rogue AP detection:
   - Enable any one of the detection mechanism.
   - Enable rogueap detection global flag.
2. After enabling rogueap and a detection mechanism, look in the roguelist context for detected APs. If no entries are found, do the following:
   - Check the global rogueap flag by doing a show in rogueap context. It should display Rogue AP status as "enable" and should also the status of the configured detection scheme.
   - Check for the AP flag in rulelist context. If it is set to "enable", then all the detected APs will be added in approved list context.
   - Check for Rulelist entries in the rulelist context. Verify it does not have an entry with MAC as "FF:FF:FF:FF:FF:FF" and ESSID as "*"
3. If you have enabled AP Scan, ensure that at least a single radio is active. AP scan does not send a scan request to an inactive or unavailable radio.

4. Just enabling detectorscan will not send any detectorscan request to any adopted AP. User should also configure at least a single radio as a detectorAP. This can be done using the set detectorap command in rogueap context.

3.4 Troubleshooting Firewall Configuration Issues

Motorola recommends adhereing to the following guidelines when dealing with problems related to WS5100 Firewall configuration:

A Wired Host (Host-1) or Wireless Host (Host-2) on the untrusted side is not able to connect to the Wired Host (Host-3) on the trusted side

1. Check that IP Ping from Host1/Host2 to the Interface on the Trusted Side of the WS5100 switch works.

   CLI (from any context) - ping <host/ip_address>

2. If it works then there is no problem in connectivity.
3. Check whether Host-1/Host-2 and Host-3 are on the same IP subnet.

   If not, add proper NAT entries for configured LANs under FireWall context.

4. After last step, check again, that IP Ping from Host1 to the Interface on the Trusted Side of the WS5100 switch works.

   If it works then problem is solved.

A wired Host (Host-1) on the trusted side is not able to connect to a Wireless Host (Host-2) or Wired Host (Host-3) on the untrusted side

1. Check that IP Ping from Host1 to the Interface on the Untrusted Side of the switch works.
2. If it works then there is no problem in connectivity.
3. Now check whether Host-1 and Host-2/Host-3 are on the same IP subnet.

   If not, add proper NAT entries for configured LANs under FireWall context.

4. Once step 3 is completed, check again, that IP Ping from Host1 to the Interface on the Untrusted Side of the switch works.

   If it works then problem is solved.

Disabling of telnet, ftp and web traffic from hosts on the untrusted side does not work.

1. Check the configuration for the desired LAN under FW context (which is under configure context).

   CLI - configure fw <LAN_Name>

2. Check whether ftp, telnet and web are in the denied list. In this case, web is https traffic and not http.
3. Ensure that "network policy" and "Ethernet port" set to the LAN is correct.

How to block the request from host on untrusted to host on trusted side based on packet classification.

1. Add a new Classification Element with required Matching Criteria
2. Add a new Classification Group and assigned the newly created Classification Element. Set the action required.
3. Add a new Policy Object. This should match the direction of the packet flow i.e. Inbound or Outbound.
4. Add the newly created PO to the active Network Policy.

5. Associate WLAN and Network Policy to the active Access Port Policy.

   Any request matching the configured criteria should take the action configured in the Classification Element.

4

Network Events and Kern Messages

This chapter includes two network event tables to provide detailed information and understanding of potential network events. These tables are:

- Table 4.1, Network Event Message/Parameter Description Lookup
- Table 4.2, Network Event Course of Action Lookup on page 4-6

Table 4.1 Network Event Message/Parameter Description Lookup

ID	Event	Message	Parameters
0	License number change	Changed license level from <XX> license number access ports to <YY> number access ports.	XX = previous license number (an integer) YY = new license number (an integer)
1	Clock change	The Wireless Switch clock was changed <XX>/ <YY> seconds.	XX = + or - YY = offset in seconds (an integer)
2	Packet discard [wrong NIC]	Discarded Packet: Wrong NIC <XX> <XX> vs <YY> from access port ZZ.	XX = Ethernet port that received the packet = 1 or 2 YY = Ethernet Port that the access port was adopted from = 1 or 2 ZZ = MAC (xx:xx:xx:xx:xx:xx) address of the Access Port
3	Packet discard [wrong VLAN]	Discarded Packet: Wrong VLAN <XX> <XX> vs <YY> from access port <ZZ>.	XX = VLAN that received the packet (an integer). YY = VLAN the access port was adopted from (an integer). ZZ = MAC (xx:xx:xx:xx:xx:xx) address of the access port.
4	AP adopt failure [general]	Adoption <XX> failed. The MAC address has been used by an existing access port.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the radio or access port.
5	AP adopt failure [policy disallow]	Access port policy prevented port with MAC <XX> from being adopted.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the access port.
6	AP adopt failure [acl disallow]	This event and message is currently not configured. It will be configured in the next service release.	Not applicable.

Table 4.1 Network Event Message/Parameter Description Lookup (Continued)

ID	Event	Message	Parameters
7	AP adopt failure [limit exceeded]	Access port <XX> was not adopted because maximum limit has been reached.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the access port.
8	AP adopt failure [license disallow]	License denied access port <XX> adoption. Maximum access ports allowed with current license = <YY>.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the access port. YY = License Level (integer).
9	AP adopt failure [no image]	Access port with MAC <XX> can not be adopted because no valid firmware image file can be found.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the access port.
10	AP status [offline]	Access port <XX> with MAC address <YY> is unavailable.	XX = Name (string) of the access port. <YY> = MAC (xx:xx:xx:xx:xx:xx) address of the access port.
		Taking access port <XX> with MAC address <YY> offline.	XX = Name (string) of the access port. <YY> = MAC (xx:xx:xx:xx:xx:xx) address of the access port.
11	AP status [alert]	Access port <XX> with MAC address <YY> is in Alert status due to country not set.	XX = Access port name (string). YY = Access port MAC (xx:xx:xx:xx:xx:xx) address.
		Access port <XX> with MAC address <YY> is in Alert status.	XX = Access port name (string) <YY> = Access port MAC (xx:xx:xx:xx:xx:xx) address.
12	AP status [adopted]	Adopted an access port <XX>.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the access port.
		Radio <XX> with Mac <YY> is adopted.	XX = Access port name (string). YY = MAC (xx:xx:xx:xx:xx:xx) address of the access port.
13	AP status [reset]	Radio <XX> with MAC <YY> was reset.	XX = Name (string) of the radio. YY = MAC (xx:xx:xx:xx:xx:xx) address of the radio.
		Reset the access port <XX>.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the access port.
14	AP config failed [wrong ESS]	Radio <XX> <YY> no ESS - configuration FAIL.	XX = Name (string) of the radio. YY = MAC (xx:xx:xx:xx:xx:xx) address of the radio.
15	AP max MU count reached	MUs for this RF port are over margin: <XX>.	XX (integer) = Number of MUs associated to this access port.
16	AP detected	Detected a new access port <XX>.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the access port.

Table 4.1 Network Event Message/Parameter Description Lookup (Continued)

ID	Event	Message	Parameters
17	Device msg dropped [info] debug	Dropping DeviceInfo message from <XX> whose parent is <YY>.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the access port. YY = MAC (xx:xx:xx:xx:xx:xx) address of the switch to which the access port is adopted.
18	Device msg dropped [loadme]	Dropping Loadme message from <XX> whose parent is <YY>.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the access port. YY = MAC (xx:xx:xx:xx:xx:xx) address of the switch to which the access port is adopted.
19	Ether port connected	Ethernet Port <XX> is connected.	XX = Ethernet port number 1 or 2.
20	Ether port disconnected	Ethernet port <XX> disconnected.	XX = Ethernet port number 1 or 2.
21	MU assoc failed [ACL violation]	ACL denied MU (XX) association.	XX = MU MAC (xx:xx:xx:xx:xx:xx) address.
22	MU assoc failed	Access port refused MU <XX> association. Error <YY>.	XX = Wireless client MAC (xx:xx:xx:xx:xx:xx) address. <YY> = Reason code number (integer).
23	MU status [associated]	Mobile Unit <XX> was associated to access port <YY>.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the MU. YY = Name (string) of the access port.
24	MU status [roamed]	Mobile Unit <XX> with MAC <YY> roamed from access port <ZZ> to (Name of the access port to which the Mobile Unit roamed).	XX = Name (string) of the MU. YY = MAC (xx:xx:xx:xx:xx:xx) address of the MU. ZZ = Name (string) of the access port the MU roamed from.
25	MU status [disassociated]	Mobile Unit <XX> with MAC address <YY> was disassociated. Reason code <ZZ>.	XX = Name (string) of the mobile unit. YY = MAC (xx:xx:xx:xx:xx:xx) address of the mobile unit. ZZ = Reason (integer) code number.
26	MU EAP auth failed	MU <XX> failed to authenticate with RADIUS server.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the mobile unit.
27	MU EAP auth success	Mobile unit <XX> successfully authenticated with EAP type <YY>, authentication valid for <ZZ> minutes.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the mobile unit. YY = EAP (integer) type ZZ = number (integer) of minutes.

Table 4.1 Network Event Message/Parameter Description Lookup (Continued)

ID	Event	Message	Parameters
28	MU Kerberos auth failed	MUs failed to authenticate with the KDC at <MU_MAC_address> (Error code <code>).	[MAC address of MU] [MAC xx:xx:xx:xx:xx of Radius server] [port on Radius server] [radius error code]
29	MU Kerberos auth success	MUs failed authentication via Kerberos. [Error code <code>] Mobile Unit with MAC <MU_MAC_address> successfully authenticated via Kerberos - authentication expires in <#> minutes.	[MAC address of MU] [Radius error code] [MAC address of MU] [# minutes authentication is valid for].
30	MU TKIP [decrypt failure]	MU <MU_MAC_address> has high decrypt failure rate.	[MAC address of MU (in 6 octets)]
31	MU TKIP [replay failure]	MU <MU_MAC_address> has high replay failure rate.	[MAC address of MU (in 6 octets)]
32	MU TKIP [MIC error]	MIC validation failed for MU %s on ESS <ID>.	[MAC address of MU] [ESSID with which MU is associated]
33	WLAN auth success	"WLAN <WLAN_name> (ESS <ESS ID>) successfully authenticated with KDC at <KDC MAC_address><KDC port>.	[WLAN name] [ESSID] [MAC xx:xx:xx:xx:xx of KDC server] [port on KDC server]
34	WLAN auth failed	WLAN <WLAN name> (ESS <ID>) could not be authenticated with KDC at <KDC MAC address> <port> after <#> attempts - still trying...	[WLAN name] [ESSID] [MAC xx:xx:xx:xx:xx of KDC server] [port on KDC server] [number of attempts]
35	WLAN max MU count reached	ACL denied MU (%s) association.	[MAC address of MU]
36	Mgt user auth failed [radius]	GUI/CLI User userid Authentication Failure: User userid rejected by Radius server RADIUS server hostname/IP address.	userid = string RADIUS server hostname/IP address = string
37	Mgt user auth rejected	NOT USED	
38	Mgt user auth success [radius]	User userid authenticated locally. User userid successfully authenticated by Radius server RADIUS server hostname/IP address.	userid = string RADIUS server hostname/IP address = string
39	Radius server timeout	Radius server %s is unreachable.	[radius server name]

Table 4.1 Network Event Message/Parameter Description Lookup (Continued)

ID	Event	Message	Parameters
40	KDC user [added]	Adding KDC User:<username> time:<timestamp>.	[user name][timestamp]
41	KDC user [changed]	Changed KDC User:<username> time:<timestamp>.	[user name] [timestamp]
42	KDC user [deleted]	Removed KDC User:<username> time:<timestamp>.	[user name] [timestamp]
43	KDC DB replaced	Replaced KDC DB:Modified Locally. Replaced KDC DB:Modified by SEMM.	
44	KDC propagation failure	KDC Propgation fails on host (<host name>). KDC Propgation fails!	[host-name]
45	WPA counter-measures [active]	Began WPA counter-measures for WLAN <WLAN name> (ESS <ESS ID>).	[name of WLAN] [ESSID]
46	Primary lost heartbeat	Primary lost heartbeat(s).	
47	Standby active	Fail-over took place, Standby machine is now in Active state.	
48	Primary internal failure [reset]	Primary internal failure, Resetting.	
49	Standby internal failure [reset]	Standby internal failure, Resetting.	
50	Standby auto-revert	Standby Auto Reverting	
51	Primary auto-revert	Primary Auto Reverting	
52	Auto channel select error	ACS failed to find a valid channel, err <channel #>. ACS failed to find a valid channel. Reusing existing channel <channel #>. ACS success. Setting radio MAC address of the access port to channel.	[Channel#] MAC address of the access port = xx:xx:xx:xx:xx:xx Channel = integer
53	Emergency Policy [active]	Emergency Switch Policy Emergency Switch Policy is activated.	Emergency Switch Policy = string
54	Emergency Policy [deactivated]	Emergency Switch Policy Emergency Switch Policy is deactivated. "Emergency Switch Policy %s is deactivated."	Emergency Switch Policy = string [previous de-activated policy name]
55	Low flash space on switch-alert	Found disk="<percent disk spaced used>" USED disk-space - VACUUMing Database in 5 secs to free-up space	percent disk spaced used = decimal (xx.xx)

Table 4.1 Network Event Message/Parameter Description Lookup (Continued)

ID	Event	Message	Parameters
56	Miscellaneous debug events KerberosWlanAuthOperation::OnStart() RADIO_TYPE_FH != pRadio->GetType() NULL == pCountry->GetFHInfo() CWlan::KerberosClientAuth()	Internal Failure, out of ethernet buffers. The license key on a WS-Lite cannot be upgraded. WSLiteValidation:FAILURE:%s is invalid %d-port license for WS-Lite. EtherPortManager::EnsureNoCollisions(FOUND PROBLEM: %s). Etherport policies \"%s\" and \"%s\" are on the same subnet(%d). " [policy name] [policy name] Began authentication process for WLAN %s (ESS %s) with KDC %lu.%lu.%lu.%lu..." [WLAN name][ESSID string][KDC MAC]. "Mobile Unit \"%s\" successfully authenticated with %s" (+) ", authentication valid for %d minutes" (or) ", no re-authentication period set" [MAC of MU][EAP type][# of minutes] "No valid channel for 802.11%s radio. Adoption is denied." [type of radio (“A” or “B” or “FH”)] "No valid country info for 802.11%s radio. Adoption is denied." [type of radio (“A” or “B” or “FH”)] "Began authentication process for WLAN %s (ESS %s) with KDC '%s'... [name of WLAN][ESSID][KDC Server Hostname] "End WPA counter-measures for WLAN %s (ESS %s)" [name of WLAN][ESSID]	[XML error string(if any)] [number of radios (APs) in-use] [string containing explanation of collision in policy]

Table 4.2 provides a list of the same events shown in Table 4.1 , but with additional information and suggestive actions to resolve or understand an event.

Table 4.2 Network Event Course of Action Lookup

ID	Event	Description	Possible Course of Action
0	License number change	A license key was entered to change the number of access ports the switch can adopt.	This event can only occur by entering a license key.
1	Clock change	The date/time setting was changed on the switch	This event can only occur by changing the date/time.

Table 4.2 Network Event Course of Action Lookup (Continued)

ID	Event	Description	Possible Course of Action
2	Packet discard [wrong NIC]	When an access port is adopted, the switch remembers which Ethernet port the access port was adopted from. The switch will only accept data from that access port through the Ethernet port which it was adopted from. If the switch receives data from that access port on another Ethernet port, it will be discarded.	The access port may have been removed and reconnected to another part of the network that is connected to the other Ethernet port of the switch. Or, the access port's logical connection to the network has changed, causing it to be connected to the other Ethernet port of the switch. If this is intentional, the access port must first be removed from the switch and readopted through the new Ethernet port. If this is unintentional, reconnect the access port to the Ethernet port that it was adopted through.
3	Packet discard [wrong VLAN]	If an Ethernet port is configured for 802.1q trunking when an access port is adopted, the switch remembers which VLAN the access port was adopted from. The switch will only accept data from that access port through the VLAN which it was adopted from. If the switch receives data from that access port on another VLAN, it will be discarded.	The access port may have been removed and reconnected to another part of the network that is connected to the other Ethernet port of the switch. Or, the access port's logical connection to the network has changed, causing it to be connected to the other Ethernet port of the switch. If intentional, the access port must be removed from the switch and readopted through the new Ethernet port. If unintentional, reconnect the access port to the Ethernet port that it was adopted through.
4	AP adopt failure [general]	An access port's request to be adopted has been rejected because there is already another access port with the same MAC address currently active on the switch.	Confirm that there are actually two access ports with the same MAC address and contact Motorola Customer Support.
5	AP adopt failure [policy disallow]	An access port's request to be adopted has been rejected because the Switch is configured to deny adoption of access ports.	If the switch is to adopt the access port, either manually adopt it by including it in the "include list" of the adoption list or by configuring the Switch to "allow adoption" of access ports.
6	AP adopt failure [acl disallow]	The access port's request for adoption was rejected because the access port is in the *exclude list* of the adoption list.	If the switch is to adopt the access port, remove the access port from the "exclude list" of the adoption list.
7	AP adopt failure [limit exceeded]	Switch ran out of licenses or, albeit unlikely, the switch ran out of memory to create a radio-object.	There are more AP devices than there are licenses. Either remove the extra APs or purchase more licenses.

Table 4.2 Network Event Course of Action Lookup (Continued)

ID	Event	Description	Possible Course of Action
8	AP adopt failure [license disallow]	Switch ran out of licenses and could not adopt this AP.	There are more AP devices than there are licenses. Either remove the extra APs or purchase more licenses.
9	AP adopt failure [no image]	It seems that the switch does not have a valid AP image firmware file to download onto the AP.	From your Web UI, go to "System Settings > Firmware Management > Available Images…" and make sure there is an image for AP's model.
10	AP status [offline]	• This access port has been unavailable for a long time. • The status of this access port has changed to Unavailable.	Unavailable means that the switch has not been able to communicate with this access port for more than 10 seconds.
11	AP status [alert]	The status of the access port has changed to Alert.	• The country code for the Switch has to be set to something other than "None" (default) before an access port can be adopted. Until then, all access ports will be at "Alert" status. • The access port needs attention. Look for other Event Notification messages for details.
12	AP status [adopted]	The status of the access port has changed to Alert.	
13	AP status [reset]	Lost heartbeat.	
14	AP config failed [wrong ESS]	There are no in-use WLANs configured on this switch.	This access port will have an Alert status until it is configured with an Access Port Policy with a valid WLAN. If the WLAN is using Kerberos security, check that the WLAN is authenticated by the KDC.
15	AP max MU count reached	An access port has reached the maximum limit of 128 MUs which can associate to a single access port.	When the limit has been reached, the access port will not allow any additional MUs to associate.
16	AP detected	A new access port was detected.	
17	Device msg dropped [info]	A DEVICEINFO message is received from an AP (with the AP configuration), but the AP claims to have another switch as parent.	There may be multiple Primary and Active WS5100s on the same physical subnet. Either remove the extra switches or configure them for "Hot Standby" operation.
18	Device msg dropped [loadme]	A LOADME request is received from an AP (a WSAP-50xx), but the AP claims to have another switch as parent.	There may be multiple Primary and Active WS5100s on the same physical subnet. Either remove the extra switches or configure them for "Hot Standby" operation.

Table 4.2 Network Event Course of Action Lookup (Continued)

ID	Event	Description	Possible Course of Action
19	Ether port connected	A previously disconnected Ethernet port was re-connected.	If you see excessive amounts of this message you may have a cable or switch hardware problem.
20	Ether port disconnected	A previously connected Ethernet port was disconnected.	If you see excessive amounts of this message you may have a cable or switch hardware problem.
21	MU assoc failed [ACL violation]	This MU was rejected as it requested to associate to the WLAN with an Access Control List.	If this is not intentional check your Access Control List and make sure this MAC address is not rejected by policy.
22	MU assoc failed	This message cannot be due to REASON CODE 80211 STATION LIMIT EXCEEDED	Either incorrect security policy is applied or policy is configured incorrectly.
23	MU status [associated]	A MU associated to an access port.	None
24	MU status [roamed]	A MU roamed from to another access port.	Refer to reason codes table for an explanation.
25	MU status [disassociated]	A MU disassociated from an access port.	
26	MU EAP auth failed	A MU EAP authentication request failed.	Invalid username or password. Login again.
27	MU EAP auth success	A MU EAP authentication request succeeded.	
28	MU Kerberos auth failed	A MU Kerberos authentication request failed	
29	MU Kerberos auth success	A MU Kerberos authentication request succeeded.	
30	MU TKIP [decrypt failure]	The switch has encountered high levels of sequential decrypt failures with this MU.	This could be suspicious. If this is a known MU, it should be re-associated.
31	MU TKIP [replay failure]	The switch has encountered high levels of sequential decrypt failures with this MU.	
32	MU TKIP [MIC error]	This MU has failed a MIC encryption. This could potentially be an attempt to break security. If this is detected twice within 60 seconds, the switch will implement WPA countermeasures.	
33	WLAN auth success		
34	WLAN auth failed		

Table 4.2 Network Event Course of Action Lookup (Continued)

ID	Event	Description	Possible Course of Action
35	WLAN max MU count reached	This is an incorrect message. It is not really the ACL that denied association; it is really that the 802.11 limit has been exceeded.	
36	Mgt user auth failed [radius]	Management user not authenticated on the switch's local user database. Management user not authenticated on the remote RADIUS server database.	
37	Mgt user auth rejected	[UNUSED]	
38	Mgt user auth success [radius]	Management user successfully authenticates on the switch's local user database. Management user successfully authenticates on the remote RADIUS user database.	
39	Radius server timeout		Check your Radius server configuration on the switch.
40	KDC user [added]		
41	KDC user [changed]		
42	KDC user [deleted]		
43	KDC DB replaced		
44	KDC propagation failure	Host name is unknown.	
45	WPA counter-measures [active]	The switch will be "down" for a short length of time and then come back up to re-associate MUs.	
46	Primary lost heartbeat	The Primary switch in Standby mode did not receive monitoring heartbeats from the Standby switch.	If this event occurs but failover does not occur, then there is possible congestion on the network causing the heartbeats to be lost. Also, look for other events prior to the lost heartbeats that might indicate a problem, such as Ethernet port disconnected.
47	Standby active	The Standby switch has changed its state from Monitoring to Active.	A failover has occurred.
48	Primary internal failure [reset]		
49	Standby internal failure [reset]		

Table 4.2 Network Event Course of Action Lookup (Continued)

ID	Event	Description	Possible Course of Action
50	Standby auto-revert	The Standby switch is auto-reverted from Active to Monitoring. This event is reported by the Standby switch.	
51	Primary auto-revert	The Primary wireless switch is auto-reverted from Halted to Connected. This event is reported by the Primary wireless switch.	
52	Auto channel select error	Misleading text. It is the Channel#, not an error, that is in the string.	
53	Emergency Policy [active]	The Emergency Switch Policy is activated.	
54	Emergency Policy [deactivated]	The Emergency Switch Policy is deactivated.	
55	Low flash space on switch-alert	The used disk space exceeds 80%. This will be reported approximately every five hours.	Remove any unused policies, ACLs, user names, files, etc.
56	Miscellaneous debug events	Case ASEVENT_EVENT_PSD_REBOOT_NOBDOS KerberosWlanAuthOperation::OnStart() RADIO_TYPE_FH != pRadio->GetType() NULL == pCountry->GetFHInfo() CWlan::KerberosClientAuth()	Switch will need to re-boot and should do so within 120 seconds.

4.1 KERN Messages

Table 4.3 Kern Messages

Module	***Message***	***Description***
ccdev.c	PKT_INFO(""Prtl ""MACSTR"" rem @ %d"", MAC2STR(prtls[idx].cfg.addr), idx);'	Radio (portal) is removed from packet driver due to inactivity."
ccdev.c	PKT_INFO(""mu ""MACSTR"" w/ aid %d added to prtl ""MACSTR,);	A mobile unit with the given mac address has been added to radio <mac>.
ccdev.c	PKT_ERR(""ccdev : %s bad cmd->index %d"", __FUNCTION__, cmd->index);	Another program module tried to set a command on a non-existing ethernet port. This is to guard against programming errors. This should not happen in the field.
ccdev.c	PKT_ERR(""ccdev : %s no vlan cfg for idx %d"", __FUNCTION__, cmd->index);	Another program module tried to set a command on non-existing vlan devices. This is to guard against programming errors. This should not happen in the field.
ccdev.c	PKT_ERR(""ccdev : %s bad cmd id : %d"", __FUNCTION__, cmd->id);	Another program module tried to set a command for a vlan device, but the command is not known to the packet driver. This is to guard against programming errors. This should not happen in the field.
ccdev.c	PKT_ERR(""%s : bad ioctl_num %d"", __FUNCTION__, ioctl_num);	Another program module sent a general command that is not known to the packet driver This is to guard against programming errors. This should not happen in the field.
ccdev.c	PKT_ERR(""ccdev : CC server not up"");	The packet driver received a packet that is destined to cell controller server, and has detected that cell controller server is not up and running. This can happen if cell controller server has crashed.
ccdev.c	PKT_WARN(""Queue to user space full, packet throttled=%d"", rd_list_dropped);	The queue from packet driver to the cell controller server is full and additional packets destined for the cell controller are being receieve. The queue limit is 1000 packets for the WS5100 switch. This can happen if cell controller process has died and the packet driver did not detected this. As a result, the system is flooded with packets that require processing by the cell controller.
crypt.c	PKT_WARN(""crypt: enabling countermeasures on wlan %d"", wlan_idx);	A condition has triggered counter measures on the specified WLAN.
crypt.c	PKT_INFO(""crypt: disabling countermeasures on wlan %d"", wlan_idx);	A condition has been satified to disable counter measures on the specified WLAN.
crypt.c	PKT_INFO(""WEP Decrypt Failed ""MACSTR""\n"", MAC2STR(mu->cfg.addr));	Decryption failed for the specified mobile MAC address.

Table 4.3 Kern Messages (Continued)

Module	***Message***	***Description***
crypt.c	PKT_INFO(""%s decrypt failure: ""MACSTR"" iv32 = 0x%x iv16 = 0x%x\n"",);	Detailed failure on WEB decrypt failure.
crypt.c	PKT_INFO(""TKIP Replay check fail ""MACSTR"" got: %x %x expecting:%x %x\n"",);	TKIP: Replay check failed for the specified MAC address.
crypt.c	PKT_WARN(""tkip: station replay counters out of sync for ""MACSTR"". deauthing\n"", MAC2STR(mu->cfg.addr));	TKIP: Station replay counters are out of sync.
crypt.c	PKT_INFO(""ccmp decrypt failed ""MACSTR"" (%u bytes)\n"", MAC2STR(hdr->src), elen);	CCMP: decrypt failed.
crypt.c	PKT_INFO(""aes replay check failed ""MACSTR"" got: %x%x expected:%x%x\n"",);	AES: Replay check failed for the specified mac address.
crypt.c	PKT_WARN(""aes: station replay counters out of sync for ""MACSTR"". deauthing\n"", MAC2STR(mu->cfg.addr));	AES: Station replay counters are out of sync.
crypt.c	PKT_INFO(""qos admission control verification failed\n"");	A mobile station has sent more packets then allowed.
crypt.c	PKT_INFO(""rx encrypted frame from ""MACSTR"" when policy is no encryption.\n"",);	Received an encrypted frame on an unencrypted WLAN.
crypt.c	PKT_INFO(""dropping clear frame from ""MACSTR"". policy requires encryption.\n"",);	Received a unencrypted frame on an encrypted WLAN.
crypt.c	PKT_INFO(""EWEP bit in WEP hdr = 1, Expected 0 ""MACSTR""\n"",);	Extended WEP mask is set on a WEP encrypted WLAN.
crypt.c	PKT_INFO(""EWEP bit in WEP hdr = 0, Expected 1 ""MACSTR""\n"",);	Extended WEP mask is not set on Keyguard, TKIP or CCMP encrypted WLANs.
crypt.c	PKT_INFO(""AES-CCMP encrypt failed ""MACSTR""\n"", MAC2STR(hdr->src));	AES-CCMP: Encrypt failed.
crypt.c	PKT_INFO(""qos admission control verification failed\n"");	The intended receiving station has exceed its bandwidth use allocated by QOS.
crypt.c	PKT_ERR(""unknown %s encryption type %d"",);	The WLAN has an encryption type that is unknown to the packet driver. This is to guard against programming errors from other modules.
crypt.c	PKT_WARN(""mic check failure ""MACSTR"". got: ""MACSTR"" calc: ""MACSTR""\n"",);	MIC check failed.
dhcp.c	PKT_WARN(""%s : wrong IP version %u"", __FUNCTION__, skb->nh.iph->version);	Received a non IP-v4 packet
dhcp.c	PKT_ERR(""%s : bad cookie %x"", __FUNCTION__, ntohl(*((U32*)posn)));	Recevied a DHCP packet with an unknown cookie.

Table 4.3 Kern Messages (Continued)

Module	***Message***	***Description***
driver.c	PKT_ERR(""device %s needs to be re-installed"", devname[idx]);	A platform specific physical device has not been installed. For example eth1 and eth2 on Monarch have not been installed.
driver.c	PKT_INFO(""Driver - deliver to Linux vlan %d\n"", PS_Get_SKB_Vlan_Tag(skb));	Mobility error
driver.c	PKT_INFO(""rx from Linux"");	The packet driver received a packet from Linux. This is for debugging purposes only.
driver.c	PKT_ERR(""Error initializing virtual device"");	The packet driver has failed to initialize its own working virtual device.
flowctl.c	PKT_WARN(""flowctl: bad tx_res, retries=%d, rate=%d"", retries, rate);	An unexpected or impossible transmit result from a WISP packet.
flowctl.c	PKT_INFO(""flowctl: no stats update for dropped seq %x"",);	The tranmittted packet corresponding to this WISP sequance can not be updated.
flowctl.c	PKT_WARN(""fc:mu removed before fc ack on prtl ""MACSTR,);	An ACK for WISP packet has arrived, but the corresponding receiving station has been deleted from system.
flowctl.c	PKT_WARN(""fc:dropped assoc resp pkt to ""MACSTR,);	An association response or reassociation response packet has not transmitted successfully.
flowctl.c	PKT_INFO(""fc:dropped %d consec pkts to ""MACSTR,);	More than 5 packets in a row to the same station have failed.
flowctl.c	PKT_INFO(""fc:mu [""MACSTR""] in psp, dropped packet %d"",);	Received a transmit result for a Mobile Unit in PSP mode.
flowctl.c	PKT_ERR(MACSTR"" prtl window wrap curr=%u, new=%u"",);	Detected a wrap around in the WISP flow control window. Note: It is expected to see the wrap around from 65535 to zero. This is not an error condition it is caused by a programming error.
flowctl.c	PKT_INFO(MACSTR"" fc window wrap curr=%u, new=%u"",);	Detected a wrap around in the WISP flow control window. Note: It is expected to see the wrap around from 65535 to zero. This is not an error condition it is caused by a programming error.
flowctl.c	PKT_ERR(MACSTR"" wisp seq %u != fc seq=%u setting to %u"",);	WISP sequence with a radio has become out of sync. Resync to the new number.
flowctl.c	PKT_INFO(""fc allocs:q full"");	Number of pending packets in the switch has exceed the limit. The limit is 10,000 for WS5100 switch.
flowctl.c	PKT_INFO(""fc:allocs back down to %u"", curr_fc_allocs);	The number of pending packets has fallen back below the limit.

Table 4.3 Kern Messages (Continued)

Module	***Message***	***Description***
flowctl.c	PKT_ERR(""fc alloc:no memory for fc allocs"");	Request from the operating system for a new packet has failed.
flowctl.c	PKT_INFO(""fc freed ack q pkt seq %d, tx time %u, now %u"",);	A packet pending ACK has been there for too long (beyond 7 seconds) and forcefully removed it..
flowctl.c	PKT_INFO(""fc q extract:seq %d not found in %d entries"", seq, count);	Received a flow control message that does not have a corresponding packet pending in the ACK queue.
flowctl.c	PKT_INFO(MACSTR"" fc send failure"", MAC2STR(prtl_ptr->cfg.addr));	A packet has failed to send due to flow control limitation.
flowctl.c	PKT_ERR(MACSTR"" fc ack timeout:curr %u,acktime=%u"",);	A radio (Access Port) with the specified MAC address has not sent flow control packets for 5 seconds.
flowctl.c	PKT_ERR(MACSTR"" fc no prtl traffic in last %d secs"",);	Heart beats for the radio with specified mac address have not occured within last 5 seconds.
flowctl.c	PKT_ERR(""flowctl : bad tx_ctl %x"", tx_ctl);	The flow control field in WISP packets is not properly formulated.
flowctl.c	PKT_ERR(MACSTR"" std queue: can't tx, fc blocked"",);	Sending to a radio has been temporarily blocked. The current packet will be dropped.
flowctl.c	PKT_INFO(""flowctl Q-Full wlan %d, ac %d (%d/%d)"", wlan_idx, ac_idx,);	The Queue for given wlan and ac is full now.
flowctl.c	PKT_INFO(MACSTR"" std queue:alloc failed, curr %d"",);	Failed to get a new queue element.
flowctl.c	PKT_INFO(MACSTR"" std q:failed"", MAC2STR(prtl_ptr->cfg.addr));	Failed to send a packet due to the above reasons.
flowctl.c	PKT_ERR(MACSTR"" can't tx, fc mgmt blocked"", MAC2STR(prtl_ptr->cfg.addr));	A WISP management packet has been dropped due to that radio being blocked.
flowctl.c	PKT_INFO(MACSTR"" fc mgmt q:alloc failed"", MAC2STR(prtl_ptr->cfg.addr));	An attempt to send a managment packet has failed due to a failure to aquire a queue element.
flowctl.c	PKT_INFO(MACSTR"" fc mgmt q:failed"", MAC2STR(prtl_ptr->cfg.addr));	Attempt to send a managment packet has failed.
flowctl.c	PKT_WARN(""mismatch(roam?): dest=""MACSTR"", its seq=%d, prtl=""MACSTR"", its seq=%d"",);	The wireless header and the WISP header have mismatched radio mac addresses.
flowctl.c	PKT_INFO(""fc can't send"");	A WISP data packet has failed to send.
flowctl.c	PKT_WARN(""std: pkt sent %d not in ack queue"", q_elem->seq);	An attempt has been made to remove a failed packet from the ACK queue, but the packet is not there.

Table 4.3 Kern Messages (Continued)

Module	***Message***	***Description***
flowctl.c	PKT_INFO(""mgmt fc can't send"");	A WISP management packet has failed to send.
flowctl.c	PKT_WARN(""mgmt fc: send failed seq %d not in ack queue"", q_elem->seq);	An attempt has been made to remove a failed packet from the ACK queue, but the packet is not there.
flowctl.c	PKT_INFO(MACSTR"" fc free queues"", MAC2STR(prtl_ptr->cfg.addr));	Remove the FC queue for the radio with the specified MAC address when deleting the radio.
flowctl.c	PKT_ERR(""Unknown fc_type = %d on ""MACSTR,);	Detected an unkown WISP flow control type.
flowctl.c	PKT_ERR(""flowctl: num_pkts_on_portal = 0, ac_idx = %d can't dec"",);	An attempt has been made to decrement the packet counter when it is already at zero.
flowctl.c	PKT_ERR(""%d not found in ack queue for ""MACSTR, seq,);	The given WISP sequence is not in the ACK queue.
flowctl.c	PKT_INFO(MACSTR"" fc window wrap around curr = %d, new = %d"",);	Flow control window wrap around occured.
flowctl.c	PKT_WARN(MACSTR"" ack q is null for seq:0x%08x"",);	Tried to update WISP with ACK sequence, but the ACK queue is empty.
flowctl.c	PKT_ERR(""Invalid Wisp cmd id: 0x%04X"", cmd);	Invalid WISP commad ID.
flowctl.c	PKT_ERR(""psp update tim: alloc skb failed"");	Tried to send a WISP update TIM, but failed to get a new buffer.
gag.c	PKT_WARN(""vlan out of range"");	Another program module try to change multicast-packet-limit for a VLAN out of range [1,4094]."
hotspot.c	PKT_ERR(""Hotspot: Netdevice does not exists for interface Vlan %d"", vlan_id);	The intended receive device does not exist.
hotspot.c	PKT_ERR(""Hotspot: Device is null"");	The intended receive device does not exist.
mob_ctl.c	PKT_INFO(""wrong arp prot %x"", arp_hdr->prot);	Mobility error.
mob_data.c	PKT_ERR(""%s : skb2tun copy failed."", __FUNCTION__);	Mobility error.
mob_data.c	PKT_ERR(""%s : skb2tun copy failed."", __FUNCTION__);	Mobility error.
pal.c	PKT_WARN(""%s : wrong IP version %u"", __FUNCTION__, skb->nh.iph->version);	When trying to update the MU's IP information, found out that the version is not IP-v4.
pal.c	PKT_INFO(""%s : wrong arp prot %x"", __FUNCTION__, arp_hdr->prot);	Recieved ARP with a non-IP protocol.

Table 4.3 Kern Messages (Continued)

Module	***Message***	***Description***
pal.c	PKT_INFO(""%s : de-authing unknown MU ""MACSTR"" on BSS ""MACSTR,);	Received a packet from an MU that is not associated. Sending de-auth forces it out.
pal.c	PKT_WARN(""%s : de-auth ""MACSTR"" tx'ing on wrong radio:""MACSTR"" should be on""MACSTR,);	Tried to send a packet for a MU through a radio that it is not currently associated. Sending de-auth to forces it out.
pal.c	PKT_ERR(""%s: invalid data sub type %X"", __FUNCTION__, sub_type);	Detected an invalid 802.11 sub type in packet.
pal.c	PKT_WARN(""pshandle:de-authing ""MACSTR"". unknown src-addr in ctl frame"", MAC2STR(rhdr->src));	Received a control frame from an unknown station. Sending de-auth forces it out..
pal.c	PKT_ERR(""%s : 802.11 data pkt too small (%d bytes)"", __FUNCTION__, skb->len);	Received a runt 802.11 packet.
pal.c	PKT_ERR(""%s: unknown frame type %x"", __FUNCTION__, ctl & MASK_CTL_FRAME_TYPE);	Received unkown 802.11 frame type.
pal.c	PKT_INFO(""PAL_Rx_From_WLAN"");	Received a wireless packet. Should be removed.
pal.c	PKT_INFO(""proxy arp resp was sent"");	A proxy ARP response was sent.
pal.c	PKT_INFO(""PD_Tx_To_Linux"");	Sent a packet to the Linux kernel. Will be removed.
pal.c	PKT_INFO(""PD_Tx_To_Wire"");	Sent a packet to Ethernet wire.
pal.c	PKT_INFO(""PAL_Defrag_ESS_Data"");	Defragmenting 802.11 data packet.
pal.c	PKT_ERR(""%s : new_skb allocation failed"", __FUNCTION__);	Failed to get a buffer from the OS.
pal.c	PKT_ERR("" vlan id %d out of range"", vlan_tag);	Received a packet with an out of range VLAN id.
pal.c	PKT_ERR(""Multicast Flooding Detected, limiting the segments in broadcast domain to %d"", copy_limit);	Detected that the swich is making too many copies of a multicast packet that uses too much system bandwidth. The switch limits the overall MC bandwith per VLAN as if the multicast-packet-limit is 32 or less. The overall MC bandwith is 3200 packets, and the number of copies for a given multicast packet is 3200/ multi-cast-packet-limit, when multicast-packet-limit =32, the number of copies 3200/32 = 100 copies. If the multicast-packet-limit is 33 or above, the overall MC bandwith is 2500 packets, and the number of copies for a given multicast packet is 3200/limit. When multicast-packet-limit is 128, e.g., the number of copies is 2500/128 = 19 copies.
pal.c	PKT_INFO(""PAL_Unicast_To_WLAN"");	Sending a unicast packet to the WLAN.

Table 4.3 Kern Messages (Continued)

Module	***Message***	***Description***
pal.c	PKT_ERR(""%s : MU ""MACSTR"" has a null prtl"", __FUNCTION__, MAC2STR(mu_ptr->cfg.addr));	The intended station is not associated with any radio.
pal.c	PKT_INFO(""Non-IP pkt, no DSCP bits. Default DSCP to 0x08"");	The packet is not an IP packet. Default DSCP value.
pal.c	PKT_INFO(""PAL_Unicast_From_LAN"");	Received 802.3 ethernet packet.
pal.c	PKT_INFO(""Failed to get new skb, skip"");	Failed to get a packet buffer from OS.
pal.c	PKT_INFO(""from switch. Sending to wire"");	Switching a packet from the switch to the Ethernet wire.
pal.c	PKT_INFO(""dropping pkt src:""MACSTR"" dst:""MACSTR,);	Failed to determine the destination for a packet.
pal.c	PKT_INFO(""proxy arp resp was sent"");	Proxy ARP response was sent.
pal.c	PKT_INFO(""dropping wisp packets to another switch ""MACSTR,);	Drop an unicast WISP packet not destined for the switch.
pal.c	PKT_INFO(""dropping L2 wisp packets in wrong direction, cmd=0x%04x"", cmd);	Received L2 WISP packet with the wrong direction bit.
pal.c	PKT_WARN(""pal: Send_2_CC call failed for a deauth-req\n"");	Packet driver tried to send a de-auth packet to CC for it to process, but it failed.
pal.c	PKT_WARN(""pal: Send_2_CC call failed for mu-remove-req\n"");	Packet driver tried to send a mu-remove-req to CC, but it failed.
proxyarp.c	PKT_INFO(""wrong arp prot %x"", arp_hdr->prot);	ARP protocol type is not IP protocol.
proxyarp.c	PKT_INFO(""gratuitous arp from ip=%u.%u.%u.%u\n"", NIPQUAD(arp_req->src_ip));	Received a gratuitious ARP.
proxyarp.c	PKT_ERR(""%s: skb alloc failed"", __FUNCTION__);	Failed to get a packet buffer from the OS when trying to send a proxy ARP response.
proxyarp.c	PKT_INFO(""arp resp: smac=""MACSTR "", sip=%u.%u.%u.%u dmac=""MACSTR "", dip=%u.%u.%u.%u\n"",);	Sending a proxy ARP response now.
ps_capwap.c	PKT_INFO(""warning: rx data from unknown portal"");	Received a data packet from an unknown portal. This could happen if the radio starts to forward traffic before it is adopted by the switch.
ps_capwap.c	PKT_INFO(""Rx inactive mu stats for unknown/ inactive mu: "" MACSTR,);	Received a MU stats update for an inactive station.
ps_capwap.c	PKT_WARN(""Unreal dt(tx_pkt) @ rate %d: 0x%08lx - 0x%08lx = 0x%08lx\n"",);	The delta on transmitted packets from radio stats is unrealistically big.

Table 4.3 Kern Messages (Continued)

Module	***Message***	***Description***
ps_capwap.c	PKT_WARN(""Unreal dt(retry) @ %d: 0x%08lx - 0x%08lx = 0x%08lx\n"",);	The delta on retry from radio stats is unrealistically big.
ps_caspwap.c	PKT_WARN(""Unreal delta tx-fail: 0x%08lx - 0x%08lx = 0x%08lx\n"",);	The delta on transmission failure from radio stats is unrealistically big.
ps_capwap.c	PKT_WARN(""capwap skb length underrun: received %d, expected %d\n"", skb->len, dlen);	The actual packet length is smaller than what the capwap header indicates.
ps_capwap.c	PKT_ERR(""%s : CC sending data pack to unknown MU"", __FUNCTION__);	CC server is sending a data packet to a station that the packet driver does not know about.
ps_capwap.c	PKT_INFO(""%s(): packet failed encryption"", __FUNCTION__);	Packet failed encryption.
ps_common.c	PKT_INFO(""no tail room to fix for runt packet"");	Tried to fix a runt Ethernet packet, but there is no room to do that.
ps_common.c	PKT_ERR(""pshandle:failed to allocate roam skbuf"");	Failed to get packet buffer from the OS.
ps_common.c	PKT_INFO(""pshandle:mu ""MACSTR"" roamed"", MAC2STR (addr));	Detected that the given MAC address has roamed.
psp.c	PKT_ERR(""psp update tim: alloc skb failed"");	Failed to get the packet buffer to update TIM.
psp.c	PKT_INFO(""psp store: max len (%d) reached. Use of a lower DTIM value recommended"", max_qlen);	Max number of PSP packets reached.
psp.c	PKT_ERR(""psp store: out of memory"");	Failed to get memory from the OS.
psp.c	PKT_WARN(""psp_tx_unicast dropping skb to unreachable mu ""MACSTR,);	Dropped packets to an unreachable MU.
psp.c	PKT_WARN(""psp:dropped %d bytes unicast to ""MACSTR, skb->len,);	Dropped number of bytes to a given station.
psp.c	PKT_WARN(""psp:deauthing ""MACSTR"" due to max-tx-fails"", MAC2STR(mu_ptr->cfg.addr));	De-auth of a station due to excessive failures.
psp.c	PKT_INFO(""prtl ""MACSTR"" bss %d psp queue full with %d pkts"",);	Radio with a given MAC address, its PSP queue is full.
psp.c	PKT_ERR(""dtim poll: recvd bad bss index"");	Received a DTIM poll with bad BSS index.
psp.c	PKT_WARN(""pspoll: psp bit not set"");	Received a PSP poll from the MU, but the PSP bit is not set.
psp.c	PKT_INFO(""psp:mu ""MACSTR"" authenticating"", MAC2STR(mu_ptr->cfg.addr));	A station with the given MAC address is in the process of authentication.
psp.c	PKT_INFO(""psp:free mu queue"");	Free PSP queue for MU.

Table 4.3 Kern Messages (Continued)

Module	***Message***	***Description***
psp.c	PKT_INFO(""psp:free portal queues"");	Free radio PSP queue.
ps_wisp.c	PKT_WARN(""radio ""MACSTR"" lost first frag of seq %04x till %04x"",);	Missed WISP packet for given sequence range.
ps_wisp.c	PKT_WARN(""radio ""MACSTR"" lost seq %u to %u"",);	Missed WISP packet for given sequence range.
ps_wisp.c	PKT_WARN(""warning: unable to queue skb"");	Failed to switch a packet from a radio to the CC.
ps_wisp.c	PKT_INFO(""warning: rx wisp data from unknown portal"");	Received a WISP data packet from an unknown portal.
ps_wisp.c	PKT_INFO(""ps_rx_from_cc: no portal to queue to"");	Received a packet from the CC, but there is no radio to send to.
ps_wisp.c	PKT_ERR(""%s : CC sending data pack to unknown MU"", __FUNCTION__);	Received a packet from the CC, but the intended MU is unknown.
ps_wisp.c	PKT_INFO(""ps_rx_from_cc: packet failed encryption"");	Failed to encrypt a packet from the CC.
ratescale.c	PKT_ERR(""%s : curr = %d allowed = %x"", __FUNCTION__,);	Tried to get to a lower or higher rate beyond the allowed rate for a MU.
ratescale.c	PKT_ERR(""ratescale : no highest rate = %x"", allowed_rates);	It is already in the highest rate setting.
ratescale.c	PKT_INFO(MACSTR"" rate[%s to %s], [%d/%d], pct:%d"",);	Ratescale is a switch from old rate to new rate.
reassembly.c	PKT_ERR(""fragment too big to copy:%d bytes"", skb->len);	Reassembed packets does not fit into a single packet buffer.
reassembly.c	PKT_ERR(""reassy:unknown cmd type"");	Unknown WISP fragment type or command.
reassembly.c	PKT_ERR(""error:fragment too big to copy:%d bytes"", copy_len);	Reassembed packets does not fit into the single packet buffer.
reassembly.c	PKT_ERR(""PS_Frag_Send unable to alloc skb"");	Failed to get packet buffer from the OS.
reassembly.c	PKT_ERR(""PS_BCMC_Frag_Send unable to alloc skb"");	Failed to get packet buffer to send BC packets.
rssi.c	PKT_ERR(""rssi : bad vals ap = %d, rd = %d, rssi = %d"", ap, rd, rssi);	Trying to convert RSSI to DBM for an unknown combination of ap, radio and rssi.
tunnel.c	PKT_INFO(""%s: Unknown tunnel=tunnel%d"", __FUNCTION__,);	Unknown
vdev.c	PKT_ERR(""null device passed to get stats routine"");	Attempted to get stats for an unknown VLAN.

5

LED Information

5.1 LED Information

The WS5100 has two vertically-stacked LEDs on its front panel. The LEDs display three colors (blue,amber, and red), and three lit states (solid, blinking, and off). The following tables decode the combinations of LED colors and states.

5.1.1 Start Up

Event	*Top LED*	*Bottom LED*
Power off	Off	Off
Power On Self Test (POST) running	All colors in rotation	All colors in rotation
POST succeeded	Blue solid	Blue solid

5.1.2 Primary

Event	*Top LED*	*Bottom LED*
Active (Continually Adopting Access Ports)	Blue blinking	Blue solid
No License to Adopt	Amber blinking	Amber blinking

5.1.3 Standby

Event	*Top LED*	*Bottom LED*
Active (Failed Over and Adopting Ports)	Blue blinking	Blue blinking
Active (Not Failed Over)	Blue blinking	Amber solid

5.1.4 Error Codes

Event	***Top LED***	***Bottom LED***
POST failed (critical error)	Red blinking	Red blinking
Software initialization failed	Amber solid	Off
Country code not configured. **Note:** During first time setup, the LEDs will remain in this state until the country code is configured.	Amber solid	Amber blinking
No access ports have been adopted	Blue blinking	Amber blinking

6

Updating the System Image

The WS510 ships with a factory installed firmware image with full feature functionality. However, Motorola periodically releases switch firmware that includes enhancements or resolutions to known issues. Verify your current switch firmware version with the latest version available from the Motorola Web site before determining if your system requires an upgrade.

Additionally, legacy users running either the 1.4.x or 2.x version switch firmware may want to upgrade to the new 3.x baseline to take complete advantage of the new diverse feature set available to them. This chapter describes the method to upgrade from either the 1.4.x or 2.x baseline to the new 3.x baseline.

CAUTION: Motorola recommends caution when upgrading your WS5100 switch image to the 3.x baseline as portions of your configuration will be lost and unrecoverable. Ensure that you have exported your switch configuration to a secure location before upgrading your switch. The upgrade.log file will contain a list of the issues found in the conversion of the configuration file to the new format.

CAUTION: If using a 1.4.x or 2.x admin user password shorter than 8 characters (such as the default motorola password), the password will be converted to the 3.x baseline admin password of "password" upon a successful update to the 3.x baseline. Ensure your existing 1.4.x or 2.x admin password is longer than 8 characters before updating, or leave as is and use "superuser" to login into an updated 3.x baseline.

CAUTION: After upgrading the switch baseline from 1.4.x or 2.x to the 3.x baseline, applet caching can produce unpredictable results and contents. After the upgrade, ensure your browser is restarted. Otherwise, the credibility of the upgrade can come into question.

6.1 Upgrading the Switch Image from 1.4.x or 2.x to Version 3.x

To upgrade a switch running either a 1.4.x or 2.x version to the latest 3.x version switch firmware:

1. Execute the PreUpgradeScript utility (or use the CLI) to ensure there is enough space on your system to perform the upgrade. The PreUpgradeScript utility should be in the same directory as the upgrade files.

2. Install the **Cfgupgrade1.0-setup** utility on a Windows desktop system by double clicking the Cfgupgrade 1.0-setup file.

   Follow the prompts displayed by the installer to install Cfgupgrade 1.0-setup.

   A WS5100 Configuration Upgrade icon gets created within the Program Files folder. The icon can be optionally created on your Windows desktop as well.

3. From the WS5100 running either 1.4.x or 2.x, create a configuration and save it on the switch.

   WS5100# save <file name> <.cfg>

   This is the configuration that will be upgraded to the new 3.x baseline.

NOTE Motorola recommends saving a copy of the switch configurartion to a secure location before the upgrade. If an error occurs with the upgrade a viable configuration will be needed to restore on the switch.

4. Copy the configuration file <.cfg> from the legacy WS5100 to the Windows system where the conversion utility resides.

   Use ftp or tftp to transfer the file.

5. Click on the **WS5100 configuration Upgrade** icon (from the Windows system).

6. Select the config file copied on to the windows system and run it.

   A folder having the same name as the config file is created. The folder contains the converted startup-config file (in the new upgraded format) along with other log files.

7. Copy the startup-config file back to the WS5100 running using either tftp or ftp.

8. Download or copy the image file <`WS5100-3.0.2.0-XX.v1`> or <`WS5100-3.0.2.0-XX.v2`> to the WS5100 running the legacy switch firmware.

NOTE If upgrading a 1.4.x version WS5100 to the new 3.x baseline, be sure you are using the <`WS5100-3.0.2.0-XX.v1`> image file. If upgrading a 2.x version WS5100 to the new 3.x baseline, be sure you are using the <`WS5100-3.0.2.0-XX.v2`> image file.

9. On WS5100 running the legacy switch firmware, type:

   WS5100#service

   WS5100#password "password"

   exec

   Upon reboot, the switch runs the 3.x image using startup-config as the running configuration.

10. Repeat the instructions above for additional switch upgrades, ensuring <`WS5100-3.0.2.0-XX.v1`> is used for 1.4.x version upgrades, and <`WS5100-3.0.2.0-XX.v2`> is used for 2.x version upgrades.

6.2 Downgrading the Switch Image from Version 3.x to 1.4.x or 2.x

If for some reason you want to downgrade your WS5100 back down to a 1.4.x or 2.x version firmware image, use one of the two following image files:

- WS5100-1.4.3.0-012R.img
- WS5100-2.1.0.0-029R.img

7

Troubleshooting SNMP Issues

The following SNMP-releated issues could require troubleshooting as issues are experienced with the WS5100 switch.

MIB Browser not able to contact the agent.

General error messages on the MIB Browser: Timeout, No Response.

The client IP where the MIB browser is present should be made known to the agent. Adding SNMP clients through CLI or Applet can do this. This can be verified by looking at /butterfly/snmp/snmpd.conf. The entries are generally present towards the end of this file.

Not able to SNMP WALK for a GET.

First check whether the MIB browser has IP connectivity to the SNMP agent on the WS5K. Use IP Ping from the PC which has the MIB Browser.

Then check if the community string is the same at the agent side and the manager (MIB Browser) side. Community name is case sensitive.

MIB not visible in the MIB browser.

The filename.mib file should be first compiled using a MIB compiler, which creates a smidb file. This file must be loaded in the mib browser.

If SETs still don't happen...

Check to see if environment variables are set. The following are the env variable to be set.

```
SNMPCONFPATH=/butterfly/snmp
MIBDIRS=/butterfly/snmp/mibs
MIBS=ALL
```

Restart the SNMP agent (the snmpd daemon)

Not getting snmptraps

Check whether snmp traps are enabled through CLI or Applet. Configure MIB browser to display notifications or traps. (This would generally be a check box in the MIB browser preferences).

Still Not Working

Double check Managers' IP Address, community string, port number, read/write permissions, and snmp version. Remember community string IS CASE SENSITIVE.

Appendix A Customer Support

Motorola's Enterprise Mobility Support Center

If you have a problem with your equipment, contact Enterprise Mobility support for your region. Contact information is available at: http://www.symbol.com/contactsupport.

When contacting Enterprise Mobility support, please provide the following information:

- Serial number of the unit
- Model number or product name
- Software type and version number

Motorola responds to calls by email, telephone or fax within the time limits set forth in support agreements. If you purchased your Enterprise Mobility business product from a Motorola business partner, contact that business partner for support.

Customer Support Web Site

Motorola's Support Central Web site, located at www.symbol.com/support provides information and online assistance including developer tools, software downloads, product manuals and online repair requests.

Downloads

http://symbol.com/downloads

Manuals

http://symbol.com/manuals

General Information

Obtain additional information by contacting Motorola at:

1-800-722-6234, inside North America

+1-516-738-5200, in/outside North America

http://www.motorola.com/

MOTOROLA INC.
1303 E. ALGONQUIN ROAD
SCHAUMBURG, IL 60196
http://www.motorola.com

72E-100959-01 Revision A
June 2007