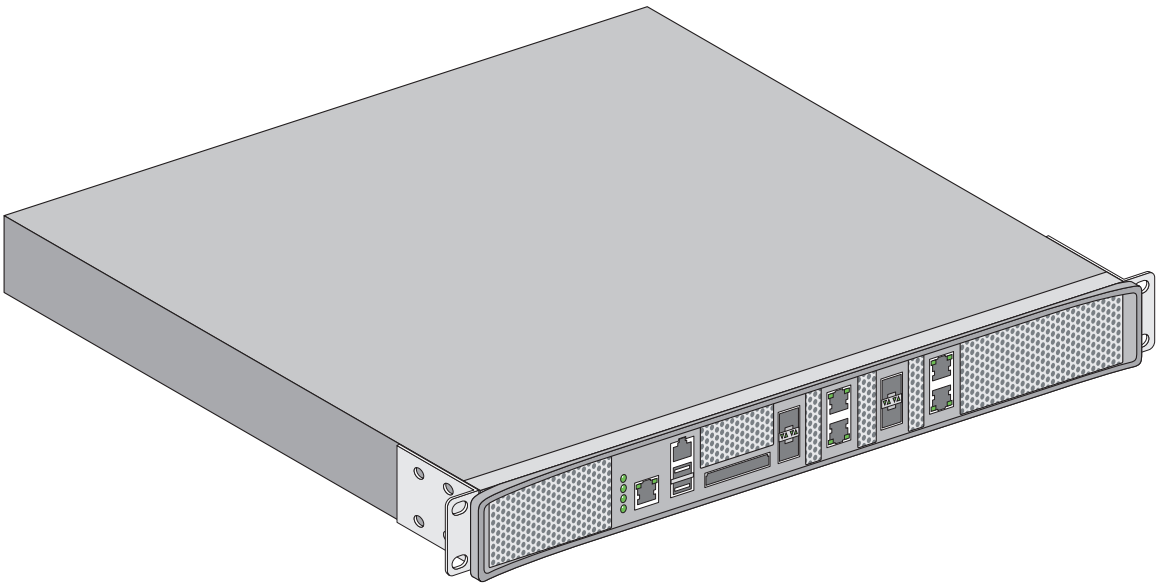
MOTOROLA

RFS7000 Series RF Switch

Troubleshooting Guide



Contents

Chapter 1. Overview

Chapter 2. LED Information

About this Guide

Introduction

This guide provides information about using the RFS7000 Series RF Switch.

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

Documentation Set

The documentation set for the RFS7000 Series RF Switch is partitioned into the following guides to provide information for specific user needs.

- **RFS7000 Installation Guide** - describes the basic setup and configuration required to transition to more advanced configuration of the switch.
- **RFS7000 CLI Reference** - describes the *Command Line Interface* (CLI) and *Management Information Base* (MIB) commands used to configure the RFS7000 Series RF Switch.
- **RFS7000 Troubleshooting Guide** - describes workarounds to known conditions the user may encounter.

Document Conventions

The following conventions are used in this document to draw your attention to important information:

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 RFS7000 Series Switch. Possible issues include

- *Switch Does Not Boot Up*
- *Switch Takes a Long Time to Start Up*
- *Switch Does Not Obtain an IP Address through DHCP*
- *Unable to Connect to the Switch using Telnet or SSH*
- *Web UI is Sluggish, Does Not Refresh Properly, or Does Not Respond*
- *Console Port is Not Responding*

1.1.1 Switch Does Not Boot Up

The RFS7000 Series Switch does not boot up to a username prompt via CLI console or Telnet.

The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Switch has no power	• Verify power cables, fuses, UPS power. The front panel LEDs lights up when power is applied to the switch. • Have a qualified electrician check the power source to which the switch is connected.
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 RFS7000 Series 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 on the Out-of-Band Management port.

The table below provides suggestions to troubleshoot this issue.

Possible Issue	Suggestions to Correct
DHCP is not configured, or not available on same network as the RFS7000 Series Switch	• Verify that the configuration for the switch has DHCP enabled. By default, the Gigabit ports have DHCP enabled. Otherwise, refer to the CLI Reference Guide or System Reference Guide for instructions on enabling the Gigabit Ethernet interfaces. • Connect another host configured for DHCP and verify it is getting a DHCP address

Possible Issue	Suggestions to Correct
DHCP is not enabled on a Gigabit Ethernet interface	• Enable DHCP for the port by using the CLI command or the Web UI to enable DHCP on the port connected to your external network. • Verify that DHCP packets are being sent to the port using a sniffer tool • If DHCP packets are seen, check to ensure that the switch is not configured for a static IP on the port.
All else..	Contact Motorola Support.

1.1.4 Unable to Connect to the Switch using Telnet or SSH

The RFS7000 Series Switch is physically connected to the network, but connecting to the switch using SSH or Telnet does not work.

The table below provides suggestions to troubleshoot this issue.

Possible Issue	Suggestions to Correct
Telnet is not enabled and/or SSH is disabled	Verify that Telnet or SSH are enabled by using the CLI or Web UI (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 that Telnet traffic is on the primary VLAN.
All else...	Contact Motorola Support.

1.1.5 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 RFS7000 Series Switch is providing the data to the browser. Occasionally, while using the Web UI 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. The table below provides suggestions to troubleshoot this issue.

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.
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.

Possible Issue	Suggestions to Correct
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/
Cannot access Web UI through a Firewall	To successfully access the switch Web UI through a firewall, UDP port 161 must be open in order for the switch's SNMP backend to function
All else...	Contact Motorola Support.

1.1.6 Console Port is Not Responding

The RFS7000 Series Switch console port is connected to the host computer's serial port, but pressing the [Enter] key gets no response from the switch.

The table below provides suggestions to troubleshoot this issue.

Possible Issue	Suggestions to Correct
Cabling issue	Ensure that a console cable is connected from the RFS7000 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 on the host computer.
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: Any COM port Terminal Settings: 19200 bps transfer rate, 8 data bits, no parity, 1 stop bit, no flow control
All else...	Contact Motorola Support.

1.1.7 GE Interface Loses VLANs After Reboot

When a GE Interface is configured as a trunk port with all VLANs (1-4094) allowed, after rebooting the interface will revert only be allowed on VLAN 1. This is a known issue and there is currently no workaround.

1.2 Access Port Issues

This section describes various issues related to access ports within the RFS7000 Series Switch network.

1.2.1 Access Ports are Not Adopted

Access ports are not being adopted. The table below provides suggestions to troubleshoot this issue.

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 RFS7000 Series Switch 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 RFS7000 Series Switch. If the switch is hung, it may begin to adopt access ports properly once it has been reset.
All else...	Contact Motorola Support.

1.2.2 Access Ports are Not Responding

Access Ports are not responding. The table below provides suggestions to troubleshoot this issue.

Possible Issue	Suggestions to Correct
Access Port not responding after converting to a Detector AP	When converting an AP300 to an Intrusion Detection Sensor, the conversion requires approximately 60 seconds.

Possible Issue	Suggestions to Correct
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 table below provides suggestions to troubleshoot this issue.

Possible Issue	Suggestions to Correct
Unadopted access port	Verify that 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 that the correct ESSID has been applied to the MU.
Ethernet port configuration issues	• Verify that 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 that 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 table below provides suggestions to troubleshoot this issue.

Possible Issue	Suggestions to Correct
Preamble differences	Verify that 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.

Possible Issue	Suggestions to Correct
Encryption Problems	If Encryption is being used, verify that the encryption settings on the MU and the switch match. If WEP Encryption is being used with non-Symbol or Motorola MUs, ensure that the key being entered is in HEX format and not a Passphrase.
Authentication Problems	If the switch is configured to use RADIUS authentication, check the RADIUS log file for any failure information.
Encryption or Authentication Problems	If you are using Authentication and/or Encryption on the switch, and the previous troubleshooting steps have not fixed the problem, try temporarily disabling Authentication and Encryption to see if that fixes the problem.

1.3.3 Poor Voice Quality Issues

VOIP MUs, BroadCast MultiCast and SpectraLink phones have poor voice quality issues. The table below 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 capabilities of the RFS7000 Series Switch.

1.4.1 Switch is Not Failing Over

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

The table below 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 that the Primary and Secondary switch are configured properly and attempt to ping each switch (using the *ping* command) from each switch.

Possible Issues	Suggestions to Correct
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.

1.5 Installation Issues

Upgrading and downgrading the RFS7000 Series Switch is possible only on the RFS7000 platform. Before upgrading or downgrading any system, save a copy of the system configuration to a FTP or TFTP server.

1.5.1 After Upgrade, Version Number Has Not Changed

After upgrading the version number has not changed. The table below 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 that the version number is correct using the CLI or the switch information page of the Web UI. Repeat the upgrade process if necessary.
All else...	Contact Motorola Support.

1.6 Miscellaneous Issues

This section describes various miscellaneous issues related to the RFS7000 Series Switch which 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 table below 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 table below 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

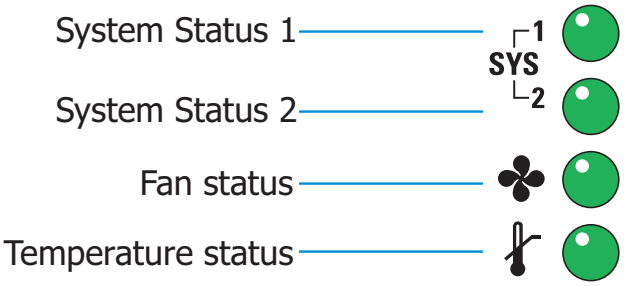
The RFS7000 Series Switch provides subsystem logging to a Syslog server. There are two Syslog systems, local and remote. Local Syslog records system information locally, on the switch. The remote Syslog sends messages to a remote host. All Syslog messages conform to the RFC 3164 message format.

2

LED Information

The RFS7010 RF Switch has four vertically-stacked LEDs on its front panel. Each of the switch's Gigabit Ethernet ports have two status LEDs. These LEDs display two colors (green & amber), and three lit states (solid, blinking, and off). The following tables decode the combinations of LED colors and states for the System Status LEDs and the Gigabit Ethernet LEDs.

2.1 System Status LEDs



2.1.1 Start Up / POST (Primary System or Redundant System)

System Status 1 LED	System Status 2 LED	Event
Off	Off	Power off
Green Blinking	Green Blinking	Power On Self Test (POST) running
Green Solid	Green Blinking	POST succeeded (Operating System Loading)
Green Solid	Off	POST succeeded (Normal Operation)
Amber Blinking	Off	POST Failure
Alternating Green Blinking & Amber Blinking	Alternating Green Blinking & Amber Blinking	Boot Up Error: Device has an invalid checksum

NOTE During switch start up, the Temperature status LED will be lit Solid Amber. This is normal behavior and does not indicate an error. At the completion of start up the Temperature Status LED will switch to Solid Green.

2.1.2 Switch Status (Primary System)

System Status 1 LED	System Status 2 LED	Event
Off	Off	Power off
Green Solid	Off	No Redundancy Feature Enabled
Green Solid	Green Solid	Redundancy Feature Enabled Actively Adopting Access Ports
Green Solid	Amber Blinking	No License to adopt Access Ports or No Country Code configured on the switch or License and Country Code configured, but no APs adopted

2.1.3 Switch Status (Redundant System)

System Status 1 LED	System Status 2 LED	Event
Off	Off	Power off
Green Solid	Off	No Redundancy Feature Enabled
Green Blinking	Green Solid	Redundant System failed over and adopting ports
Green Blinking	Alternating Green Blinking & Amber Blinking	Redundant System not failed over.
Green Solid	Amber Blinking	No License to adopt Access Ports or No Country Code configured on the switch or License and Country Code configured, but no APs adopted

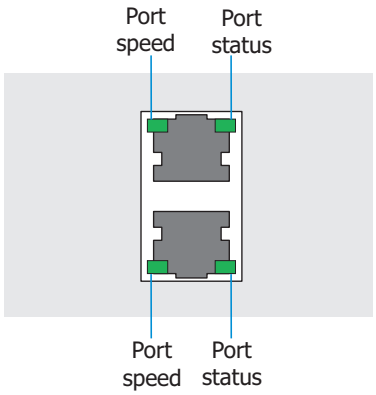
2.2 Fan LED

Fan LED	Event
Off	System Off / POST Start
Green Blinking	POST in Process
Green Solid	All System Fans Normal Operation
Amber Solid	Redundant Cooling Failure System Operational
Amber Blinking	System Cooling Failure *System will be held in reset until the issue is resolved*

2.3 Temperature Status LED

Temperature LED	Event
Off	System Off
Green Solid	Ambient Inlet Temperature is within specified operating limit
Amber Solid	Ambient Inlet Temperature is near the maximum operating temperature During switch start up this LED will be lit Solid Amber. This is normal behavior and does not indicate an error.
Amber Blinking	Ambient Inlet Temperature is above the maximum specified operating temperature *System will be held in reset until the issue is resolved*

2.4 RJ-45 Gigabit Ethernet LEDs



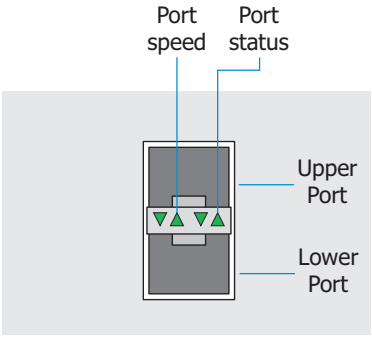
2.4.1 RJ-45 Port Speed LED

Port Speed LED	Event
Off	10 Mbps
Green Solid	100 Mbps
Green Blinking	1000 Mbps
Amber Blinking	Port Fault

2.4.2 RJ-45 Port Status LED

Port Status LED	Event
Off	No Link or Administratively shut down
Green Solid	Link present
Green Blinking	Activity: Transmit and Receive
Amber Blinking	Link Fault

2.5 SFP Gigabit Ethernet LEDs



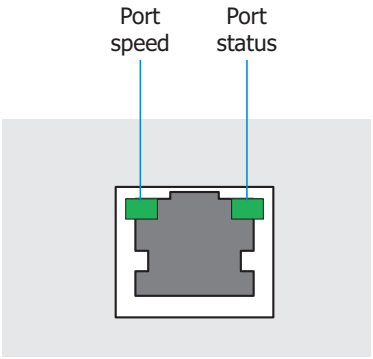
2.5.1 SFP Port Speed LED

Port Speed LED	Event
Green Blinking	1000 Mbps
Amber Blinking	Module or Tx/Rx Fault Loss

2.5.2 SFP Port Status LED

Port Status LED	Event
Off	No Link or Administratively shut down
Green Solid	Link present / Operational
Amber Blinking	Module or Tx/Rx Fault Loss

2.6 Out of Band Management Port LEDs



2.6.1 Out of Band Management Port Speed LED

Port Speed LED	Event
Off	10 Mbps
Green Solid	100 Mbps
Amber Blinking	Port Fault

2.6.2 Out of Band Management Port Status LED

Port Status LED	Event
Off	No Link
Green Solid	Link present
Green Blinking	Activity: Transmit and Receive
Amber Blinking	Link Fault

3

Network Events & Kern Messages

This chapter includes two network event tables to provide detailed information and understanding of the RFS7000 Series RF Switch network events that can occur. These tables are:

- *Network Event Message/Parameter Description Lookup*
- *Network Event Course of Action Lookup*
- *KERN Messages*

3.1 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.

3.1 Network Event Message/Parameter Description Lookup

ID	Event	Message	Parameters
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.
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.

3.1 Network Event Message/Parameter Description Lookup

ID	Event	Message	Parameters
16	AP detected	Detected a new access port <XX>.	XX = MAC (xx:xx:xx:xx:xx:xx) address of the access port.
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.

3.1 Network Event Message/Parameter Description Lookup

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]

3.1 Network Event Message/Parameter Description Lookup

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)

3.1 Network Event Message/Parameter Description Lookup

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]

3.2 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.

3.2 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 Symbol 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.

3.2 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 RFS7000s 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 RFS7000s on the same physical subnet. Either remove the extra switches or configure them for "Hot Standby" operation.

3.2 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		

3.2 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]		

3.2 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.

3.3 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.*

3.3 KERN Messages (Continued)

Module	Message	Description
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 RFS7000. 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.*

3.3 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.*

3.3 KERN Messages (Continued)

Module	Message	Description
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.*
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.*

3.3 KERN Messages (Continued)

Module	Message	Description
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 RFS7000.*
flowctl.c	PKT_INFO(""fc:allocs back down to %u"", curr_fc_allocs);	*The number of pending packets has fallen back below the limit.*
flowctl.c	PKT_ERR(""fc alloc:no memory for fc allocs"");	*Request from the operating system for a new packet has failed.*

3.3 KERN Messages (Continued)

Module	Message	Description
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.*

3.3 KERN Messages (Continued)

Module	Message	Description
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.*
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.*

3.3 KERN Messages (Continued)

Module	Message	Description
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.*
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..*

3.3 KERN Messages (Continued)

Module	Message	Description
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.*

3.3 KERN Messages (Continued)

Module	Message	Description
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.*
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.*

3.3 KERN Messages (Continued)

Module	Message	Description
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.*
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.*

3.3 KERN Messages (Continued)

Module	Message	Description
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.*

3.3 KERN Messages (Continued)

Module	Message	Description
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.*
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.*

3.3 KERN Messages (Continued)

Module	Message	Description
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.*

4

MU Disassociation Codes

4.1 802.11 Mobile Unit Disassociation Codes

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.

4.1 802.11 Mobile Unit Disassociation Codes (Continued)

ID	802.11 or Motorola/WPA Reason Code	Description
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.
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.

5

Troubleshooting SNMP Issues

The following SNMP-releated issued could require troubleshooting as SNMP issues are experienced with the RFS7000 switch.

5.1 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.

5.2 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.

5.3 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.

5.4 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)

5.5 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).

5.6 Still Not Working

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

6

Security Issues

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

- *Switch Password Recovery*
- *RADIUS Troubleshooting*
- *Rogue AP Detection Troubleshooting*
- *Troubleshooting Firewall Configuration Issues*

6.1 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:

   ```
   RFS7000 login: cli
   ```

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

   ```
   User Access Verification

   Username: restore
   Password: restoreDefaultPassword

   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.

6.2 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 Radius server configuration with the Switch's VLAN interface, IP address and subnet, which have been marked as management
- Save the current configuration
- Ensure that the WLAN settings haves been set to use the on-board/local Radius server by entering the local IP address or the switch management VLAN IP address

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 that 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 RFS7000 (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 a VLAN interface IP address which can communicate with 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 that the RADIUS Accounting server reachable
- Verify that the port number being configured on accounting configuration matches that of external RADIUS Accounting Server
- Verify that the shared secret being configured on accounting configuration matches that of external RADIUS Accounting Server

6.2.1 Troubleshooting RADIUS Accounting Issues

Use the following guidelines when configuring RADIUS Accounting

1. The RADIUS Accounting records are supported for clients performing 802.1X EAP based authentication or using the Hotspot functionality.
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 del command in the enable context.
5. If using the on-board RADIUS Accounting server, the files would be logged under the path: /flash/log/radius/radacct/

6.3 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 anyone of the detection mechanisms, 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 "Motorola 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.

6.4 Troubleshooting Firewall Configuration Issues

Motorola recommends adhereing to the following guidelines when dealing with problems related to RFS7000 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 RFS7000 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 RFS7000 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.

Appendix A Customer Support

Motorola's Enterprise Mobility Support Center

If you have a problem with your equipment, contact Enterprise Mobility support at *emb.support@motorola.com*

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-103892-01 Revision A
January 2008