613-000626 Rev.A 061006

fMAP
Log / Troubleshooting Manual
Release 8.0

Issue 1

Allied Telesis

About this Manual

This manual includes all log messages produced by the fMAP products, helps to isolate any problems associated with the log message and alarm to a specific component, and provides steps to repair or replace the component and clear the log message or alarm.

- Section 1 provides an overview of how the log message and alarm system is designed so that messages and alarms are generated at the local, remote (server), and NMS interfaces.
- Section 2 lists all of the log messages produced by the fMAP products and includes their associated Log Categories (such as CARD005), as well as Traps and Reason Codes. From this list the user can understand the scope of the problem and know which components to test.
- Section 3 lists the alarm messages (usually the Reason Code/Alarm Message) of the log and associates it with the specific log, the status of the alarm, and the status of the card LEDs.
- Sections 4 lists the traps/MIB specifications for fMAP devices. Highlighted are whether a MIB and an associated trap come from standards or from a fMAP MIB.

Table of Contents

1. Overview of Logs / Alarms System

1.1 Interfaces for Communicating with Devices

To receive event and alarm indicators from the fMAP devices, interfaces must have been configured so that these indicators are sent to the proper place and are filtered when necessary. This Section provides an overview of these interfaces.

Note: It is assumed that the user has set up the interfaces described in this Section and can readily communicate with the system through the MGMT or inband upstream port. However, a condition or conditions may exist where the user cannot communicate with the system or the user is not receiving logs on their configured log server or the NMS. If the condition(s) cannot be cleared, the user should contact Allied Telesis Technical Support.

1.1.0.1 fMAP

Figure 1-1 shows the physical and protocol interfaces that allow the fMAP product to communicate with management systems. One of two IP interfaces can be used:

- The MGMT Ethernet interface that transports only management data packets.
- An in-band Ethernet interface that interleaves user data packets with management data packets on the uplink, using a VLAN interface. In using a VLAN interface the management data packets are always VLAN-tagged.

Over these two interfaces, the TELNET or SNMP agent can be configured.

Note: Only one interface can be enabled at a time; enabling an interface will disable an interface already enabled. If necessary, the ENABLE IP INTERFACE command will automatically disable the other IP Interface.

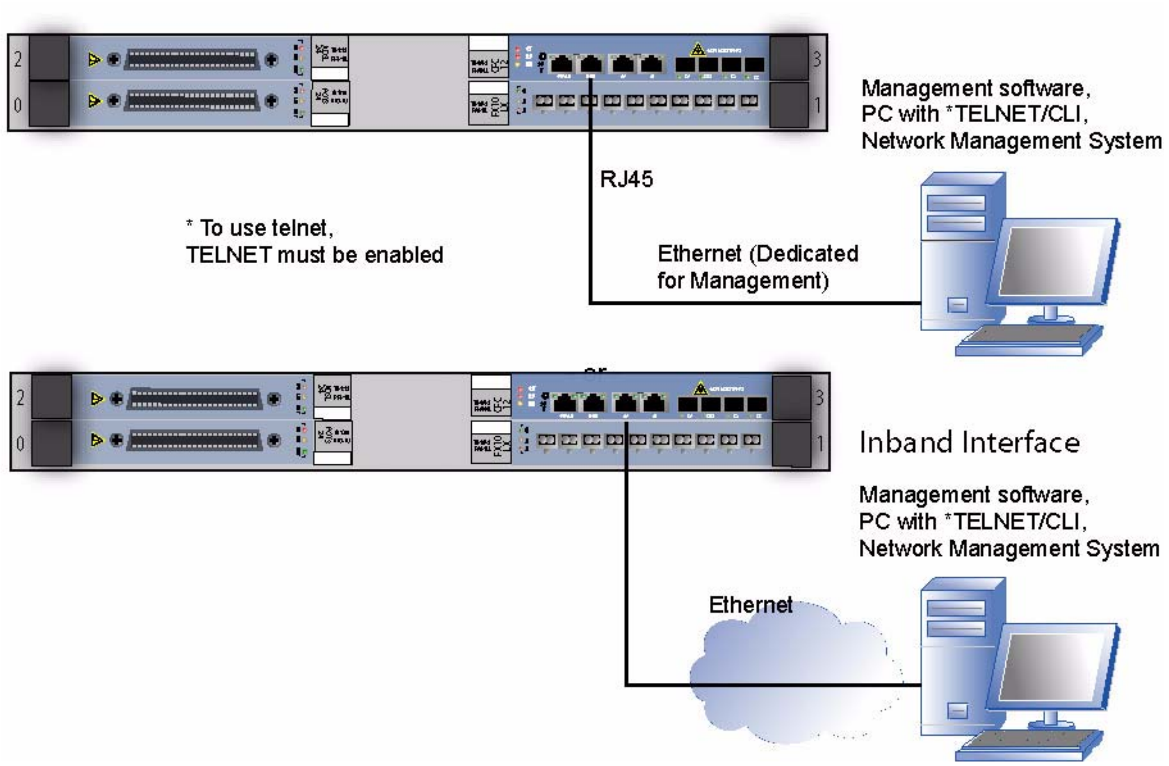


FIGURE 1-1 **Connections for Management Interfaces for the fMAP**

To enable TELNET access for the management ethernet interfaces, TELNET must be enabled. The user can then choose which interface to use and supply the IPADDRESS and SUBNETMASK for the fMAP product that will be used by the management device when a user logs in.

Note: These interfaces should be set up using the local RS232 interface. See the following Caution.

⚠	***If the user disables or deletes an IP interface, and the user is currently using that interface to communicate with the fMAP product, the interface will be immediately disconnected.***

1.1.0.2 PING

The system provides the user with the ability to ***ping*** network devices from the CLI command line interface.

An example of the PING command:

```
officer SEC> PING 172.16.17.18
officer SEC> PING 172.16.17.18 (172.16.17.18)
64 bytes from 172.16.17.18 (172.16.17.18): icmp_seq=1
--- 172.16.17.18 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
```

TABLE 1-1 PING command

Noun	Verb	Syntax	Description
PING	PING	PING={ipaddress|hostname} [DELAY=1..900] [LENGTH=1..65535] [NUMBER={1..65535|CONTINUOUS }] [TIMEOUT=1..900]	The PING command provides the user with the ability to determine whether a network device is accessible or not.

1.2 Types of Alarm Indicators

When the OAM system is configured as described in Chapter 3 of the **fMAP User Guide**, indicators for faults or potential faults are easy to generate, store, and output. The OAM system produces the following event and alarm indications: logs, Traps, and LED alarm indicators. These events are described in more detail below.

1.2.1 Alarm Severity

Allied Telesis system alarms are organized by order of severity level. They are Critical, Major, and Minor. Each level is described here.

1.2.1.1 Critical

Critical is the highest, most sever level of alarm. An alarm with a severity level of critical means that system service is being detrimentally affected. It requires the user’s immediate attention.

When a critical alarm conditions is raised, the CRIT LED on the CFC faceplate will be illuminated. The FAULT LED on a card faceplate may also be illuminated.

A log indicating a critical alarm will be prefaced by “***C**” as the first two characters in the first line of text. An example of a critical alarm log is illustrated below.

```
*C SYS009 2003-12-04 13:29:57 0327 FAULT
System: Raised Port Outage Threshold
```

FIGURE 1-2 Critical alarm log

1.2.1.2 Major

Major is the second highest level of alarm. An alarm with a severity level of major means that system service may be affected. The user must immediately investigate a major alarm.

When a major alarm conditions is raised, the MAJOR LED on the CFC faceplate will be illuminated. The FAULT LED on a card faceplate may also be illuminated.

A log indicating a major alarm will be prefaced by “**” as the first two characters in the first line of text. An example of a major alarm log is illustrated below.

```
**   PORT003   2003-12-04   13:30:04   0356
FAULT
Location: Slot: 5 Port: 1
Description: Port Fault Set
Reason Code: Loss Of Link
```

FIGURE 1-3 Major alarm log

1.2.1.3 Minor

Minor is the lowest level of alarm. An alarm with a severity level of minor means that system service is not affected. However, this alarm condition could lead to a major or critical alarm condition; therefore, the user should investigate the alarm.

When a minor alarm conditions is raised, the MINOR LED on the CFC faceplate will be illuminated. The FAULT LED on a card faceplate may also be illuminated.

A log indicating a minor alarm will be prefaced by “*” as the first character in the first line of text. An example of a minor alarm log is illustrated below.

```
 * SYS009 2003-12-04 15:20:31 2669 FAULT
System: Raised Port Outage Threshold
```

FIGURE 1-4 Minor alarm log

Some alarm conditions begin as a minor alarm, but as the alarm condition continues, its level will be raised. For example, a port outage threshold alarm may initially be raised as a minor alarm. However, if more ports encounter the same alarm condition and the number of ports in alarm increases, after a certain threshold is reached, the alarm will become a major alarm. Furthermore, if the alarm condition continues and even more ports encounter the same alarm condition and the number of ports in alarm increases, after a third threshold is reached, the alarm will become a critical alarm. Thresholds for this example, a port outage, are:

- Minor - Less than 24 downstream ports are impacted by card failures and there is at least one uplink available.
- Major - More than 24 but less than 128 downstream links are impacted by card faults and there is at least one uplink available.
- CRITICAL - More than 128 downstream ports are impacted by card faults and/or there is no uplink available.

1.2.2 Port Outage Threshold Configuration

In release 4.0, port outage thresholds can be configured by the Allied Telesis system user. Alarms can be configured to be either MAJOR, MINOR, or CRITIAL.

An example follows:

```
officer SEC>> SHOW ALARMS THRESHOLD
 Threshold Mark
 --------------------------------------
 MINOR                                 1
 MAJOR                                 24
 CRITICAL                              128
officer SEC>> SET ALARMS THRESHOLD MINOR=7 MAJOR=32 CRITICAL=96
Warning(033613): 6 ports can go out of service before
an alarm is raised if the MINOR threshold is 7.
 Threshold Mark
 --------------------------------------
 MINOR                                 7
 MAJOR                                 32
 CRITICAL                              96
 Info (010017): Operation Successful
officer SEC>> SETDEFAULTS ALARMS THRESHOLD
 Threshold Mark
 --------------------------------------
 MINOR                                 1
 MAJOR                                 24
 CRITICAL                              128
 Info (010017): Operation Successful
officer SEC>> SHOW ALARMS THRESHOLD
```

```
Threshold Mark
------------------------------------
MINOR                                1
MAJOR                                24
CRITICAL                             128
```

Note that the system will default to known thresholds if they have not been configured. Defaults are:

- MINOR - Less than or 24 ports
- MAJOR - 25-127 ports
- CRITICAL - More than 128 ports

TABLE 1-2 Port Outage Thresholds commands

Noun	Verb	Syntax	Description
ALARMS THRESHOLD	SET	SET ALARMS THRESHOLD [MINOR=value] [MAJOR=value] [CRITICAL=value]	The alarm thresholds control when the MINOR, MAJOR, and CRITICAL Port Outage Threshold alarms are raised. The values must be non-zero and satisfy the condition of MINOR, MAJOR, or CRITICAL. These signify the lowest number of ports for that alarm to be raised. Critical - Minimum number of ports before a CRITICAL alarm is raised. Major - Minimum number of ports before a MAJOR alarm is raised. Minor - Minimum number of ports before a MINOR alarm is raised. Setting minor to anything greater than one is allowed, but not recommended.That means that (MINOR - 1) ports can be out of service before the threshold alarm is raised. Note: When all UPLINK ports are out of service, a CRITICAL alarm will be raised regardless of the threshold values.
ALARMS THRESHOLD	SETDEFAULTS	SETDEFAULTS ALARMS THRESHOLD	This command sets all alarm threshold values back to the factory defaults.
ALARMS THRESHOLD	SHOW	SHOW ALARMS THRESHOLD	Displays the current settings for port alarm thresholds.

1.2.3 Logs

fMAP products provide totally flexible logging functionality. Refer to the **fMAP User Guide**, Section 4, for detailed descriptions of the log system and instructions for configuring log output. Refer to Section 2 of this document for a description of the log output and a listing of all the logs produced by the fMAP devices.

1.2.4 Relationship of Logs and Traps with Device Interfaces

Since there are multiple ways to report a device status as well as multiple interfaces to display them, the following summarizes how they are related:

Traps are produced and associated with:

- Standard (RFC-based) MIBs
- ATN Enterprise (ATN Enterprise MIB and Ext. Eth. DS3 MIB) – These are the fMAP products

All traps produce logs, and these logs have associated log messages, reason codes, and severities.

Some logs, on the other hand, do not have an associated trap. These are usually for status or update information.

1.2.5 CARD and PORT Logs (Information, Degrading and Failing Conditions)

The two most common logs for card and port logs are CARD023, CARD005, PORT013, and PORT003 logs.

- CARD023 logs are intended to indicate INFO conditions that do not affect state, such as file corruption, database upgrade, multicast stream limit, and inconsistent load.
- CARD005 covers all failing and degrading conditions.

Note: Both of those logs generate the same SNMP trap.

- PORT005 logs are for degrading conditions, and PORT013 is informational only.

1.2.6 LED

These products are equipped with LED alarm indicators on the front panels of system cards. See the **fMAP Component Specification** for detailed descriptions of system LEDs. The following table lists and describes the LED alarm indicators for each card type

Note: In the specific procedures, the alarm LEDs are included since they help to isolate the faulty component. The user should, however, study and refer to this table since they help in understanding the overall system design.

TABLE 1-3 **LED indicators**

Card Type	LED	Meaning	Notes
ADSLn /	PULL	n/a	The card has been disabled, is out of service and can be removed for replacement. Note: All subscribers provisioned on this card are now out of service.
	FAULT	Minor, Major, Critical	A fault is present on the card. Check for logs associated with this card and display the fault using the SHOW ALARMS command. Note: All subscribers provisioned on this card may be experiencing a service interruption.
	INSRV	n/a	The card has been enabled and is in service.

TABLE 1-3 LED indicators (Continued)

Card Type	LED	Meaning	Notes
CFCn	PULL	n/a	The card has been disabled, is out of service and can be removed for replacement. Note: If the system is configured for simplex mode, all subscribers are now out of service.
	FAULT	See Minor, Major, Critical LEDs	A fault is present on the card. Check for logs associated with this card and display the fault using the SHOW ALARMS command. Note: If the system is configured for simplex mode, all subscribers may be experiencing a service interruption.
	INSRV	n/a	The card has been enabled and is in service.
	ACT	n/a	For systems configured for duplex mode, this LED indicates that this CFC is Active
	CRIT	Critical	A Critical system alarm is present. Check for logs associated with this card and display the fault using the SHOW ALARMS command. Note: If the system is configured for simplex mode, all subscribers may be experiencing a service interruption.
	MAJOR	Major	A Major system alarm is present. Check for logs associated with this card and display the fault using the SHOW ALARMS command. Note: If the system is configured for simplex mode, all subscribers may be experiencing a service interruption.
	MINOR	Minor	A Minor system alarm is present. Check for logs associated with this card and display the fault using the SHOW ALARMS command. Note: All subscribers provisioned on this system may be experiencing a service degradation.
FAN8 Fan Controller	PULL	n/a	The card has been disabled, is out of service and can be removed for replacement.
	FAULT	Minor, Major, Critical	A fault is present on the card. Check for logs associated with this card and display the fault using the SHOW ALARMS command.
	INSRV	n/a	The card has been enabled and is in service.

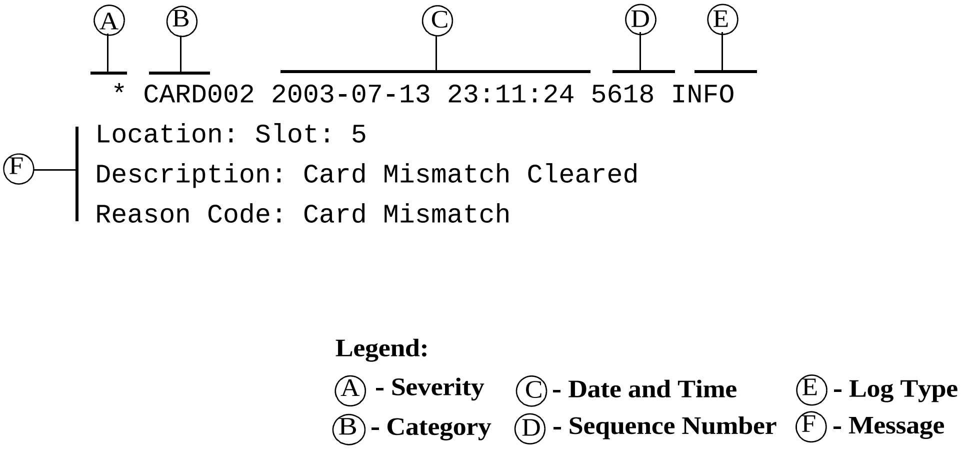
TABLE 1-3 LED indicators (Continued)

Card Type	LED	Meaning	Notes
FC7	PULL	n/a	The card has been disabled, is out of service and can be removed for replacement.
	FAULT	Minor, Major, Critical	A fault is present on the card. Check for logs associated with this card and display the fault using the SHOW ALARMS command.
	INSRV	n/a	The card has been enabled and is in service.
Fiber	PULL	n/a	The card has been disabled, is out of service and can be removed for replacement. Note: All subscribers provisioned on this card are now out of service.
	FAULT	Minor, Major, Critical	A fault is present on the card. Check for logs associated with this card and display the fault using the SHOW ALARMS command. Note: All subscribers provisioned on this card may be experiencing a service interruption.
	INSRV	n/a	The card has been enabled and is in service.
	Link	n/a	When illuminated, indicates that the port is operationally UP and data traffic is flowing over the port.
GEn	PULL	n/a	The card has been disabled, is out of service and can be removed for replacement. Note: If the system is provisioned with a single up link with no standby, all subscribers provisioned are now out of service.
	FAULT	Minor, Major, Critical	A fault is present on the card. Check for logs associated with this card and display the fault using the SHOW ALARMS command. Note: All subscribers provisioned on this system may be experiencing a service interruption.
	INSRV	n/a	The card has been enabled and is in service.
	LINK	n/a	The TCP/IP link is UP.

2. Interpreting Log Messages

2.1 Log Formats

The fMAP product produces management logs that provide information about all changes that occur. Figure 2-1 shows an example log.



```
 * CARD002 2003-07-13 23:11:24 5618 INFO
Location: Slot: 5
Description: Card Mismatch Cleared
Reason Code: Card Mismatch
```

FIGURE 2-1 Sample Log Produced by the fMAP product

2.1.1 Log Messages from the CLI

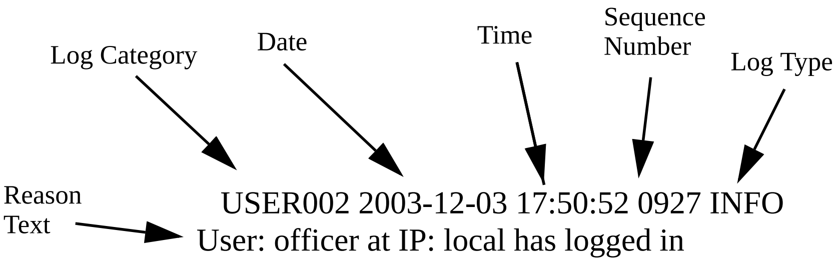
Use the SHOW LOG command to filter logs immediately in the output, for example to show only logs that have a severity of CRITICAL.

2.1.2 Examples

Examples of system logs follow:

2.1.2.1 Informational (INFO) logs

These logs record events that may have an associated trap. Those that do have a an associated trap are included in this document.

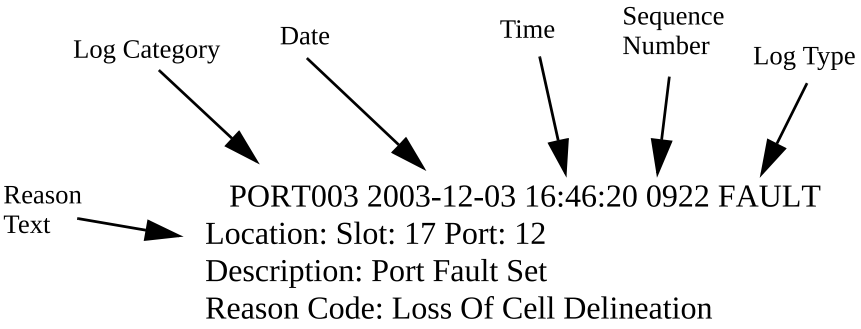


```
USER002 2003-12-03 17:50:52 0927 INFO
User: officer at IP: local has logged in
```

FIGURE 2-2 Informational log

2.1.2.2 Fault logs

These are the logs that have associated traps as well as reason codes and are the ones included in this document.

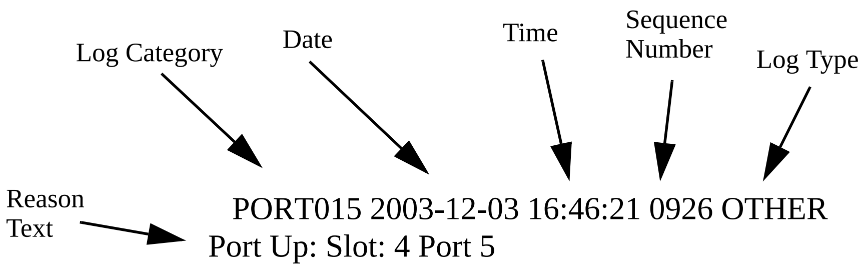


```
PORT003 2003-12-03 16:46:20 0922 FAULT
Location: Slot: 17 Port: 12
Description: Port Fault Set
Reason Code: Loss Of Cell Delineation
```

FIGURE 2-3 Fault log

2.1.2.3 Other logs

Logs of the type OTHER are for events such as a change of state and are useful for monitoring system activity as the system goes through changes in configuration. Some logs can have associated traps and these are included in this document.



```
PORT015 2003-12-03 16:46:21 0926 OTHER
Port Up: Slot: 4 Port 5
```

FIGURE 2-4 **Other logs**

2.2 Log Message Reference

This Log Message Reference lists the trap-associated logs and uses the following attributes:

- Category - These are explained in Section 1 and include the number within the category. NMS messages have the category NMS.
- Type - The types possible are FAULT, OTHER, INFO, and PROGRESS INDICATOR. For the NMS, the type is the associated configuration area (such as Discovery).
- Trap Text - This is the message passed with the log; these are listed in the NMS trap parser.
- Severity - These are critical, major, minor, and warning.
- Log Message - This is the text string that specifies the problem, and may include variables that identify a specific component.
- Reason Code - This can further identify the problem.
- Overview - This explains the scope of the problem and the possible faulty components.
- The log messages are listed by Category, Reason Code, and Trap Text. Reading the logs with these attributes allows the user to quickly find the log in this table.

2.3 Network Loops

Network loops may be indicated by service degradations, connectivity problems on a link(s), etc. If the user suspects the presence of a network loop, they should attempt to find the loop and correct it. Some things that the user should look at are recent port and interface provisioning, recent EPSR provisioning, recent STP provisioning, and recent wiring and connections made within their network or connections external to their network.