SSE-F3548S/SSE-F3548SR

RMON

User's Guide

Revision 1.0

The information in this USER'S GUIDE has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person organization of the updates. Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

DISCLAIMER OF WARRANTY ON SOFTWARE AND MATERIALS. You expressly acknowledge and agree that use of the Software and Materials is at your sole risk. FURTHERMORE, SUPER MICRO COMPUTER INC. DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR MATERIALS IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SUPER MICRO COMPUTER INC. OR SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE SOFTWARE AND/OR MATERIALS PROVE DEFECTIVE, YOU (AND NOT SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICE, REPAIR, OR CORRECTION.

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES INCLUDING NEGLIGENCE, SHALL SUPER MICRO COMPUTER INC. BE LIABLE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OR INABILITY TO USE THE SOFTWARE OR MATERIALS, EVEN IF SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Super Micro's total liability for all claims will not exceed the price paid for the hardware product.

Manual Revision 1.0
Release Date: 3/2/2020

Document Revision History

Date	Revision	Description
03/2/2020	1.0	Initial document.

Contents

1 RMON Overview

Remote monitoring (RMON) is a method similar to Simple Network Management Protocol (SNMP) and uses a client-server model to monitor/manageremote devices on the network. RMON and SNMP differ in the approach used:

- RMON is used for "flow-based" monitoring, while SNMP is often used for "device-based" management. The data collected in RMON deals mainly with traffic patterns rather than the status of individual devices as in SNMP.
- RMON is implemented basedon SNMP. RMON sends traps to the management device to notify the abnormality of the alarm variables by using the SNMP trap mechanism. Traps in RMON and those in SNMP have different monitored targets, triggering conditions, and report contents.
- RMON provides an efficient means of monitoring subnets. The managed device sends a trap to the management device automatically once an alarm has reached a certain threshold value.
- Unlike SNMP, the management device need not get the values of MIB variables multiple times for comparison. Hence the communication traffic between the management device and the managed device is reduced.

RMON provides statistics and alarm functionality to monitor managed devices.

- The statistics function tracks traffic information on the network segments connecting to its ports. For e.g. number of oversize packets received.
- The alarm function aids in monitoring the value of a specified MIB variable. Italso handleevents such as trap or log to be sent to the management device when its value reaches a particular threshold. For e.g. rate of packets received reaches a certain value.

RMON protocol allows multiple monitors or management devices. A monitor provides two ways of data gathering:

- Using RMON probesfrom which Management devices can get data directly and control network resources. In this approach, management devices can obtain all RMON MIB information.
- RMON agents in routers and switches. Management devices exchange data with RMON agents using SNMP operations, which, due to system resources limitation, may not cover all MIB information but four groups of information, alarm, event, history, and statistics, in most cases.

Supermicro supports minimal RMON agent implementation for Ethernet interfaces.

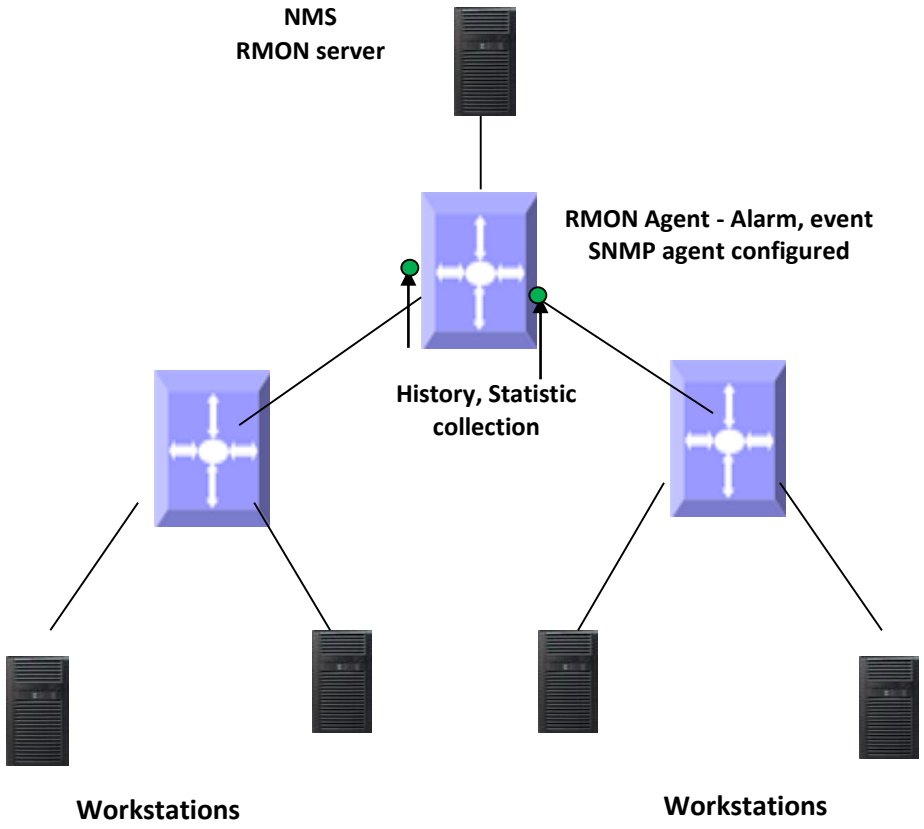

Figure RMON-1: RMON Operation

2 RMON Groups

Supermicro supports four groups from RMON MIB1 defined by RMON specifications: event group, alarm group, history group and statistics group.

2.1 Alarm group

The RMON alarm group monitors specified alarm variables, such as total number of received packets on an interface. Once an alarm entry is defined, the switch checks the value of the monitored alarm variable at the specified interval. When the value of the monitored variable is greater than or equal to the upper threshold, an upper event is triggered; when the value of the monitored variable is smaller than or equal to the lower threshold, a lower event is triggered. The event is then handledas specified in the event group.

If the value of a specified alarm MIB variable fluctuates, then the rising alarm and falling alarm alternate i.e. only the first one triggers an alarm event.

2.2 Event Group

The event group defines event indexes and controls the generation and notifications of the events triggered by the alarms defined in the alarm group. The events can be handled by either of the following ways:

- Logging event related information in the event log table of the RMON MIB of the switch.
- Trap: Sending a trap to notify the occurrence of this event to the management device.

2.3 Statistics

RMON statistics function is implemented by either the Ethernet statistics group or the history group. The objects of the statistics are different for both these groups;however both groups record statistics on the interfaceas a cumulative sum for a particular period.

2.3.1 History group

The history group specifies periodic collection of traffic information statistics on an interface and saves the statistics in the history record table. The statistics data includes bandwidth utilization, number of error packets, and total number of packets.

2.3.2 Ethernet statistics group

The statistics group specifies collection of various traffic statistics information on an Ethernet interface and saves it in the Ethernet statistics table. The statistics data includes network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, and packets received etc.

3 RMON Configuration

This section describes RMON configuration for Supermicro switches.

Parameter	Default Value
RMON status	Disabled
Collection statistics	None
Collection history	None
Alarms	None
Events	None

3.1 Enabling RMON

RMON is disabled by default in Supermicro switches. Follow the below steps to enable RMON.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	set rmon enable	Enable RMON in the switch.
Step 3	End	Exit from Configuration mode.
Step 4	Show rmon	Display RMON status.

The “set rmon disable” command disables RMON in the switch.

RMON must be enabled before any other RMON configuration.

The example below shows the commands used to enable RMON.
SMIS# configure terminal
SMIS(config)# **set rmon enable**
SMIS(config)# end
SMIS# show rmon
RMON is enabled

3.2 Configuring Alarms and Events

The alarm group periodically takes statistical samples from variables and compares them with the configured thresholds. When a threshold is crossed, an event is generated using the alarm mechanism. The event group generates events whenever an alarm condition takes place in the device. The alarm group calls the event group, so an event must already be createdfor the alarm to call.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	rmon alarm <alarm-number><mib-object-id (255)><sample-interval-time (1-65535)>{absolute | delta } rising-threshold <value (0-2147483647)><rising-event-number (1-65535)> falling-threshold <value (0-2147483647)><falling-event-number (1-65535)> [owner <ownername (127)>]	(Optional) Set an alarm on a MIB object. alarm-number - Alarm Number. This value ranges between 1 and 65535. mib-object-id - The mib object identifier. sample-interval-time - Time in seconds during which the alarm monitors the

		MIB variable. This value ranges between 1 and 65535 seconds. absolute - Used to test each mib variable directly. delta - Used to test the change between samples of a variable. rising-threshold - A number at which the alarm is triggered. This value ranges between 0 and 2147483647. falling-threshold*value* - A number at which the alarm is reset. This value ranges between 0 and 2147483647. NOTE: Falling threshold must be less than rising threshold. rising-event-number - The event number to trigger when the rising threshold exceeds its limit. This value ranges between 1 and 65535. falling-event-number - The event number to trigger when the falling threshold exceeds its limit. This value ranges between 1 and 65535. Owner – Owner of the alarm, string of length 127.
Step 3	rmon event <number (1-65535)> [description <event-description (127)>] [log] [owner <ownername (127)>] [trap <community (127)>]	(Optional) Add an event in the RMON event table that is associated with an RMON event number. Number - Event number Description - Description of the event Log - Used to generate a log entry Owner - Owner of the event, , in range 1- 127 characters

		Trap - Used to generate a trap. The SNMP community string is to be passed for the specifiedtrap. NOTE : When RMON event trap is enabled, SNMP agent must be configured prior to configuring the RMON alarm function as described in SNMP Configuration guide (www.supermicro.com).
Step 4	end	Exit from Configuration mode.
Step 5	show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history [history-index (1-65535)] [overview]]	Display RMON statistics, alarms, events history and overview.

The “no rmon alarm <number (1-65535)>” and“no rmon event <number (1-65535)>” commandsdelete the RMON alarm configuration and RMON event configuration respectively.

When the alarm variable is the MIB variable defined in the history group or the Ethernet statistics group, RMON Ethernet statistics function or RMON history statistics function should be configured on the particular Ethernet interface, elsethe creation of the alarm entry fails, and no alarm event is triggered.

3.3 Configuring Statistics

The RMON Ethernet statistics group collects statistics for each monitored interface on the switch and stores them in the Ethernet statistics table. Only one statistics entry can be createdper interface.
The RMON Ethernet history group collects a periodic statistical sampling of the data collected by the Ethernet statistics group and stores them in the Ethernet history table. Multiple history entries can be configured on one interface, however all should have different values.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <*interface-type*><*interface-id*> or **interface range <*interface-type*><*interface-id*>** **….**	(Optional) Enters the interface configuration mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx interface-id is in slot/port format for all physical interfaces.

		To configure multiple interfaces, use the “interface range …” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	rmon collection stats <index (1-65535)> [owner <ownername (127)>]	(Optional) Enable RMON statistic collection on the interface index - Statistics table index, in range 1-65535 owner - Optional field that allows you to enter the name of the owner of the RMON group of statistics with a string length of 127
Step 4	rmon collection history <index (1-65535)> [buckets <bucket-number (1-65535)>] [interval <seconds (1-3600)>] [owner <ownername (127)>]	(Optional) Enable history collection for the specified number of buckets and time period index - History table index, in range 1-65535 buckets - The maximum number of buckets desired for the RMON collection history group of statistics. interval - The number of seconds in each polling cycle, in range 1-3600 owner - Optional field - allows the user to enter the name of the owner of the RMON group of statistics, string of length 127.
Step 5	show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history [history-index (1-65535)] [overview]]	Display RMON statistics, history and overview.

The “no rmon collection stats <index (1-65535)>” and “no rmon collection history <index (1-65535)>” commands delete the RMON collection configuration.

3.4 RMON Configuration Example

A sample RMON configuration of alarms, events and collection statistics and History in a Supermicro switch is specified below.

1) Enable RMON
2) Create events for Rising and falling threshold.
3) Create the alarm for the MIB object in 1 1.3.6.1.6.3.16.1.2.1.4table.
4) Create statistics collection on an interface.
5) Display all RMON configurations.

```
SMIS# configure terminal
SMIS(config)# set rmon enable
SMIS(config)# rmon event 1 description rise log owner smicro1 trap PUBLIC
SMIS(config)# rmon event 2description fall log owner smicro1 trap NETMAN
SMIS(config)# rmon alarm 1 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.1012 absolute  rising-threshold 2 1
falling-threshold 1 2 owner smicro1
SMIS(config)# interface Fx 0/5
SMIS(config-if)# rmon collection history 1 buckets 2 interval 20
SMIS(config-if)# rmon collection stats 1
SMIS(config-if)# end
SMIS# show rmon statistics
RMON is enabled
Collection 1 on Fx0/5 is active, and owned by monitor,
 Monitors ifEntry.1.5 which has
 Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
 # of packets received of length (in octets):
 64: 0, 65-127: 0, 128-255: 0,
 256-511: 0, 512-1023: 0, 1024-1518: 0

SMIS# show rmon events
RMON is enabled
Event 1 is active, owned by smicro1
 Description is rise
 Event firing causes log and trap to community PUBLIC,
 Time last sent is Apr 29 10:12:20 2013
 Logging Event With Description : rise
Event 2 is active, owned by smicro1
 Description is fall
```

```
 Event firing causes log and trap to community NETMAN,
 Time last sent is Apr 29 10:11:01 2013

SMIS# show rmon history
RMON is enabled

Entry 1 is active,  and owned by
 Monitors ifEntry.1.5 every 20 second(s)
 Requested # of time intervals, ie buckets, is 2,
 Granted # of time intervals, ie buckets, is 2,
  Sample 2 began measuring at Apr 29 10:13:52 2013
   Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
   # of dropped packet events is 0
   Network utilization is estimated at 0
  Sample 3 began measuring at Apr 29 10:14:12 2013
   Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
   # of dropped packet events is 0
   Network utilization is estimated at 0

SMIS# show rmon alarms
RMON is enabled
Alarm 1 is active,  owned by smicro1
 Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every 2 second(s)
 Taking absolute samples, last value was 2
 Rising threshold is 2, assigned to event 1
 Falling threshold is 1, assigned to event 2
 On startup enable rising or falling alarm

SMIS# show rmon history overview
RMON is enabled
Entry 1 is active,  and owned by
 Monitors ifEntry.1.5 every 20 second(s)
 Requested # of time intervals, ie buckets, is 2,
 Granted # of time intervals, ie buckets, is 2,

SMIS# show rmon statistics 1 alarms events history 1

RMON is enabled
Collection 1 on Fx0/5 is active, and owned by monitor,
```

```
 Monitors ifEntry.1.5 which has
 Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
 # of packets received of length (in octets):
 64: 0, 65-127: 0, 128-255: 0,
 256-511: 0, 512-1023: 0, 1024-1518: 0
Alarm 1 is active,  owned by smicro1
 Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every 2 second(s)
 Taking absolute samples, last value was 2
 Rising threshold is 2, assigned to event 1
 Falling threshold is 1, assigned to event 2
 On startup enable rising or falling alarm

Event 1 is active, owned by smicro1
 Description is rise
 Event firing causes log and trap to community PUBLIC,
 Time last sent is Apr 29 10:12:20 2013
 Logging Event With Description : rise
Event 2 is active, owned by smicro1
 Description is fall
 Event firing causes log and trap to community NETMAN,
 Time last sent is Apr 29 10:11:01 2013
Entry 1 is active,  and owned by
 Monitors ifEntry.1.5 every 20 second(s)
 Requested # of time intervals, ie buckets, is 2,
 Granted # of time intervals, ie buckets, is 2,
  Sample 4 began measuring at Apr 29 10:14:32 2013
   Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
   # of dropped packet events is 0
   Network utilization is estimated at 0
  Sample 5 began measuring at Apr 29 10:14:52 2013
   Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
   # of dropped packet events is 0
   Network utilization is estimated at 0
SMIS# write startup-config
```

```
Building configuration, Please wait. May take a few minutes ...
[OK]
SMIS# show running-config
Building configuration...
ID   Hardware Version              Firmware    OS       Boot Loader
0        SSE-F3548              1.0.0.0     6        0.0.0.0vlan 1
ports fx 0/1-24 untagged
ports cx 0/1-3 untagged
exit
set rmon enable
rmon event 1 description rise log owner smicro1  trap PUBLIC
rmon event 2 description fall log owner smicro1  trap NETMAN
rmon alarm 1 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 2 absolute rising-thresh
old 2 1 falling-threshold 1 2 owner smicro1
interface Fx 0/5
rmon collection stats 1 owner monitor
rmon collection history 1 buckets 2 interval 20
exit
```

3.5 Configuring Port Rate Limit

Rate limit is disabled by default in Supermicro switches. Follow the below steps to enable the port rate limit.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <*interface-type*><*interface-id*> or interface range <*interface-type*><*interface-id*> ….	(Optional) Enters the interface configuration mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20

		If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	rate-limit output <rate-value-kbps (1-10000000)><burst-value-kbits (1-10000000)>	Enables the egress rate limit for the interface(s), set to the closest rate (kbps) and burst size (kbits) as the hardware capabilities. Rate limiting is applied to packets sent out on a particular interface. Rate limit and burst size in range of1-10000000.
Step 4	End	Exits the configuration mode.
Step 5	show interface [{ [<interface-type><interface-id>] rate-limit	Displays the rate limit configuration on an interface

The “no rate-limit output” command disablesthe ratelimit on a particular interface**.**

The example below shows the commands used to configure the rate limit.
SMIS# configure terminal
SMIS(config)# interface Fx 0/20
SMIS(config-if)# rate-limit output 500000 4800
SMIS(config-if)# end

SMIS# show interface Fx 0/20 rate-limit
Fx0/20
Rate Limit : 500000 Kbps
Burst Size : 4800 Kbps

3.6 Configuring HOL Blocking Prevention

HOL is enabled by default in Supermicro switches. Follow the steps below to disable HOL blocking.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no hol blocking prevention	Disables HOL blocking
Step 3	End	Exits the configuration mode.
Step 4	show interfaces [{ [<interface-type><interface-id>]	Displays theinterface configuration.

The “hol blocking prevention” command enables HOLblocking.

The example below shows the commands used to disable HOL blocking.

```
SMIS# configure terminal
SMIS(config)# interface Fx 0/4
SMIS(config-if)# no hol blocking prevention
SMIS(config-if)# end
SMIS# show interface Fx 0/4

Fx0/4 up, line protocol is down (not connect)
Bridge Port Type: Customer Bridge Port
Hardware Address is 00:30:48:e3:04:78
MTU  1500 bytes, Full duplex, 25 Gbps,  Auto-Negotiation
HOL Block Prevention disabled.
Input flow-control is off, output flow-control is off

Link Up/Down Trap is enabled
Reception Counters
  Octets               : 0
  Unicast Packets      : 0
  Broadcast Packets    : 0
  Multicast Packets    : 0
  Pause Frames         : 0
  Undersize Frames     : 0
  Oversize Frames      : 0
  CRC Error Frames     : 0
  Discarded Packets    : 0
  Error Packets        : 0
  Unknown Protocol     : 0

Transmission Counters
  Octets               : 0
  Unicast Packets      : 0
  Non-Unicast Packets  : 0
  Pause Frames         : 0
  Discarded Packets    : 0
  Error Packets        : 0
```

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
Web Site:	www.supermicro.com

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer Support)
Web Site:	www.supermicro.com.nl

Asia-Pacific

Address:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
Web Site:	www.supermicro.com.tw