VIA Networking Technologies, Inc.

VSNMP-GE User Guide

Revision 1.50
May 19, 2004

VIA Networking Technologies, INC.

Copyright Notice:

Disclaimer Notice:

No license is granted, implied or otherwise, under any patent or patent rights of VIA Networking Technologies Inc. VIA Networking Technologies Inc. makes no warranties, implied or otherwise, in regard to this document and to the products described in this document. The information provided by this document is believed to be accurate and reliable as of the publication date of this document. However, VIA Networking Technologies Inc. assumes no responsibility for any errors in this document. Furthermore, VIA Networking Technologies Inc. assumes no responsibility for the use or misuse of the information in this document and for any patent infringements that may arise from the use of this document. The information and product specifications within this document are subject to change at any time, without notice and without obligation to notify any person of such change.

Offices:

USA Office:
940 Mission Court
Fremont, CA 94539
USA
Tel: (510) 683-3300
Fax: (510) 683-3301 -or- (510) 687-4654
Web: http://www.vntek.com

Taipei Office:
8th Floor, No. 533
Chung-Cheng Road, Hsin-Tien
Taipei, Taiwan ROC
Tel: (886-2) 2218-5452
Fax: (886-2) 2218-5453
Web: http://www.vntek.com.tw

Revision History

Document Release	Date	Revision	Initials
1.20	9/16/03	Initial Release.	Checa
1.30	11/18/03	Update cover.	Checa
1.40	04/16/04	Remove “VT6121” from product list.	Checa
1.50	05/19/04	Change supported adapter name.	Checa

TABLE OF CONTENTS

1. Introduction

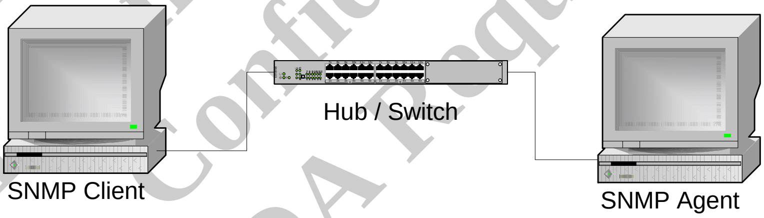
Network statistics and control information are easily retrieved by using standard SNMP protocol. Network administrator could use MIB browser to get the information from remote host if it is SNMP protocol available. VIA Networking Rhine-GE Family Gigabit Ethernet Adapter supports standard MIB-II counters and some of the RMON counters in the device driver. However, there are some other component should be installed for the full SNMP operations.

1. SNMP service: Microsoft provides SNMP service in Microsoft platform. Users need to install SNMP service for SNMP protocol.
2. SNMP extension agent: SNMP extension agent is a vendor provided software. For the RMON counter support, a SNMP extension agent is provided by VIA Networking to make it visible for MIB browser because RMON is not the default support counter in Microsoft SNMP service.

2. Configuration Example

Configuration	SNMP Client
PC	Clone PC
MB	ASUS P3B-F
DRAM	SDRAM 128MB
NIC	One of VIA Networking Rhine-GE Family Gigabit Ethernet Adapter
NIC Driver	1.17
OS	Windows 98 SE
SNMP Client Software	MG-SOFT MIB Browser Professional Edition 7.0.0.3730

Configuration	SNMP Agent
PC	Clone PC
MB	ASUS P3B-F
DRAM	SDRAM 128MB
NIC	One of VIA Networking Rhine-GE Family Gigabit Ethernet Adapter
NIC Driver	1.17
OS	Windows 2000 Professional
SNMP Agent Module	Windows SNMP Service
SNMP Agent Trap Module	Windows SNMP Trap Service



3. SNMP service operation

1.1 Install SNMP service in Windows 2000/XP/Server 2003

In Microsoft windows 2000, XP and Server 2003, SNMP service installation procedure is listed as the following:

1. Click **Start**, point to **Settings**, click **Control Panel**, double-click **Add/Remove Programs**, and then click **Add/Remove Windows Components**.
2. In **Components**, click **Management and Monitoring Tools** (but do not select or clear its check box), and then click **Details**.
3. Select **Simple Network Management Protocol** check box, and click **OK**.
4. Click **Next** to do the installation.

Note:

1. You must be logged on as an administrator or a member of the Administrators group in order to complete this procedure. If your computer is connected to a network, network policy settings might also prevent you from completing this procedure.
2. SNMP starts automatically after installation.
3. For Windows Server 2003, community policy needed to add manually in order to query the status of SNMP service.
   - First you need to open Control Panel→Administrative Tools→Services, then locate SNMP service in the service list.
   - Second open SNMP Service→Properties, and click the Security tab. Add a pair of Community/Rights to the list of Accepted Community Names.

1.2 Install SNMP service in Windows 98

In Microsoft windows and 98, SNMP service installation procedure is listed as the following:

1. Click **Start**, point to **Settings**, click **Control Panel**, double-click **Network**, and then click **Add**.
2. In the **select Network Components Type** dialog box, double click **Service**.
3. In the **select Network Service** dialog box, click **Have Disk**.
4. In the **Install From Disk** dialog box, type the path to the **\TOOLS\RESKIT\NETADMIN\SNMP** directory on the windows 98 compact disc, and then click **OK**.
5. In the **select Network Service** dialog box, select **Microsoft SNMP agent** from the **Models** list, and then click **OK**.
6. In the **System Setting Change** dialog box, click **OK** to restart the system and finish the installation.

Note:

1. SNMP starts automatically after system restart.

1.3 Install SNMP service in Windows NT4

In Microsoft windows NT4, SNMP service installation procedure is listed as the following:

1. Click **Start**, point to **Settings**, click **Control Panel**, double-click **Network.**
2. In the **Network** dialog box, click **Services** tab.
3. In the **Services** tab, click **Add**.
4. In the **Select Network Service** dialog box, select **SNMP Service** from the **Network Service** list, and then click **OK**.
5. In the **Windows NT Setup** dialog box, type the Windows NT Source Path, and then click **Continue**.
6. After **Windows NT Setup** finish file-copy, in the **Windows SNMP Properties** dialog box click **OK.**
7. In the **Network** dialog box, **SNMP Service** will add to the N**etwork Services** list control in the **Services** tab, and then click **Close**.
8. In the **System Setting Change** dialog box, click **OK** to restart the system and finish the installation.

Note:

1. You must be logged on as an administrator or a member of the Administrators group in order to complete this procedure. If

your computer is connected to a network, network policy settings might also prevent you from completing this procedure.

2. SNMP starts automatically after installation.

1.4 Start or stop SNMP service in Windows 2000/XP/Server 2003

1. Click **Start**, point to **Settings**, and click **Control Panel**. Double-click **Administrative Tools** and then double-click **Computer Management**.
2. In the console tree, click **Services**.
3. In the details pane, click **SNMP Service**
4. On the **Action** menu, click **Start**, **Stop**, or **Restart**.

2 VIA SNMP extension agent operation

2.1 Install VIA SNMP extension agent in Windows 2000/XP/Server 2003

In Microsoft windows 2000, XP and Server 2003, VIA SNMP extension agent installation procedure is listed as the following:

1. Make sure you install **Windows SNMP Service** before install VIS SNMP extension agent.
2. In the folder contains VIA SNMP extension agent package, there are two version of setup program
3. A Self-Extracting EXE and the VSNMP-GE subfolder contains uncompressed setup program.
4. Double Click on the **Self-Extracting EXE** or the **setup.exe** in the VSNMP-GE subfolder to launch the setup program.
5. Following the instruction of the setup program, to finish the setup of **VIA SNMP extension agent**.

Note:

1. You must be logged on as an administrator or a member of the Administrators group in order to complete this procedure. If your computer is connected to a network, network policy settings might also prevent you from completing this procedure.
2. VIA SNMP extension agent starts automatically after installation.
3. The setup program will prompt your to remove previous installation and to update miniport driver of your network adaptor if needed before installation.

2.2 Install VIA SNMP extension agent in Windows 98

In Microsoft windows and 98, VIA SNMP extension agent installation procedure is listed as the following:

1. Make sure you install **Windows SNMP Service** before install VIS SNMP extension agent.
2. In the folder contains VIA SNMP extension agent package, there are two version of setup program
3. A Self-Extracting EXE and the VSNMP-GE subfolder contains uncompressed setup program.
4. Double Click on the **Self-Extracting EXE** or the **setup.exe** in the VSNMP-GE subfolder to launch the setup program.
5. Following the instruction of the setup program, to finish the setup of **VIA SNMP extension agent**.

Note:

1. VIA SNMP extension agent starts automatically after system restart.

2.3 Install VIA SNMP extension agent in Windows NT4

In Microsoft windows NT4, VIA SNMP extension agent installation procedure is listed as the following:

1. Make sure you install **Windows SNMP Service** before install VIS SNMP extension agent.
2. In the folder contains VIA SNMP extension agent package, there are two version of setup program
3. A Self-Extracting EXE and the VSNMP-GE subfolder contains uncompressed setup program.
4. Double Click on the **Self-Extracting EXE** or the **setup.exe** in the VSNMP-GE subfolder to launch the setup program.
5. Following the instruction of the setup program, to finish the setup of **VIA SNMP extension agent**.

Note:

1. VIA SNMP extension agent starts automatically after system restart.

2.4 Remove VIA SNMP extension agent in Windows platform

1. Click **Start**, point to **Settings**, and click **Control Panel**. Double-click **Add/Remove Programs.**
2. In the list of installed program, choose **VIA VSNMP-GE**.
3. Click Add/Remove button to remove VIA SNMP extension agent.

3 MIB-II and RMON counter support in VIA Networking Rhine-GE Family Gigabit Ethernet Adapter

3.1 MIB-II counters

Currently, VIA Networking Rhine-GE Family Gigabit Ethernet Adapter support most of the standard MIB-II counters. The table below lists the MIB-II interface group supported OIDs.

3.1.1 OID in Interface Group

	OID in Interface Group	Attribute	Description
1	ifNumber	Integer (32-bit), Read-Only	The number of network interfaces (regardless of their current status) present on this system.
2	IfIndex	Integer (32-bit), Read-Only	A unique value for each interface.
3	IfDescr	OCTET STRING, Read-Only	A textual string containing information about the interface.
4	IfType	Integer (32-bit), Read-Only	The type of interface.
5	ifMTU	Integer (32-bit), Read-Only	The size of largest datagram, which can be sent/received on the interface, specified in octets.
6	ifSpeed	Gague (32-bit), Read-Only	An estimate of the interface’s bandwidth in bits per second.
7	ifPhysAddress	OCTET STRING, Read-Only	The interface’s physical address.
8	ifAdminStatus	Integer (32-bit), Read-Write	The desired state of the interface.
9	ifOperstatus	Integer (32-bit), Read-Only	The current operational state of the interface.
10	ifLastChange	TimerTick, Read-Only	The value of sysUpTime at the time the interface entered its current operational state.
11	ifInOctets	Counter (32-bit), Read-Only	The total number of octets received on the interface.
12	ifInUcastPkts	Counter (32-bit), Read-Only	The total number of unicast packets delivered to a higher-layer protocol.
13	ifInNUcastPkts	Counter (32-bit), Read-Only	The total number of non-unicast packets delivered to a higher-layer protocol.
14	ifInDiscards	Counter (32-bit), Read-Only	The number of inbound packets, which were chosen to be discarded even though no error had been detected.
15	ifInErrors	Counter (32-bit), Read-Only	The number of inbound packets that contained errors.
16	ifInUnknowProtos	Counter (32-bit), Read-Only	The number of packets received through the interface, which were discarded because of an unknown or unsupported protocol.
17	ifOutOctets	Counter (32-bit),	The total number of octets transmitted out of the interface.

		Read-Only	
18	ifOutUcastPkts	Counter (32-bit), Read-Only	The total number of packets that higher-protocols requested be transmitted to an uncast address.
19	IfOutNUcastPkts	Counter (32-bit), Read-Only	The total number of packets that higher-protocols requested is transmitted to a non-uncast address.
20	IfOutDiscards	Counter (32-bit), Read-Only	The number of outbound packets, which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
21	IfOutErrors	Counter (32-bit), Read-Only	The number of outbound packets that could not be transmitted because of errors.
22	IfOutQLen	Gague (32-bit), Read-Only	The length of output packet queue.
23	IfSpecific	Object Identifier, Read-Only	A reference to MIB definitions specific to the particular media being used to realize the interface.

3.2 RMON counters

Currently, VIA Networking Rhine-GE Family Gigabit Ethernet Adapter support some of the standard RMON counters. The table below lists the RMON Ethernet Statistics, History, Alarm and Event group supported OIDs.

3.2.1 OID in Statistic Group

	OID in Statistics Group	Attribute	Description
1	etherStatsIndex	Integer (32-bit), Read-Only	The value of this object uniquely identifies this etherStats entry.
2	etherStatsDataSource	Object Identifier, Read-Write	This object identifies the source of the data that this etherStats entry is configured to analyze.
3	etherStatsDropEvents	Counter (32-bit), Read-Only	The total number of events in which packets were dropped by the probe due to lack of resources.
4	etherStatsOctets	Counter (32-bit), Read-Only	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
5	etherStatsPkts	Counter (32-bit), Read-Only	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
6	etherStatsBroadcastPkts	Counter (32-bit), Read-Only	The total number of good packets received that were directed to the broadcast address.
7	etherStatsMulticastPkts	Counter (32-bit), Read-Only	The total number of good packets received that were directed to a multicast address.
8	etherStatsCRCAlignErrors	Counter (32-bit), Read-Only	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
9	etherStatsUndersizePkts	Counter (32-bit), Read-Only	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) but were otherwise well formed.
10	etherStatsOversizePkts	Counter (32-bit),	The total number of packets received that were longer

		Read-Only	than 1518 octets (excluding framing bits, but including FCS octets) but were otherwise well formed.
11	etherStatsFragments	Counter (32-bit), Read-Only	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
12	etherStatsJabbers	Counter (32-bit), Read-Only	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
13	etherStatsCollisions	Counter (32-bit), Read-Only	The best estimate of the total number of collisions on this Ethernet segment.
14	etherStatsPkts64Octets	Counter (32-bit), Read-Only	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
15	etherStatsPkts65to127Octets	Counter (32-bit), Read-Only	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
16	etherStatsPkts128to255Octets	Counter (32-bit), Read-Only	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
17	etherStatsPkts256to511Octets	Counter (32-bit), Read-Only	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
18	etherStatsPkts512to1023Octets	Counter (32-bit), Read-Only	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
19	etherStatsPkts1024to1518Octets	Counter (32-bit), Read-Only	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
20	EtherStatsOwner	OCTET STRING, Read- Write	The entity that configured this entry and is therefore using the resources assigned to it.
21	EtherStatsStatus	Integer, Read-Write	The status of this etherStats entry. (The 4 possible values are listed below.) ● Valid (1) ● CreateRequest (2) ● UnderCreation (3) ● Invalid (4)

3.2.2 OID in History Group

	OID in History	Attribute	Description

	Group		
1	historyControlIndex	Integer (16-bit), Read-Only	An index that uniquely identifies an entry in the historyControl table
2	HistoryControlDataSource	Object Identifier, Read-Write	This object identifies the source of the data for which historical data was collected and placed in a media-specific table on behalf of this historyControlEntry.
3	HistoryControlBucketsRequested	Integer (16-bit), Read-Write	The requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this historyControlEntry.
4	HistoryControlBucketsGranted	Integer (16-bit), Read-Only	The number of discrete sampling intervals over which data shall be saved in the part of the media-specific table associated with this historyControlEntry.
5	HistoryControlInterval	Integer(1..3600), Read-Write	The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this historyControlEntry.
6	HistoryControlOwner	OCTET STRING, Read- Write	The entity that configured this entry and is therefore using the resources assigned to it.
7	HistoryControlStatus	Integer, Read-Write	The status of this ether historyControl Stats entry. (The 4 possible values are listed below.) ● Valid(1) ● createRequest(2) ● underCreation(3) ● invalid(4)
8	EtherHistoryIndex	Integer (16-bit), Read-Write	The history of which this entry is a part.
9	EtherHistorySampleIndex	Integer (32-bit), Read-Only	An index that uniquely identifies the particular sample this entry represents among all samples associated with the same historyControlEntry.
10	EtherHistoryIntervalStart	TimerTick, Read-Only	The value of sysUpTime at the start of the interval over which this sample was measured.
11	EtherHistoryDropEvents	Counter (32-bit), Read-Only	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval.
12	EtherHistoryOctets	Counter (32-bit), Read-Only	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
13	EtherHistoryPkts	Counter (32-bit), Read-Only	The number of packets (including bad packets) received during this sampling interval.
14	EtherHistoryBroadcastPkts	Counter (32-bit), Read-Only	The number of good packets received during this sampling interval that were directed to the broadcast address.
15	EtherHistoryMulticastPkts	Counter (32-bit), Read-Only	The number of good packets received during this sampling interval that were directed to a multicast address.
16	EtherHistoryCRCAlignErrors	Counter (32-bit), Read-Only	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

17	EtherHistoryUndersizePkts	Counter (32-bit), Read-Only	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) but were otherwise well formed.
18	EtherHistoryOversizePkts	Counter (32-bit), Read-Only	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
19	EtherHistoryFragments	Counter (32-bit), Read-Only	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
20	EtherHistoryJabbers	Counter (32-bit), Read-Only	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
21	EtherHistoryCollisions	Counter (32-bit), Read-Only	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.
22	EtherHistoryUtilization	Gague (0..10000), Read-Only	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

3.2.3 OID in Alarm Group

	OID in Alarm Group	Attribute	Description
1	alarmIndex	Integer (16-bit), Read-Only	An index that uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device.
2	alarmInterval	Integer, Read-Write	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
3	alarmVariable	Object Identifier, Read-Write	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Counter, Gauge, or TimeTicks) may be sampled.
4	alarmSampleType	Integer, Read-Write	The method of sampling the selected variable and calculating the value to be compared against the thresholds. .(The 2 possible value is listed below.) ● absoluteValue(1)____the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. ● deltaValue(2)____ the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.
5	alarmValue	Integer, Read-only	The value of the statistic during the last sampling period. This is the value that is compared with the rising and falling thresholds.
6	alarmStartupAlarm	Integer,	The alarm that may be sent when this entry is first set to

		Read-Write	valid. If the first sample after this entry becomes valid is greater than or equal to the risingThreshold and alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3), then a single rising alarm will be generated. If the first sample after this entry becomes valid is less than or equal to the fallingThreshold and alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3), then a single falling alarm will be generated.
7	alarmRisingThreshold	Integer, Read-Write	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. A single event will also be generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3). After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.
8	alarmFallingThreshold	Integer, Read-Write	A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated. A single event will also be generated if the first sample after this entry becomes valid is less than or equal to this threshold and the associated alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3). After a falling event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the alarmRisingThreshold.
9	alarmRisingEventIndex	Integer (16-bit), Read-Write	The index of the eventEntry that is used when a rising threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object.
10	alarmFallingEventIndex	Integer (16-bit), Read-Write	The index of the eventEntry that is used when a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object.
11	alarmOwner	OCTET STRING, Read-Write	The entity that configured this entry and is therefore using the resources assigned to it.
12	AlarmStatus	Integer, Read-Write	The status of this etherStats entry.(The 4 possible value is listed below.) ● valid(1) ● createRequest(2) ● underCreation(3) ● invalid(4)

3.2.4 OID in Event Group

	OID in Event Group	Attribute	Description

	eventTable		A list of events to be generated.
1	eventIndex	Integer (16-bit), Read-Only	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur.
2	eventDescription	OCTET STRING, Read- Write	A comment describing this event entry.
3	eventType	Integer, Read-Write	The type of notification that the probe will make about this event. (The 4 possible value is listed below.) ● none(1) ● log(2) ● snmp-trap(3) -- send an SNMP trap ● log-and-trap(4)
4	eventCommunity	OCTET STRING SIZE (0.. 127), Read-Write	If an SNMP trap is to be sent, it will be sent to the SNMP community specified by this octet string. This object shall be set to a string of length zero if it is intended that mechanism be used to specify the destination of the trap.
5	eventLastTimeSent	TimeTicks, Read- only	The value of sysUpTime at the time this event entry last generated an event. If this entry has not generated any events, this value will be zero.
6	eventOwner	OCTET STRING SIZE (0.. 127), Read-Write	The entity that configured this entry and is therefore using the resources assigned to it.
7	eventStatus	Integer, Read-Write	The status of this etherStats entry.(The 4 possible value is listed below.) ● valid(1) ● createRequest(2) ● underCreation(3) ● invalid(4)
	logTable		A list of events that have been logged.
1	logEventIndex	Integer (16-bit), Read-Only	The event entry that generated this log entry. The log identified by a particular value of this index is associated with the same eventEntry as identified by the same value of eventIndex.
2	logIndex	Counter (32-bit), Read-Only	An index that uniquely identifies an entry in the log table amongst those generated by the same eventEntries. These indexes are assigned beginning with 1 and increase by one with each new log entry.
3	logTime	TimeTicks, Read- only	The value of sysUpTime when this log entry was created.
4	logDescription	OCTET STRING SIZE (0..255), Read-Write	An implementation dependent description of the event that activated this log entry.