บทที่2
แนวคิดและทฤษฎีที่เกี่ยวข้อง

โปรแกรมแสดงสถานะเครือข่ายนี้ทำงานอยู่บนพื้นฐานของ Simple Network Management Protocol (SNMP) ซึ่งช่วยให้โปรแกรมสามารถติดต่อขอข้อมูลกับอุปกรณ์ต่างๆ ในระบบเครือข่ายได้ โดยข้อมูลเหล่านี้จะช่วยให้ทราบถึงสถานะของแต่ละอุปกรณ์ในระบบเครือข่ายได้

2.1 SNMP

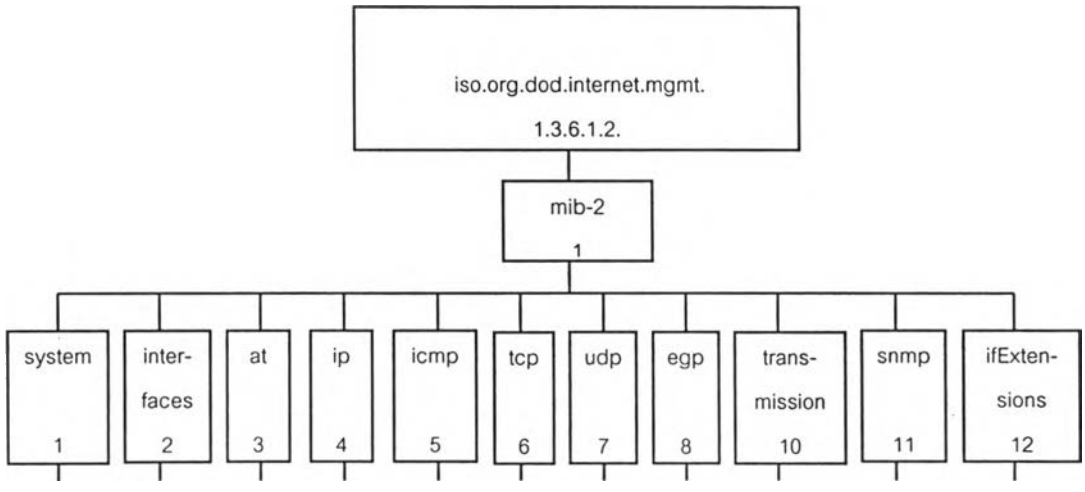
SNMP เป็นโพรโตคอล (protocol) ที่ถูกออกแบบมาให้ทำงานในชั้นของแอปพลิเคชัน (application) ซึ่งเป็นส่วนหนึ่งของระบบ Transmission Control Protocol/Internet Protocol (TCP/IP) โดยมีจุดมุ่งหมายให้ทำงานกับ User Data Protocol (UDP) เป็นหลักเนื่องจาก UDP มีขนาดเล็กและไม่ต้องการทรัพยากรมากเท่ากับ TCP ในการทำงานของ SNMP จะต้องประกอบด้วยส่วนต่างๆ ต่อไปนี้

- ตัวจัดการ
- ตัวแทน
- Management Information Base (MIB)

ตัวจัดการและตัวแทนโดยทั่วๆ ไปแล้วก็คือโปรแกรมที่ทำงานอยู่บนอุปกรณ์ต่างๆ ที่ทำงานอยู่ในระบบเครือข่าย โดยตัวแทนจะทำหน้าที่ส่งข้อมูลของอุปกรณ์ที่มันทำงานอยู่ให้แก่ตัวจัดการ ข้อมูลต่างๆ ของอุปกรณ์จะถูกเก็บรวบรวมในรูปของ MIB

2.2 MIB

International Organization for Standardization (ISO) และ International Telegraph and Telephone Consultative Committee (CCITT) ได้กำหนดโครงสร้างข้อมูลสารสนเทศขึ้นมาคือ ISO and CCITT Structure of Information และ MIB ก็เป็นส่วนหนึ่งโครงสร้างข้อมูลสารสนเทศนี้ดังรูปที่ 2.1

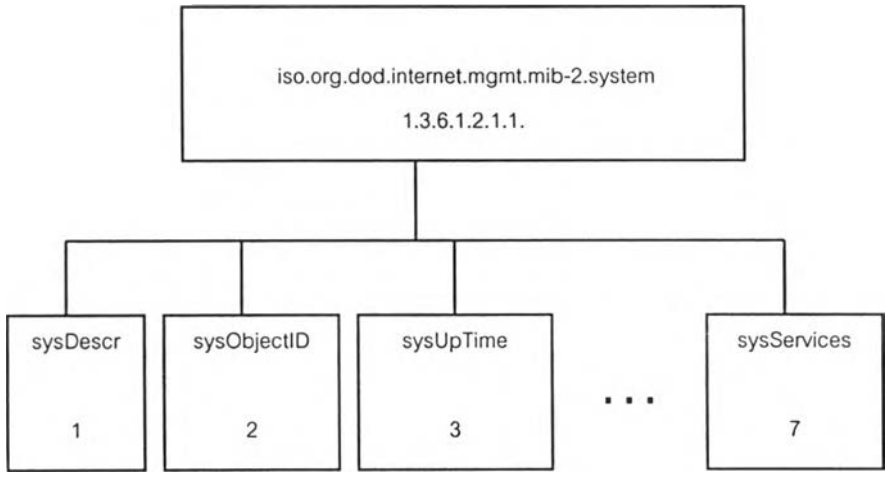


รูปที่ 2.1 โครงสร้างของ MIB-2

จากรูปที่ 2.1 แสดงให้เห็นถึงโครงสร้างของ MIB-2 ซึ่งมีการปรับปรุงจาก MIB ในบางส่วนเพื่อให้ครอบคลุมถึงข้อมูลที่เกิดขึ้นใหม่เช่น ATM, Host Management, Directory Services Managment และเทคโนโลยีใหม่อื่นๆ

ข้อมูลใน MIB แต่ละตัวจะมีหมายเลขประจำตัว เรียกว่า OBJECT IDENTIFIER หมายเลขประจำตัวนี้เป็นการระบุตำแหน่งของข้อมูลใน ISO and CCITT Structure of Information tree ประกอบด้วยตัวเลขและจุดทศนิยม โดยที่ตัวเลขซ้ายสุดจะเป็นหมายเลขรากของต้นไม้ (tree) จากนั้นก็เป็นหมายเลขของโหนด (node) ลูกไล่ลงมาจนถึงโหนดที่ต้องการโดยหมายเลขของแต่ละโหนดจะถูกแยกออกจากกันด้วยจุดทศนิยม เช่น OBJECT IDENTIFIER ของกลุ่มระบบ (system) จะเป็น 1.3.6.1.2.1.1

การเรียกดูข้อมูลจากตัวแทนจะเป็นการอ่านข้อมูลใน ISO and CCITT Structure of Information tree ของแต่ละอุปกรณ์ โดยข้อมูลเหล่านี้เป็นใบ (leaf) ของต้นไม้ทั้งสิ้น เช่น ภายใน iso.org.dod.internet.mgmt.mib-2.system มีโครงสร้างดังนี้



รูปที่ 2.2 โครงสร้างของ iso.org.dod.internet.mgmt.mib-2.system

หากต้องการเข้าถึงข้อมูล sysDescr ซึ่งเป็นข้อมูลที่ใบจะต้องอ้างไปที่ OBJECT IDENTIFIER หมายเลข 1.3.6.1.2.1.1.1.0 เป็นต้น

ทุกครั้งที่ต้องการเข้าถึงข้อมูลที่ใบต้องเติม .0 ตรงท้ายสุด แต่หากใบที่ต้องการอ้างถึงนั้นเป็นข้อมูลที่อยู่ในตาราง ต้องกำหนดว่าในข้อมูลประเภทนั้นต้องการเข้าถึงข้อมูลอันดับที่เท่าไร เช่น iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifType (1.3.6.1.2.1.2.2.1.3) เป็นข้อมูลชนิดของอินเตอร์เฟส (interface) หากต้องการเข้าถึงข้อมูลนี้ต้องกำหนดว่าอินเตอร์เฟสไหน เช่น อินเตอร์เฟสที่ 2 OBJECT IDENTIFIER คือหมายเลข 1.3.6.1.2.1.2.2.1.3.2

ภายใน MIB-2 มีการแบ่งข้อมูลเป็นกลุ่มเป็นดังนี้

2.2.1 กลุ่มระบบ (system)

แสดงรายละเอียดทั่วไปของอุปกรณ์นั้นได้แก่ ชนิดของฮาร์ดแวร์ (hardware), ระบบปฏิบัติการ, ระยะเวลาของระบบตั้งแต่เริ่มทำงาน โครงสร้างข้อมูลของกลุ่มระบบเป็นดังนี้

1.3.6.1.2.1.1 system

1 sysDescr

2 sysObjetID

3 sysUpTime

4 sysContact

5 sysName

6 sysLocation

7 sysServices

โดยที่ตัวเลขในแต่ละบรรทัดคือหมายเลข OBJECT IDENTIFIER ของข้อมูลแต่ละตัว เช่น ข้อมูลในกลุ่มนี้หมายเลข OBJECT IDENTIFIER จะต้องขึ้นต้นด้วย 1.3.6.1.2.1.1 ดังนั้นหมายเลข OBJECT IDENTIFIER ของ sysDescr จะเป็น 1.3.6.1.2.1.1.1.0

2.2.2 กลุ่มอินเตอร์เฟส (interface)

เป็นกลุ่มข้อมูลเกี่ยวกับฟิสิคอลแอดเดรส (physical interface) ของอุปกรณ์เกี่ยวกับการติดตั้งและข้อมูลที่แสดงถึงเหตุการณ์ต่างๆ ที่เกิดขึ้นกับแต่ละอินเตอร์เฟสข้อมูลเหล่านี้ได้แก่ จำนวนอินเตอร์เฟส, ชนิดของอินเตอร์เฟส, ความเร็ว, ฟิสิคอลแอดเดรส, ปริมาณข้อมูลที่ไหลเข้าออกในแต่ละอินเตอร์เฟสเป็นต้น

โครงสร้างของกลุ่มอินเตอร์เฟสเป็นดังนี้

1.3.6.1.2.1.2 interface

1 ifNumber

2 ifTable

1 ifEntry

1 ifIndex

2 ifDescr

3 ifType

4 ifMtu

5 ifSpeed

6 ifPhysAddress

7 ifAdminStatus

8 ifOperStatus

9 ifLastChange

10 ifInOctets

11 ifInUcastPkts

12 ifInNUcastPkts

13 ifInDiscards

14 ifInErrors

15 ifInUnknownProtos

16 ifOutOctets

17 ifOutUcastPkts

18 ifOutNUcastPkts

19 ifOutDiscards

20 ifOutErrors

21 ifOutQLen

22 ifSpecific

2.2.3 กลุ่ม Address Translation (AT)

ข้อมูลกลุ่มนี้เป็นข้อมูลที่เกี่ยวกับการทำ AT ในกลุ่มนี้ประกอบด้วยตาราง 1 ตาราง โดยในแต่ละแถวประกอบด้วยหมายเลขเครือข่าย (network address) และฟิสิคอลแอดเดรส (physical address) โดยทั่วๆ ไปหมายเลขเครือข่ายจะเป็นหมายเลข IP (IP address) ส่วนฟิสิคอลแอดเดรสนั้นขึ้นอยู่กับประเภทของเครื่อข่ายเช่น ถ้าเป็น Ethernet ก็จะใช้หมายเลข Ethernet (Ethernet address) เป็นฟิสิคอลแอดเดรสเป็นต้น

โครงสร้างของ AT เป็นดังนี้

1.3.6.1.2.1.3 at

1 atTable

1 atEntry

1 atIfIndex

2 atPhysAddress

3 atNetAddress

2.2.4 กลุ่ม Internet Protocol (IP)

ประกอบด้วยข้อมูลเกี่ยวกับ IP ของอุปกรณ์ซึ่งประกอบด้วยตาราง 3 ตารางคือ

- ipAddrTable เก็บหมายเลข IP ซึ่งแต่ละหมายเลข IP จะถูกกำหนดให้กับแต่ละอินเตอร์เฟสของอุปกรณ์
- ipRouteTable เก็บข้อมูลสำหรับการทำการเลือกเส้นทางในเครือข่ายอินเตอร์เน็ต (internet routing) ซึ่งข้อมูลเหล่านี้จะขึ้นอยู่กับโพรโตคอลที่ใช้ในการทำการเลือกเส้นทาง
- ipNetToMediaTable เป็นตารางที่จะใช้ในการแปลงหมายเลข IP ให้เป็นฟิสิคอลแอดเดรสโดยข้อมูลหมายเลข IP และฟิสิคอลแอดเดรสในตารางนี้จะเหมือนกับในตาราง atTable

โครงสร้างของ ip เป็นดังนี้

1.3.6.1.2.1.4 ip

1 ipForwarding

2 ipDefaultyTTL

3 ipInReceives

4 ipInHdrErrors

5 ipInAddrErrors

6 ipForwDatagrams

7 ipInUnknownProtos

8 ipInDiscards

9 ipInDelivers

10 ipOutRequests

11 ipOutDiscards

12 ipOutNoRoutes

13 ipReasmTimeout

14 ipReasmReqds

15 ipReasmOKs

16 ipReasmFails

17 FragOKs

18 ipFragFails

19 ipFragCreates

20 ipAddrTable

1 ipAddrEntry

1 ipAdEntAddr

2 ipAdEntIfIndex

3 ipAdEntNetMask

4 ipAdEntBcastAddr

5 ipAddEntReasmMaxSize

21 ipRouteTable

1 ipRouteEntry

1 ipRouteDest

2 ipRouteIfIndex

3 ipRouteMetric1

4 ipRouteMetric2

5 ipRouteMetric3

6 ipRouteMetric4

7 ipRouteNextHop

8 ipRouteType

9 ipRouteProto

10 ipRouteAge

11 ipRouteMask

12 ipRouteMetric5

13 ipRouteInfo

22 ipNetToMediaTable

1 ipNetToMediaEntry

1 ipNetToMediaIfIndex

2 ipNetToMediaPhysAddress

3 ipNetToMediaNetAddress

4 ipNetToMediaType

2.2.5 กลุ่ม Internet Control Message Protocol (ICMP)

เก็บข้อมูลเกี่ยวกับการทำงานของ ICMP โดยมีโครงสร้างดังนี้

1.3.6.1.2.1.5 icmp

1 icmpInMsgs

2 icmpInErrors

3 icmpInDestUnreachs

4 icmpInTimeExcds

5 icmpInParmProbs

6 icmpInSrcQuenchs

7 icmpInRedirects

8 icmpInEchos

9 icmpInEchoReps

10 icmpInTimestamps

11 icmpInTimestampReps

12 icmpInAddrMasks

13 icmpInAddrMaskReps

14 icmpOutMsgs

15 icmpOutErrors

16 icmpOutDestUnreachs

17 icmpOutTimeExcds

18 icmpOutParmProbs

19 icmpOutSrcQuenchs

20 icmpOutRedirects

21 icmpOutEchos

22 icmpOutEchoReps

23 icmpOutTimestamps

24 icmpOutTimestampReps

25 icmpOutAddrMasks

26 icmpOutAddrMaskReps

2.2.6 กลุ่ม Transmission Control Protocol (TCP)

เก็บข้อมูลเกี่ยวกับการทำงานของ TCP ของอุปกรณ์ ในกลุ่มนี้มีตารางอยู่ 1 ตารางคือ tcpConnTable ซึ่งจะเก็บข้อมูลการติดต่อของอุปกรณ์กับอุปกรณ์อื่นๆ โดยใช้โพรโตคอล TCP ที่เกิดขึ้นในขณะนั้น

1.3.6.1.2.1.6 tcp

1 tcpRtoAlgorithm

2 tcpRtoMin

3 tcpRtoMax

4 tcpMaxConn

5 tcpActiveOpens

6 tcpPassiveOpen

7 tcpAttempFails

8 tcpEstabResets

9 tcpCurrEstab

10 tcpInSegs

11 tcpOutSegs

12 tcpRetransSegs

13 tcpConnTable

1 tcpConnEntry

1 tcpConnState

2 tcpConnLocalAddress

3 tcpConnLocalPort

4 tcpConnRemAddress

5 tcpConnRemPort

14 tcpInErrs

15 tcpConnRemPort

2.2.7 กลุ่ม User Datagram Protocol (UDP)

เก็บข้อมูลเกี่ยวกับการทำงานของ UDP ในกลุ่มนี้มีตารางอยู่ 1 ตารางคือ udpTable ซึ่งจะเก็บข้อมูลของหมายเลข IP และพอร์ต UDP (UDP port) ซึ่งถูกใช้โดยโปรแกรมที่ทำงานบนอุปกรณ์และกำลังรอดาต้าแกรม UDP (UDP datagram) โปรแกรมนี้ถูกเรียกว่า listener

1.3.6.1.2.1.7 udp

1 udpInDatagrams

2 udpNoPorts

3 udpInErrors

4 udpOutDatagrams

5 udpTable

1 udpEntry

1 udpLocalAddress

2 udpLocalPort

2.2.8 กลุ่ม Exterior Gateway Protocol (EGP)

เก็บข้อมูลเกี่ยวกับการทำ EGP ของอุปกรณ์ในกลุ่มนี้มีตาราง 1 ตารางคือ egpNeighTable ข้อมูลในตารางนี้เป็นข้อมูลที่จำเป็นสำหรับการสื่อสารกับอุปกรณ์อื่นที่จะทำ EGP ด้วย

1.3.6.1.2.1.8 egp

1 egpInMsgs

2 egpInErrors

3 egpOutMsgs

4 egpOutErrors

5 epgNeighTable

1 egpNeighEntry

1 egpNeighState

2 egpNeighAddr

3 egpNeighAs

4 egpNeighInMsgs

5 egpNeighInErrs

6 egpNeighOutMsgs

7 egpNeighOutErrs

8 egpNeighInErrMsgs

9 egpNeighOutErrMsgs

10 egpNeighStateUps

11 egpNeighStateDowns

12 egpNeighIntervalHello

13 egpNeighIntervalPoll

14 egpNeighMode

15 egpNeighEventTrigger

6 egpNeighEventTrigger

2.2.11 กลุ่ม Simple Network Management Protocol (SNMP)

เก็บข้อมูลที่เกี่ยวกับการทำงานของ SNMP ต่างๆ มีโครงสร้างดังนี้

1.3.6.1.2.1.11 snmp

1 snmpInPkts

2 snmpOutPkts

3 snmpInBadVersions

4 snmpInBadCommunityNames

5 snmpInBadCommunityUses

6 snmpInASNParseErrs

8 snmpInTooBigs

9 snmpInNoSuchNames

10 snmpInBadValues

11 snmpInReadOnlys

12 snmpInGenErrs

13 snmpInTotalReqVars

14 snmpInTotalSetVars

15 snmpInGetRequests

16 snmpInGetNexts

17 snmpInSetRequests

18 snmpInGetResponses

19 snmpInTraps

20 snmpOutTooBigs

21 snmpOutNoSuchNames

22 snmpOutBadValues

24 snmpOutGenErrs

25 snmpOutGetRequests

26 snmpOutGetNexts

27 snmpOutSetRequests

28 snmpOutGetResponses

29 snmpOutTraps

30 snmpEnableAuthntraps

2.3 เม็สเสจ SNMP

เม็สเสจที่ใช้ใน SNMP ประกอบด้วย

- GetRequest เป็นเม็สเสจที่ตัวจัดการส่งไปให้ตัวแทนเพื่อบอกว่าตัวจัดการต้องการทราบข้อมูลอะไรจากตัวแทนซึ่งกำหนดโดย OBJECT INDENTIFIER ที่ส่งไปพร้อมกับเม็สเสจ
- GetNextRequest เม็สเสจชนิดนี้ต่างจาก GetRequest ตรงที่ข้อมูลที่ส่งกลับมาจากตัวแทนจะไม่ใช่ข้อมูลของ OBJECT IDENTIFIER ที่ตัวจัดการส่งไปแต่จะเป็นข้อมูลของ OBJECT IDENTIFIER ตัวถัดไปใน ISO and CCITT Structure of Information tree
- SetRequest เป็นเม็สเสจที่ตัวจัดการใช้บอกให้ตัวแทนเปลี่ยนแปลงข้อมูลต่างๆ ใน MIB ของอุปกรณ์นั้นๆ
- GetResponse เป็นเม็สเสจที่ตัวแทนใช้ในการส่งผลลัพธ์กลับมาให้ตัวจัดการจากการที่ตัวจัดการส่ง GetRequest, GetNextReques หรือ SetRequest
- Trap เป็นเม็สเสจที่ตัวแทนส่งให้ตัวจัดการเพื่อรายงานเหตุการณ์หรือปัญหา

เม็สเสจที่ใช้ใน SNMP นั้นมีรูปแบบดังนี้

Version	community	SNMP PDU

เม็สเสจ SNMP

PDU type	request-id	0	0	variable-bindings

GetRequest PDU, GetNextRequest PDU และ SetRequest PDU

PDU type	requeat-id	error-status	Error-index	variable-bindings

GetResponse PDU

PDU type	Enterprise	agent-addr	Generic-trap	Specific-trap	time-stamp	variable-bindings

Trap PDU

Name 1	Value 1	name 2	Value 2	...	name n	value n

Variable-binding

รูปที่ 2.3 รูปแบบของเม็สเสจ SNMP

จากรูปที่ 2.3 แสดงรูปแบบของ SNMP เม็สเสจ ซึ่งประกอบด้วย 3 ส่วนคือ

- รุ่น (version) ของ SNMP เป็นตัวระบุว่าเม็สเสจที่ส่งไปเป็นรุ่นอะไร สำหรับการพัฒนาโปรแกรมแสดงสถานะเครือข่ายจะเป็นรุ่น 1
- ระหัสผ่าน (community) ตัวแทนทุกตัวจะต้องมีระหัสผ่านอยู่ 2 ตัวคือระหัสผ่านสำหรับการอ่านข้อมูลซึ่งจะใช้ในเม็สเสจ GetRequest และ GetNextRequest โดยทั่วไปจะกำหนดให้เป็น "public" และ "private" สำหรับการเปลี่ยนแปลงค่าของ MIB ซึ่งจะใช้ใน GetRequest
- SNMP Protocol Data Unit (PDU) เป็นส่วนที่เก็บรายละเอียดของเม็สเสจที่ต้องการส่ง

ในแต่ละ PDU จะประกอบไปด้วยข้อมูลต่างๆ ดังนี้

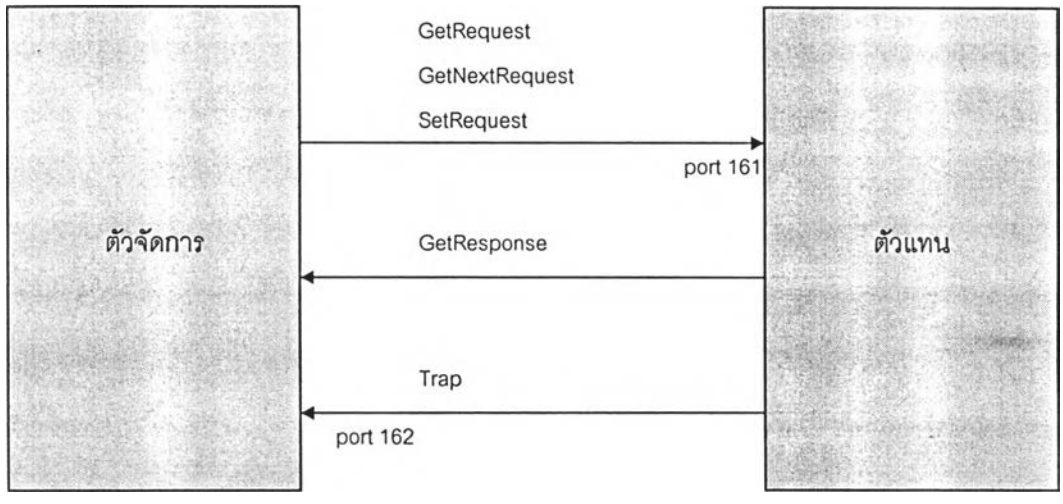
- ประเภทของ PDU (PDU type) เป็นข้อมูลที่บอกให้ทราบชนิดของ PDU ว่าเป็น GetRequest, GetNextRequest, SetRequest, GetResponse หรือ Trap
- หมายเลขเม็สเสจ (request-id) ส่วนตัวจัดการจะกำหนดหมายเลขให้กับแต่ละเม็สเสจที่ส่งไปให้ตัวแทนเมื่อตัวแทนส่งเม็สเสจกลับมา หมายเลขเม็สเสจนี้ก็จะถูกส่งกลับมาด้วย เพื่อเป็นการบอกว่าเม็สเสจที่ตัวแทนส่งมานั้นเป็นการตอบสนองกับเม็สเสจใดของตัวจัดการ
- error-status และ error-index ข้อมูลทั้งสองตัวนี้จะใช้ร่วมกันในการบอกสาเหตุของความผิดพลาดที่เกิดขึ้นในการติดต่อกับตัวแทน ดังแสดงในตารางที่ 2.1
- variable-bindings ประกอบด้วยรายชื่อของ OBJECT IDENTIFIER กับค่าของมันใน GetRequest PDU และ GetNextRequest PDU ค่าของ OBJECT IDENTIFIER จะกำหนดให้เป็น "null" เมื่อตัวแทนส่ง GetResponse กลับมาค่าของ OBJECT IDENTIFIER ก็จะเปลี่ยนเป็นข้อมูลของ OBJECT IDENTIFIER ที่อยู่ในอุปกรณ์ที่ตัวแทนทำงานอยู่
- Enterprise เป็นชนิดของอุปกรณ์ที่สร้าง Trap ขึ้นมา
- agent-addr เป็นที่อยู่ (address) ของอุปกรณ์ที่สร้าง Trap
- generic-trap แสดงประเภทของ Trap ได้แก่ coldStart(0), warmStart(1), linkDown(2), linkUp (3), authenticationFailure(4), egpNeighborLoss(5), enterpriseSpecific(6)
- specific-trap คือหมายเลขของ Trap ที่สร้างขึ้น
- time-stamp ช่วงเวลาตั้งแต่เริ่มต้นทำงานของอุปกรณ์จนถึงเวลาที่ Trap ถูกสร้างขึ้น

ข้อผิดพลาด	error-status	Error-index	รายละเอียด
NoError	0	0	ไม่มีข้อผิดพลาด
ToBig	1	0	ข้อมูลในเม็สเสจ GetResponse มีขนาดยาวเกินกว่าขนาดของเม็สเสจ
NoSuchName	2	ลำดับที่ของตัวแปร (variable) ในเม็สเสจที่ทำให้เกิดความผิดพลาด	ตัวแปรที่กำหนดไม่มีอยู่ใน MIB
BadValue	3	ลำดับที่ของตัวแปรในเม็สเสจที่ทำให้เกิดความผิดพลาด	SetRequest ให้ตัวแทนเปลี่ยนค่าที่ไม่เหมาะสมให้กับตัวแปร เช่น เปลี่ยนข้อมูลที่เป็นอักขระให้กับตัวแปรที่เป็นตัวเลข
ReadOnly	4	ลำดับที่ของตัวแปรในเม็สเสจที่ทำให้เกิดความผิดพลาด	SetRequest ให้ตัวแทนเปลี่ยนค่าของตัวแปรชนิดอ่านได้อย่างเดียว (read-only)
GenErr	5	ลำดับที่ของตัวแปรในเม็สเสจที่ทำให้เกิดความผิดพลาด	ไม่สามารถระบุประเภทของความผิดพลาดได้

ตารางที่ 2.1 แสดงค่าของ error-status และ error-index

จากตารางที่ 2.1 แสดงค่าของ error-index และ error-status ใน GetResponse PDU เช่น หากไม่มีข้อผิดพลาดเกิดขึ้นค่าของ error-index และ error-status จะเป็น 0

2.4 การรับส่งเม็สเสจใน SNMP



รูปที่ 2.4 แสดงการรับ-ส่งเม็สเสจระหว่างตัวจัดการกับตัวแทน

การทำงานของ SNMP ประกอบด้วย 2 ส่วน คือส่วนตัวจัดการและส่วนตัวแทน การทำงานของ SNMP จะเริ่มจากการที่ตัวจัดการส่งเม็สเสจไปให้กับตัวแทนซึ่งกำลังรอรับเม็สเสจที่พอร์ตหมายเลข 161 หากมีเม็สเสจ GetRequest, GetNextRequest หรือ SetRequest เข้ามาตัวแทนก็จะตอบสนองโดยการส่งเม็สเสจ GetResponse กลับไป