جامعة حماه
كلية العلوم التطبيقية
السنة الثالثة
ادارة الشبكات الحاسوبية

المهندسة مها جحا

المحاضرة الثانية والثالثة

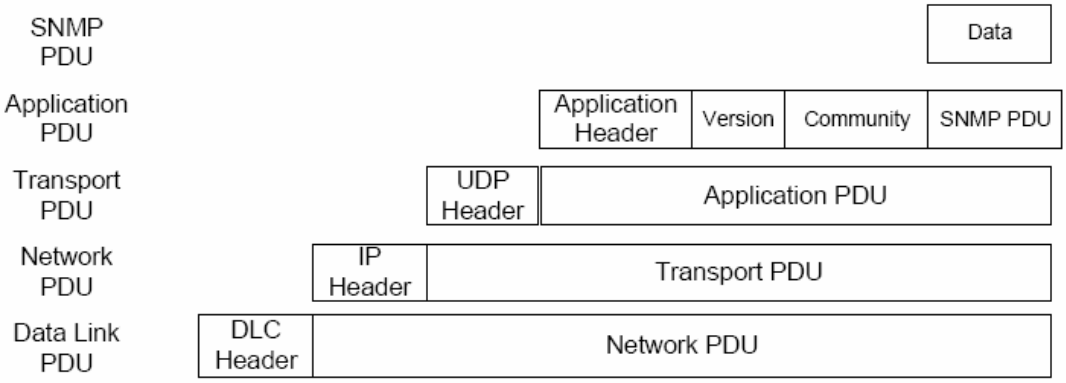
SNMPv1:
Communication and Functional Models

اعداد المهندسة : مها رضوان جحا

١ الموديل الاتصالاتي

الاتصال بين كينونات البروتوكول protocol entities ينجز بتغليف الرسائل في رزم معلومات تمرر عبر بروتوكول UDP. تتألف الرسائل في SNMP من معرف النسخة اسم ال community ، ووحدة معطيات البروتوكول(Protocol Data Unit (PDU الشكل ٤.١ يوضح رسالة SNMP مغلفة. رقم النسخة واسم الـ community تضاف إلى وحدة المعطيات ثم يضاف إليها ترويسة التطبيقات application header ثم تمرر

الرسالة كاملة إلى طبقة النقل لتشكل وحدة معطيات بروتوكول SNMP ، بروتوكول النقل المستخدم هو UDP فتضاف ترويسة UDP في طبقة النقل وأيضًا الرسالة الناتجة تشكل وحدة معطيات بروتوكول النقل Transport PDU وتمرر لطبقة الشبكة ثم يضاف IP header لوحدة معطيات النقل وينتج لدينا وحدة معطيات بروتوكول الشبكة Network PDU وتمرر لطبقة الربط Data Link Layer وتضاف ترويسة هذه الطبقة للرسالة قبل أن تتم عملية إرسال الإطار إلى وسط الفيزيائي.وفيما يلي الشكل ٤.١



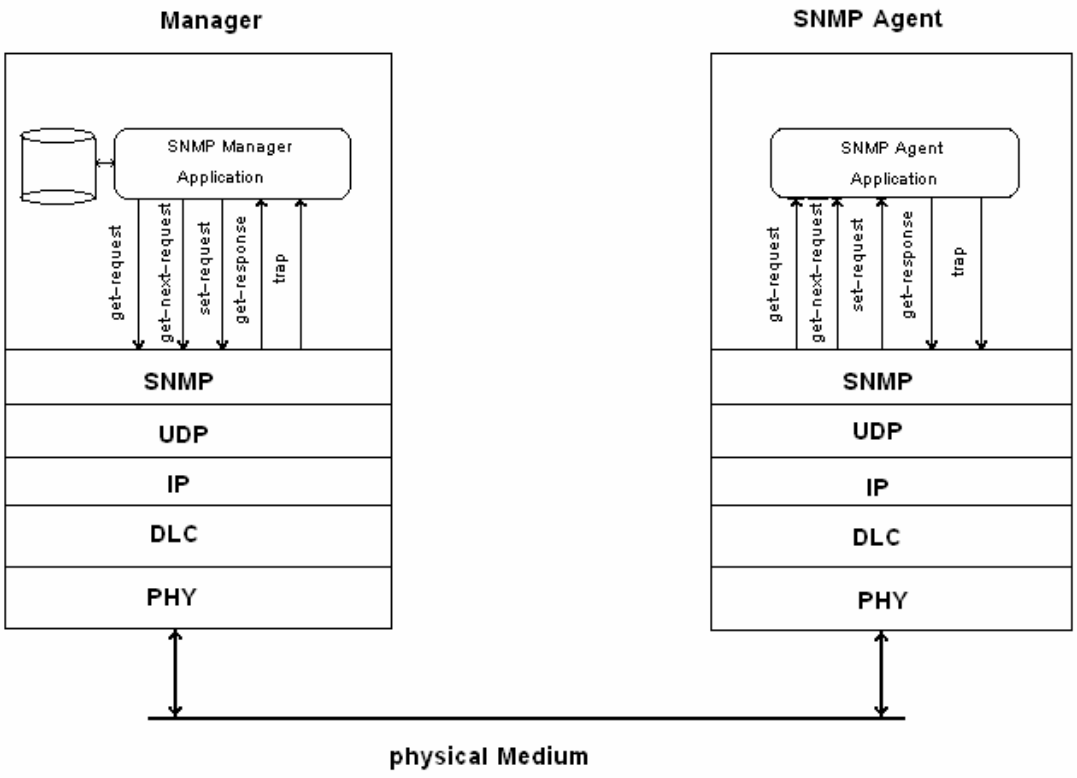
أما عن أسباب استخدام بروتوكول UDP في عملية التخاطب التي تتم بين محطة الإدارة والعميل:

١- في حالة استخدام SNMP في شبكة محلية فإن احتمال ضياع الرسالة ضئيل جداً

٢- بما أن رسائل SNMP تستخدم في عمليات تقصي Polling تكرر بأزمنة دورية صغيرة (لأنها تستخدم في مراقبة الشبكة) فإذا ضاع أحدها فإن الرسالة في عملية التقصي التالية سوف تدلنا على القيمة الضائعة.

٣- التقليل من الضغط على الشبكة.

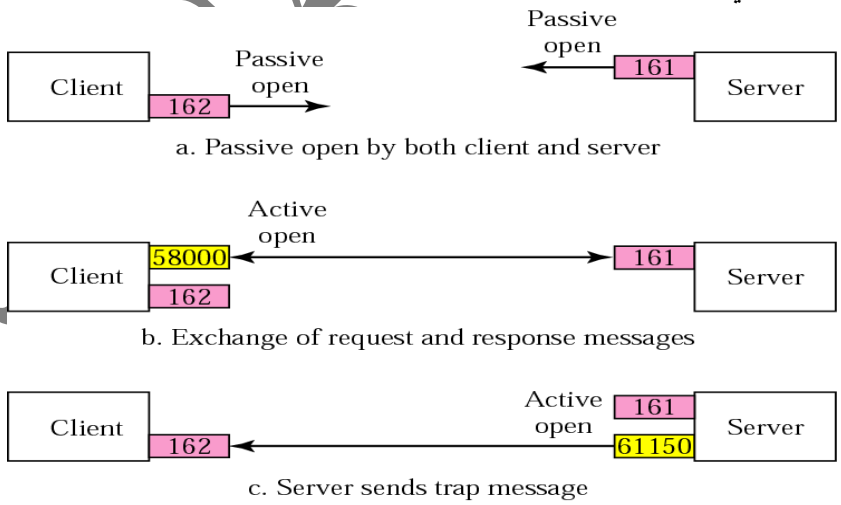
مها جحا



١.١ رسالة البروتوكول SNMP Message

تستقبل رسائل SNMP على المنفذ 161 port عند الوكيل

باستثناء رسائل Tarp التيُ تستقبل على المنفذ 162 port عند محطة إدارة الشبكة NMS



هنالك خمس أنواع من "وحدات معطيات البرتوكول" SNMP PDU يتم تضمينها جميعاً في رسالة موحدة تسمىSNMP Message لها نفس البنية وتتكون الرسالة من ثلاث حقول:

١. رقم نسخة SNMP : SNMP version حتى يعرف الطرف الأخر الذي تصله الرسالة مع أي نسخة من البروتوكول يتم التخاطب معه
٢. "اسم التجمع" أو Community Name لمعرفة إذا كانت PDU التي ضمن الرسالة تقوم بعملية (إما قراءة عن طريق GetRequest أو تغير لقيمة غرض إدارة طريق SetRequest
٣. وحدة معطيات البروتوكول SNMP PDU

ويبلغ الطول الأعظمي للـ SNMP PDU في 484 بايت في SNMP v1. من الضروري أن تكون "وحدات معطيات البروتوكول" (PDUs) الخمسة مدعومة من قبل جميع الإصدارات وهي :GetRequest-PDU، GetNextRequest-PDU، GetResponse-PDU، SetRequest-PDU و Trap-PDU

١.١.١ وحدات معطيات البروتوكول:

يتضمن فعلياً ستة أوامر أساسية PDU بأن الجزء الثاني من الرسالة وهو SNMPتكمن البساطة في بروتوكول وهي:

١. **Get**: تستخدمه محطة إدارة الشبكة للحصول على الأغراض المنشأة من عميل ما .
٢. **Get Next:** يستخدم للحصول على الغرض **التالي** اعتماداً على اسم غرض حالي، وذلك ضمن شجرة الأغراض الخاصة بوكيل ما.
٣. **Set:** لتغير قيمة غرض ما ضمن عميل ما.
٤. **Get-Response**: ويتم توليدها من قبل الوكيل/العميل، وتكون رداً على أحد الطلبات التالية: Get-Request , GetNext-Request , Set-Request , Get-Response
٥. **Trap**: مقاطعة برمجة تصدر من طرف العميل وترسل إلى محطة إدارة الشبكة لإعلامه بحدوث حدث ما في الشبكة. ولقد عرّف RFC1098 الأحداث التي تسبب هذه المقاطعات فيما يلي بعض أنوع Traps:

i. بينة وحدات المعطيات الأربعة الأولى: GetRequest، GetNextRequest، GetResponse ،SetRequest

العمليات الأساسية التي تقوم بها كينونة البروتوكول تتضمن الخطوات التالية: "كينونة البروتوكول" protocol entity المولّدة للرسالة تقوم ببناء الـPDU كنمط معطيات ASN.1 ثم تمرر هذه PDU مع اسم communityوعناوين النقل، العنوان المحلي وعنوان الهدف إلى قسم التوثيق authentication scheme الذي يعيد غرض ASN.1 جديد ليضاف إليه رقم النسخة واسم community وُترمز باستخدام BER قبل أن يتم إرسالها. العملية المقابلة تجري عند الم ستقبل : يتم فحص أخطاء الإرسال إن وجدت حيث يمكن أن يتولد Trap في حال فشل التوثيق authentication failure ، وفي حال الاستقبال الخالي من الأخطاء يتم توليد رسالة جواب(رد)على الرسالة المستقبلة إذا كانت الرسالة get أو set. الأغراض القابلة للإدارة managed objects تدعى متحولات variable يرتبط مع كل متحول قيمة، الثنائية المُشكلة من معرف الغرض مع القيمة يدعى varbind وكل وحدة معطيات PDU تحوي varbind وللسهولة وزيادة الفاعلية يمكن لل PDU أن تحوي قائمة

المهندسة مها جحا

من المتحولات List of varbinds ترسل في رسالة واحدة. بنية ASN.1 التي توصف رسائل set، get موضحة في الشكل 4.4, 4.3

```
--request/response information
requested ::=
INTEGER
ErrorStatus ::=
            INTEGER {
                  noError(0)
                  tooBig(1)
                  noSuchName(2)
                  badValue(3)
                  readOnly(4)
                  genErr(5)
            }
ErrorIndex ::=
            INTEGER
--variable bindings
VarBind ::=
            SEQUENCE {
                  name ObjectName
                  value ObjectSyntax
            }
VarBindList ::=
            SEQUENCE OF VarBind
```

الشكل4.3

PDU Type	RequestID	Error Status	Error Index	VarBind 1 name	VarBind 1 value	...	VarBind n name	VarBind n value

الشكل4.4

نمط الـ PDU للرسائل الأربع التالية معرف في RFC 1157 كنمط Tagged مشتق من نمط PDU مشترك مع تغير الرقم المعرف لنمط الرسالة (أي الوسمة Tag) حيث أن لهذه الرسائل البنية نفسها وتختلف فقط بالرقم المعرف (الـ Tag) لنوع الرسالة حتى يستطيع الوكيل أو المدير تميز معنى الرسالة:

```
GetRequest-PDU ::=
    [0] IMPLICIT PDU

GetNextRequest-PDU ::=
    [1] IMPLICIT PDU

GetResponse-PDU ::=
    [2] IMPLICIT PDU

SetRequest-PDU ::=
    [3] IMPLICIT PDU
```

المهندسة جحا

في الشكل 4.4 الحقول التالية:

- **PDU-Type** رقم معرف لنوع الرسالة، ويأخذ قيمة واحدة من القيم الأربعة التالية:

Get-request-PDU=a0hex

GetNext-request-PDU=a1x

Set-request-PDU =a2x

Get-response-PDU=a3x

- **Request ID**: رقم تسلسلي يعطى للطلبات ويستخدم بهدف معرفة الجواب القادم لأي طلب، فمثلاً عندما يأتي جواب برقم ١٠ فيكون هو جواب للطلب رقم ١٠، ويفيد في تعقب الرسائل، كما يقدم أداة بسيطة لمعالجة عدم الوثوقية في حال استخدام بروتوكول النقل UDP وحالة تكرار الرسالةDuplicated message

- **Error Status**: عدد الأخطاء ونوع الخطأ، تكون قيمة هذا الحقل صفر عادةً إلا في حالة كان الأمر هو Response تعدل قيمة هذا الحقل حيث يمكن أن تأخذ إحدى هذه القيم

Status	*Name*	*Meaning*
0	noError	No error
1	tooBig	Response too big to fit in one message
2	noSuchName	Variable does not exist
3	badValue	The value to be stored is invalid
4	readOnly	The value cannot be modified
5	genErr	Other errors

١) noError: في حالة عدم وجود خطأ.

٢) tooBig: في حال كان حجم رسالة الرد (مع القيم) كبيرة أكبر من الحجم الأعظمي لرسالة البروتوكول.

٣) noSuchName: في حالة السؤال أو طلب تغير غرض غير موجود.

٤) badValue : في حالة إسناد قيمة إلى متحول مع اختلاف أنماط المعطيات (في حالة رسالة SetRequest)

مثال: إسناد قيمة integer إلى متحول من نمط string.

المهندسة جحا

٥) Readonly: وهو الخطأ الناتج عن محاولة إعطاء قيمة لغرض ما، وهو للقراءة فقط،(في حالة رسالةSetRequest)

٦) genErr: وهو أي خطأ غير الأخطاء السابقة.

- **Error Index**: رقم يدل على مكان الخطأ في سلسلة معرفات الأغراض التي تم السؤال عنها في قائمة VarBindList، ويأخذ أحد القيمتين التاليتين:

١) Null: وهي حالة الحقل لا يلزم مثلاً في رسالة Get-Request.

٢) رقم : يمثل مكان الخطأ في سلسة المتحولات (VarBind List).

- **Variable bindings**: وهي عبارة عن أزواج من الحقول يتألف كل زوج من قسمين هما:

١) VarBind Name: يمثل معرف الغرض (Object OID) الذي تريد قراءة قيمته أو تغير قيمته.

٢) VarBind Value: القيمة التي يود المدير إسنادها لهذا الغرض، في حالة رسالة Get يأخذ القيمة NULL

وبما أنه يوجد سلسلة من الـ VarBind فإنه بإمكاننا إسناد قيم أو جلب مجموعة من الأغراض في رسالة واحدة.

ii. رسالة TRAP

الشكل 4.5 يوضح بنية رزمة المعلومات الخاصة ب Trap وتحوي n متحول (varbind) والجدول4.1 يوضح أنواع رسائل Trap العامة.

PDU Type	Enterprise	Agent Address	Generic Trap Type	Specific Trap Type	Timestamp	VarBind 1 name	VarBind 1 value	...	VarBind n name	VarBind n value

الشكل 4.5 generic Traps

وحقول هذه الرسالة هي:

- **PDU Type**: يأخذ القيمة Trap-PDU.

- **Enterprise** : يحدد Enterprise OID للعميل الذي أصدر الـ Trap، وبذلك نعرف إلى مُصنِّع يتبع الجهاز الذي أصدر الإنذار

- **Agent Address**: أي عنوان IP address للعميل الذي أصدر الـ Trap، ولذلك كي يعرف مستقبل الرسالة من أرسل الإنذار.

- **Generic Trap Type**: يأخذ أحد القيم التالية:

  - ColdStart:

    وهي قيام العميل Agent بتهئية نفسه أو إعادة تهيئة نفسه، مع تغير في إعدادات الوكيل agent configuration

  - Warm Start:

    وهي قيام العميل بإعادة تهيئة نفسه، مع عدم تغير في إعدادات الوكيل

  - Link Down:

    تتعلق بإرسال إنذار بالواجهة (دليل الواجهة ifIndex) التي تغيرت حالتها، من تشغيل إلى إطفاء.

  - LinkUp

    تتعلق بإرسال إنذار بالواجهة التي تغيرت حالتها، من إطفاء إلى تشغيل.

  - Authentication Failure:

    استخدم community خاطئة غير مشتركة بين الطرفين.

- **Specific Trap Type**: وهو يحدد أي Trap غير موجود في Generic Trap Type.

- **Time Stamp**: وهو زمن آخر عملية Reinitialization للغرض (الزمن مقدراً بـ ١٠٠ ميلي ثانية منذ تشغيل الوكيل)

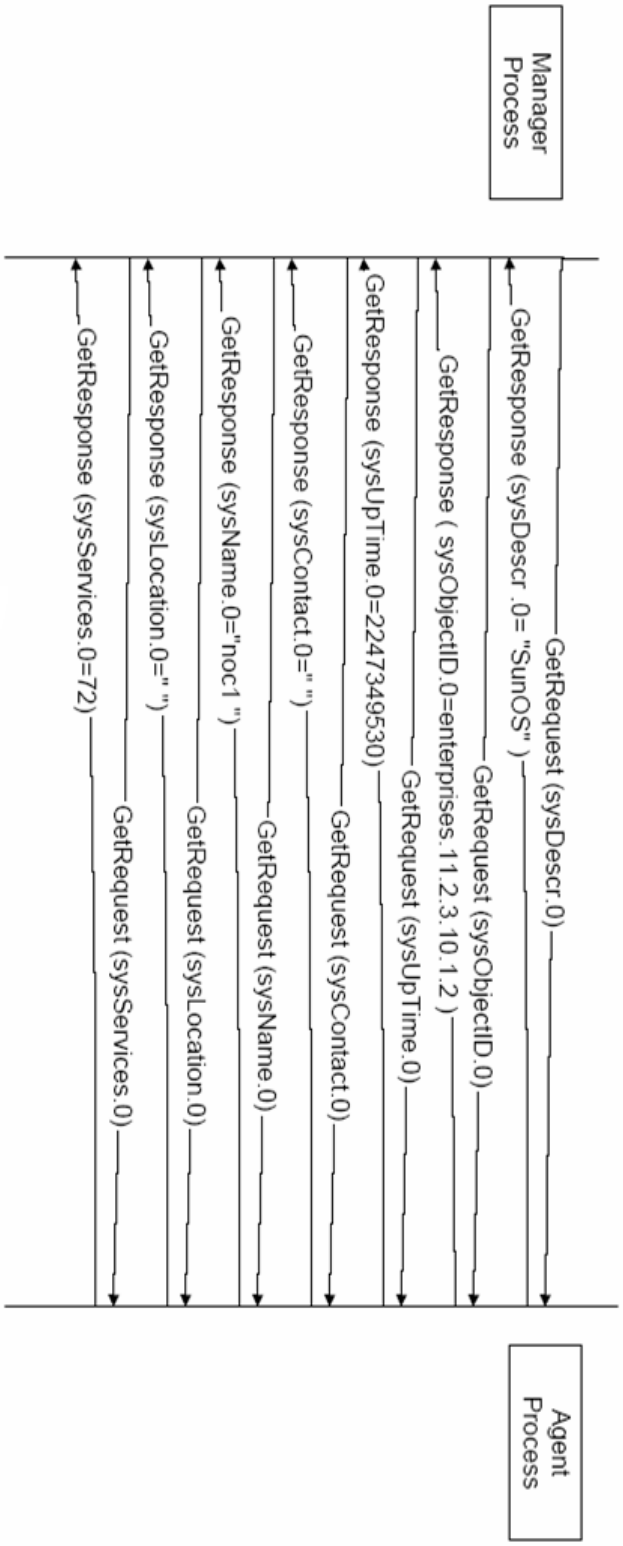
المهندسة مها جحا

Generic Trap Type	Description (brief)
coldStart(0)	Sending protocol entity is reinitializing itself; agent's configuration or protocol entity implementation may be altered
warmStart(1)	Sending protocol entity is reinitializing itself; agent configuration or protocol entity implementation not altered
linkDown(2)	Failure of one of the communication links
linkUp(3)	One of the links has come up
authenticationFailure(4)	Authentication failure
egpNeighborLoss(5)	Loss of EGP neighbor
enterpriseSpecific(6)	Enterprise-specific trap

١.٢ Operations

عمليات SNMP تضم رسائل get وset من المدير إلى العميل ورسائل get وtrap من موجهة العميل إلى المدير. عملية العمليات هذه بدراسة الآن وسنقوم :بالتفصيل GetRequest-PDU الشكل 4.6 يوضح العمليات تتالي
GetRequest بتعليمة العمليات هذه تبدأ system group النظام. مجموعة في الموجودة الأغراض قيم طلب في عملية وتليها العميل إلى المدير من ترسل التي GetRequest-PDU المعطيات البروتوكول وحدة باستخدام GetResponse-PDU بالجواب الخاصة المعطيات وحدة للطلب ويتضمن جواب وهي GetResponse ا من المرسلة والرسائل الشكل، من اليمنى على الجهة العميل عند وتنتهي اليسرى الجهة من تبدأ المدير من الرسائل 4.6 المقابل.وفيما يلي الشكل بالطرف في الشكل وتنتهي من اليميني الجانب في تبدأ لعميل

المهندسة مها جحا



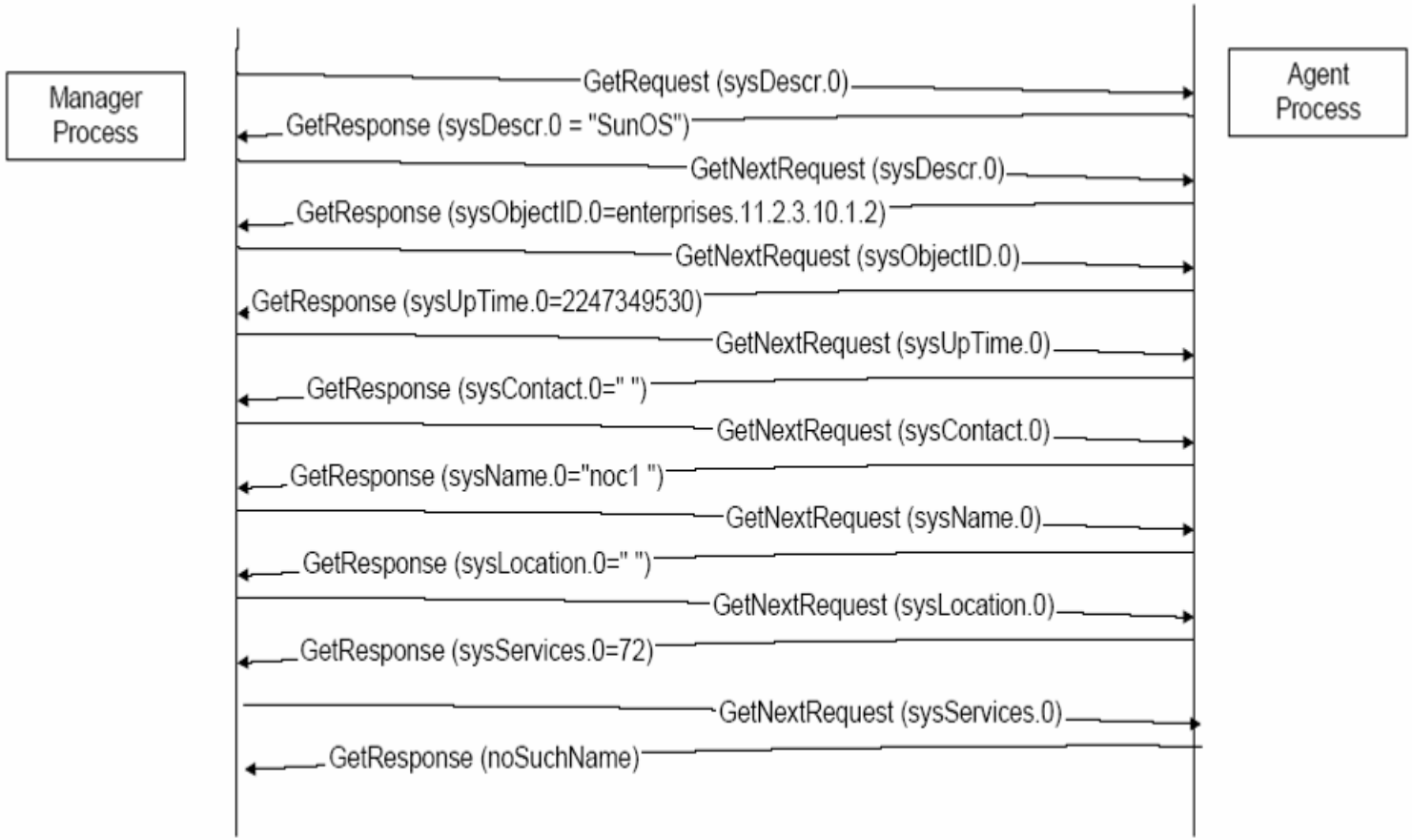
الأغراض قيم تمثل الرسائل الموضحة الشكل. في الأسفل نحو اتجهنا كلما الزمن تقدم مع العمليات تتالي يتقدم بتعليمة 4.6الشكل في العمليات سلسلة المدير يبدأsystem group النظام. مجموعة في الموجودة السبعة Sun" بقيمة GetResponse-PDUالعميل. يعيدsysDescrقيمة الغرض لجلبGetRequest-PDU

القيمة ويستقبلsysObjectIDالغرض أجل من الطلب المدير بإرسال يقوم ثم"OS بالغرض الخاصة72 القيمة المدير يستقبل حتى الطلب والرد عمليات وتستمر"enterprise.11.2.3.10.1.2" أنه إلا زمني كتسلسل الرسائل يوضح الشكل أن من الرغم علىsysServices وهي. النظام مجموعة في الأخير في والموضحةvarbind listالمتحولات قائمة باستخدام وذلك واحدة برسالة القيم على جميع الحصول الممكن من 4.5الشكل

GetNextRequest-PDU

القيمة هي هذه التعليمة في المطلوبة القيمة أن باستثناء السابقةGetRequestلتعليمة جدًا مشابهة التعليمة هذه تسلسل4.7الشكل يوضح الطلب. في رسالةObject Identifierالمحدد الغرض يلي الذي بالغرض الخاصة تعليمة. باستخدام النظام مدير قبل منsystem groupالنظام مجموعة من المعلومات طلب عند العمليات sysDescrللغرض موجهةGetRequest-PDUهي الأولى يظهر بالشكل،الرسالة وكماGetNextRequest GetNextRequest-PDUرسالة بإصدار المدير يقوم ثم" sun OS " بالقيمة. الطلب هذا على ويكون الجواب اسم بإيجاد العميل يقوم الرسالة. لهذه كوسيطsysDescrبالغرض الخاصOIDالغرض محدد على تحوي وقيمته sysObjectIDالغرض أنه فيجد الطلب في رسالة المحدد الغرض تمامًا يلي الذي الغرض GetNextRequest-PDUللرسالة كوسيط يستخدمه الذي للمدير ويعيده"enterprise. 11.2.3.10.1.2" الحالة لايجد هذه وفيsysServicesالغرض هو وسيط تحوي التي الطلب رسالة إلى نصل حتى...ا وهكذا التالية الخطأ. رسالة ضمن"no such name"القيمة فيعيدMIBال شجرة في الغرض هذا يلي غرض أي العميل

المهندسة مها جحا


Manager Process
Agent Process
GetRequest (sysDescr.0)
GetResponse (sysDescr.0 = "SunOS")
GetNextRequest (sysDescr.0)
GetResponse (sysObjectID.0=enterprises.11.2.3.10.1.2)
GetNextRequest (sysObjectID.0)
GetResponse (sysUpTime.0=2247349530)
GetNextRequest (sysUpTime.0)
GetResponse (sysContact.0=" ")
GetNextRequest (sysContact.0)
GetResponse (sysName.0="noc1 ")
GetNextRequest (sysName.0)
GetResponse (sysLocation.0=" ")
GetNextRequest (sysLocation.0)
GetResponse (sysServices.0=72)
GetNextRequest (sysServices.0)
GetResponse (noSuchName)

٢ مثال عملي

٢.١ تنصيب وإعداد المدير والوكيل

يجب أن نقوم الأتيsystemلإدارة جهاز والحصول على قيم أغراض الإدارة في عقدة

١. تنصيب برنامج إدارة مثل MG-Soft browser على الجهاز المراد ليصبح بذلك NMS: Network Management Station
٢. تنصيب خدمة SNMP على الجهاز المراد إدارته، أي تنصيب الوكيل Agent
٣. القيام بإعداد خدمة SNMP على الأجهزة المراد إدارتها
   a. تعريف Community Names التي يحق لها التخاطب مع هذا الوكيل (استخدم public بحقوق readOnly و private بحقوق read/write حيث أن هذه communities معرفة مسبقاً by default في برنامج المدير mg-soft browser ويمكن تغيرها).
   b. تعريف مجموعة محددة من IP للمدراء الذين يحق له إدارة هذا الوكيل
   c. تعريف Community Names التي سوف توضع في رسائل الـ TRAP
   d. تعريف مجموعة محددة من IP للمدراء الذين سوف يرسل إليهم رسائل TRAP
٤. التأكد أن هنالك اتصال منطقي logical connection بين الجهازين عن طريق القيم بـ ping من المدير إلى الوكيل، في حال حدوث:
   a. TimeOut: قد يكون السبب هو
      i. الوصلة الفيزيائية لأحد الجهازين مقطوعة
      ii. وجود جدار ناري (مثل Windows Firewall) يمنع وصول الطرد من نوع بروتوكول ICMP
      iii. وجود مضاد فيروسات معه جدار ناري
      iv. عدم إعداد الجهاز كجزء من شبكة محلية
   b. Destination Unreachable: أي لا يوجد طريق بين الجهازين، أي أن كل منها في شبكة subnet ولا يوجد موجه بينهما، وبالتالي يجب إضافة موجه يقوم بتوجيه الرسائل بين الجهازين.
٥. شغل برنامج لاقط الباكتات Wireshark وابدأ بالتقاط الباكتات (capture→interface→start)

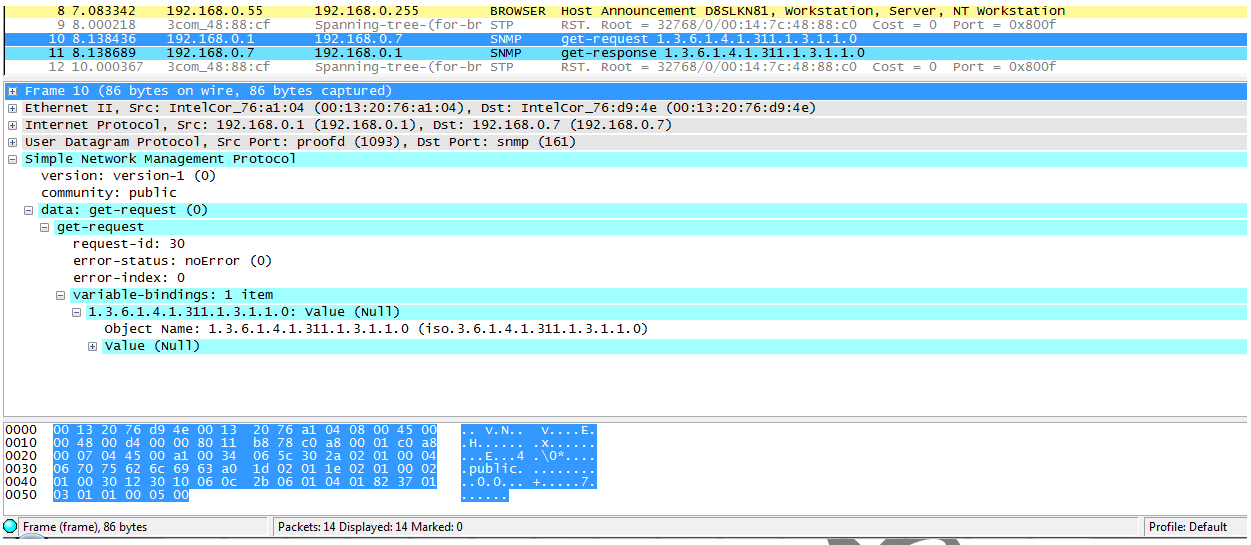
٢.٢ توليد رسائل SNMP المختلفة

للقيام بـ:MG-Soft browserاستخدم برنامج

٢.٢.١ توليد رسالة get

شغل برنامج الإدارة، ضع عنوان IP للجهاز المراد إدارته وقم بعمل Contact معه يجب أن تحصل على قيمة sysUptime (فعلياً عملية contact تقوم بعمل get sysUptime)

وقم بعملية get للغرض ، sysDescription يجب أن تستطيع تلقط رسالة get ورسالة get-response



٢.٢.٢ توليد رسالة get-Next

، sysDescription لغرض getNext قم بعمل

٢.٢.٣ توليد رسالة set

(اسم المسؤول للاتصال به sysContact (مكان الجهاز الذي يحوي العميل) و sysLocation لغرض setقم بعمل في حال اكتشاف حدوث عطل في الجهاز)،

٢.٢.٤ توليد رسالة trap

يمكن أن تلقطها عند جهاز العميل الذي سيولدها أو عند جهاز المدير الموضوع TRAPلاحظ أن جميع رسائل الـ فقط.TRAP للمدراء الذين سيرسل لهم الوكيل رسائل الـ ip addressعنوانه في قائمة

١) توليد warmstart

عند الوكيلsnmp وقم بإعادة تشغيل خدمة servicesاذهب إلى قائمة

٢) توليد coldstart

عند الوكيلsnmp وقم بإعادة تشغيل خدمة servicesاذهب إلى قائمة

٣) توليد linkdown

قم بفصل كبل الشبكة عن الشبكة عن الجهاز

٤) توليد linkup

قم بوصل كبل الشبكة عن الشبكة عن الجهاز

٥) توليد authenticationfailure

غير معرف عند العميل.community name لغرض إدارة باستخدام getقم بعمل

٢.٢.٥ توليد رسالة get-response مع أخطاء