الفصل الثامن
Chapter 8

سرية إدارة الشبكات
Network Management Security

المقرر:

1.8 المفاهيم الأساسية لبروتوكول إدارة الشبكات البسيط 8.1 Basic concepts of SNMP

معمارية إدارة الشبكات Network Management Architecture
معمارية بروتوكول إدارة الشبكات Network Management Protocol Architecture
البروكسيز Proxies
الإصدار الثاني من بروتوكول إدارة الشبكات البسيط SNMPv2

2.8 تسهيل مجتمع الإصدار الأول من بروتوكول إدارة الشبكات البسيط 8.2 SNMPv1 Community Facility

المجتمعات و أسماء المجتمع Communities and Community Names
خدمات التوثق Authentication Services
خدمات البروكسي Proxy Services

1.8 المفاهيم الأساسية لبروتوكول إدارة الشبكات البسيط 8.1 Basic concepts of SNMP

معمارية إدارة الشبكات Network Management Architecture

إن نظام إدارة الشبكة(Network Management System) هو عبارة عن مجموعة من الأدوات تقوم بعمليات المراقبة و التحكم بالشبكة، و هي متكاملة من النواحي التالية:

- للقيام بمعظم أو كل مهام إدارة الشبكة يوجد هناك واجهة تشغيل واحدة (Single operator interface) حيث تحتوي على مجموعة من الأوامر القوية و السهلة الاستخدام.
- يوجد كمية قليلة من المعدات المنفصلة (Minimal amount of separate equipment) ، بمعنى أن الهاردوير و السوفت وير التي تتطلبها إدارة الشبكة تكون مشتركة في جهاز مستخدم موجود.

العناصر الرئيسية في بروتوكول إدارة الشبكات البسيط (SNMP key elements)

- محطة الإدارة (Management station).
- وكيل الإدارة (Management agent).
- قاعدة المعلومات الإدارية (Management information base).
- بروتوكول إدارة الشبكة (Network Management protocol).

العنصر الأول : محطة الإدارة (Management station):

و هي عبارة عن جهاز قائم بذاته ، و لكنه قد يكون عبارة عن مقدرة منفذة في نظام مشترك. و في كلا الحالتين ، فإن الـ (Management Station) تعمل كواجهة لمدير الشبكة (الشخص البشري الذي يديرها).
و في الحدود الدنيا ، يجب على الـ (Management Station) أن تتضمن الآتي:

- مجموعة من التطبيقات الإدارية التي تهتم بتحليل البيانات (Data analysis) و الاسترجاع من الأخطاء (Fault recovery) و ما إلى ذلك ..
- واجهة (Interface) يمكن لمدير الشبكة من خلالها أن يراقب و يتحكم بالشبكة.
- المقدرة على ترجمة متطلبات مدير الشبكة إلى مراقبة و تحكم حقيقي بالعناصر البعيدة في الشبكة.
- قاعدة بيانات للمعلومات التي يتم استخلاصها من قواعد المعلومات الإدارية لكل الكينونات التي يتم إدارتها بواسطة هذه الشبكة.

العنصر الثاني: وكيل الإدارة (Managament agent):

- و هو عبارة عن مجموعة من الـ (Platforms) الأساسية . مثل ، المضيفات (hosts) و الجسور (bridges) و المسيرات (routers) و الـ (hubs) . و هذه كلها يمكن أن تعد مع برتوكول الـ (SNMP) بحيث يمكن إدارتها من الـ (Management Station).
- يستجيب الـ (Management agent) لطلبات المعلومات (information requests) و طلبات الأحداث (action requests) القادمة من الـ (Management Station).

العنصر الثالث : قاعدة إدارة المعلومات (Management Information Base) :

- لإدارة موارد الشبكة، يتم تمثيل كل مورد من هذه الموارد كـ (object). وهذا الـ (object) في الأساس هو عبارة عن متغير بياني يمثل أحد مجالات الـ (managed agent).
- مجموعة الـ (objects) التي تمثل موارد الشبكة ككل نطلق عليها: قاعدة إدارة المعلومات (Management Information Base) و اختصاراً نقول (MIB).
- تعمل الـ (MIB) كمجموعة من نقاط الوصول إلى الـ (Management Station) عند الـ (agent).
- تقوم الـ (Management Station) بعمليات المراقبة عن طريق استرجاع قيمة الـ (MIB objects). و بإمكان الـ (Management Station) أن تسبب في حدوث (action) معين عند الـ (agent) أو تغير إعدادات الـ (agent) عن طريق تعديل قيم (objects) مخصصة.

العنصر الرابع : بروتوكول إدارة الشبكة (Network Management protocol):

- و هو البروتوكول الذي يتم من خلاله ربط الـ (Management Station) مع الـ (agent).
- و البروتوكول المستخدم لإدارة شبكات الـ (TCP/IP) يعرف ببروتوكول إدارة الشبكة البسيط (SNMP).

القدرات الأساسية لبروتوكول الـ (SNMP):

- خاصية الـ (Get) : و هي تمكن الـ (Management Station) من استرجاع قيم الـ (objects) الموجودة عند الـ (agent).
- خاصية الـ (Set) : و هي تمكن الـ (Management Station) من ضبط قيم الـ (objects) الموجودة عند الـ (agent).
- خاصية الـ (Notify) : و هي تمكن الـ (agent) من تنبيه الـ (Management Station) بالأحداث المهمة.

معمارية بروتوكول إدارة الشبكات (Network Management Protocol Architecture):

كما هو واضح من الاسم، فإن بروتوكول الـ (SNMP) هو عبارة عن أداة بسيطة لإدارة الشبكة. و هو يعرف (MIB) محدودة و سهلة التنفيذ للمتغيرات المعيارية و كذلك جداول ذات بعد ثنائي. و أيضاً يعرف بروتوكولاً لتمكين الـ (manger) من عمل (get) أو (set) لمتغيرات الـ (MIB) و تمكين الـ (agent) من إصدار تنبيهات غير مستحثة (unsolicited notifications) و يطلق عليها (traps).

قوة بروتوكول الـ (SNMP):

- يعد هذا البروتوكول من البروتوكولات سهلة التنفيذ.
- يستهلك موارد شبكية و معالجة متواضعة.
- بنية هذا البروتوكول و كذلك بنية الـ (MIB) سهلة بما فيه الكفاية لدعم ميزة المعالجة الداخلية (interoperability) بين أقسام الإدارة (management sections) وبرمجيات الـ (agents).

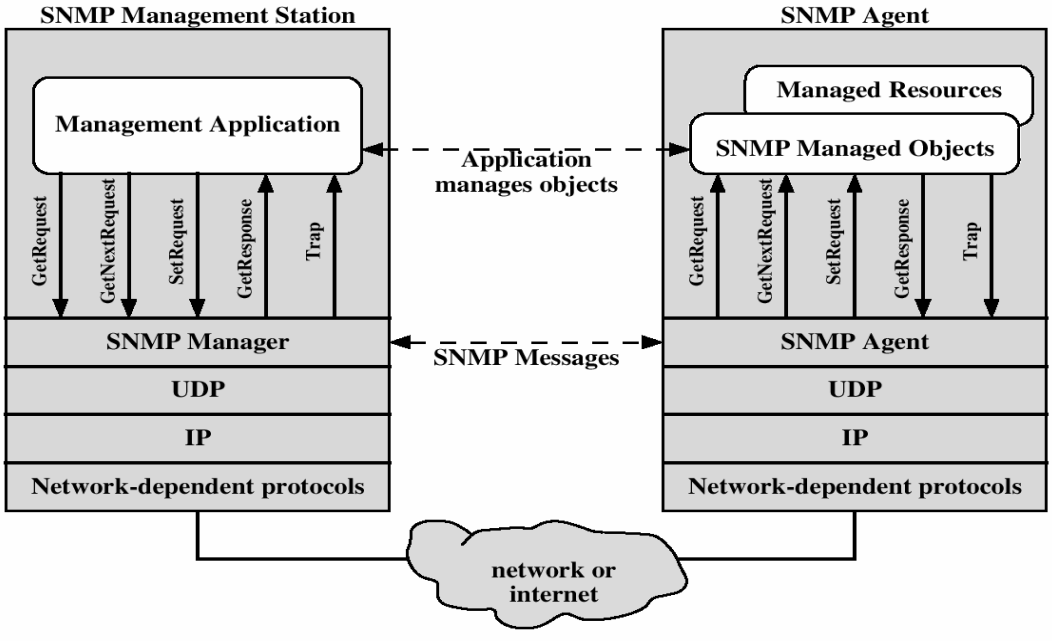
ميزات تصميم بروتوكول الـ (SNMP):

- صمم ليكون بروتوكولاً في المستوى التطبيقي (application-level protocol).
- يعد جزءاً من بروتوكول الـ (TCP/IP).
- معد للعمل فوق الـ (User Datagram Protocol) أو ما نطلق عليه اختصارا (UDP).

سياق بروتوكول الـ (SNMP):

- يشرح الشكل التالي ، سياق بروتوكول الـ (SNMP).
- من الـ (Management Station) تقوم الـ (management applications) بإصدار ثلاثة أنواع من الـ (SNMP messages) ، هي :
  - GetRequest.
  - GetNextRequest.
  - SetRequest.

- الرسالتان الأوليتان هما عبارة عن نوعين من أنواع الـ (get function).
- يقوم الـ (agent) بالإخطار بهذه الثلاث الرسائل في شكل رسالة (GetResponse) ، و يتم تمرير هذه الرسالة إلى أعلى حيث الـ (management application).
- قد يقوم الـ (agent) بإصدار (trap message) للاستجابة لحدث ما يؤثر في الـ (MIB) و الموارد الأساسية المدارة.
- بما إن الـ (SNMP) يعتمد على الـ (UDP) و الذي هو (connectionless protocol)، فإن الـ (SNMP) سيكون أيضاً (connectionless): بمعنى أنه لا توجد (connections) مستمرة بين الـ (Management Station) و الـ (agents) التابعين لها. بدلاً عن ذلك تكون كل التبادلات (exchanges) منفصلة بين الـ (Management Station) و الـ (agents).

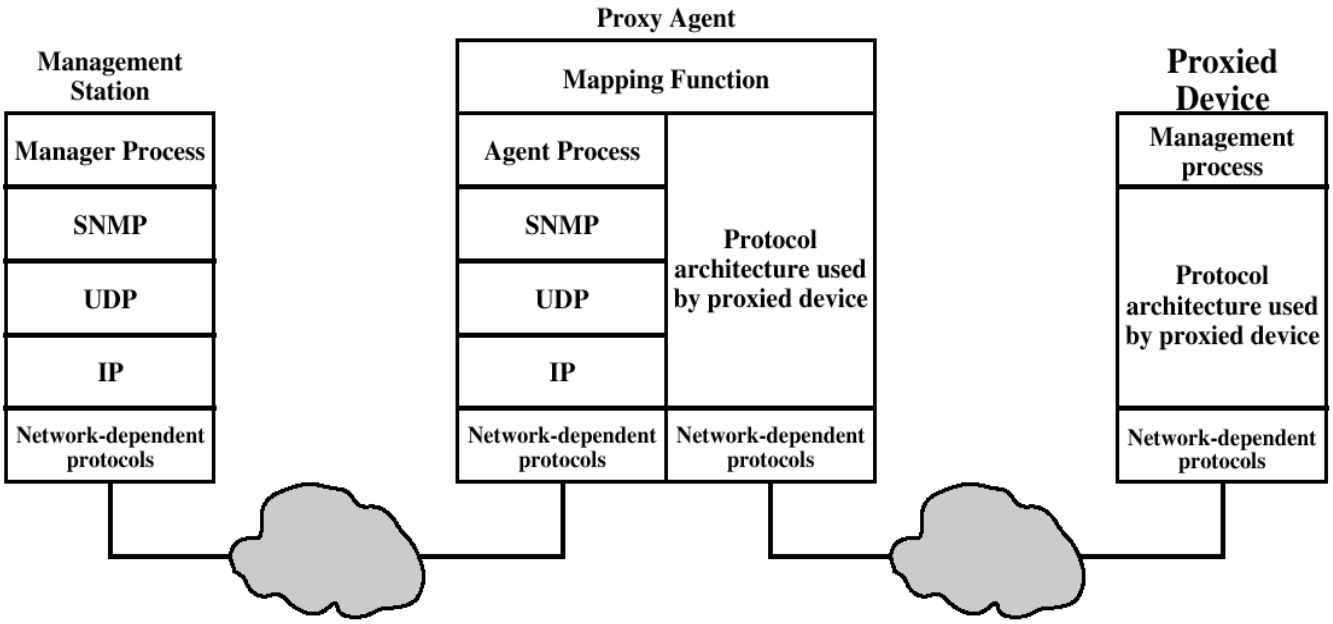


البروكسيز (Proxies):

- في (SNMPv1) ، يجب على كل الـ (agents) و كذلك الـ (Management Stations) أن تدعم الـ (UDP) و الـ (IP).
- و هذا يحد من الإدارة المباشرة لمثل هذه الأجهزة و يمنع أجهزة أخرى مثل بعض الـ (Bridges) و الـ (Modems) و التي لا تدعم أي جزء من مجموعة بروتوكول الـ (TCP/IP).
- للتغلب على مشكلة الأجهزة التي لا تنفذ بروتوكول الـ (SNMP) تم تطوير مفهوم الـ (Proxy).
- و حسب هذا المفهوم يعمل الـ (SNMP agent) كـ (proxy) لواحد أو أكثر من ألأجهزة الأخرى.

تهيئة البروكسي (Proxy Configuration):

- تقوم الـ (Management Station) بإرسال استعلامات إلى الـ (proxy agent) الخاص بجهاز معين.
- يقوم الـ (proxy agent) بتحويل أي استعلام إلى الـ (management protocol) الذي يستخدمه هذا الجهاز.
- عندما تصل استجابة الاستعلام إلى الـ (agent) فإنه يقوم بتمريرها إلى الـ (Management Station).
- و بشكلٍ مشابه، إذا قام جهاز ما بإرسال تنبيه بحدث معين :فإن الـ (proxy) يقوم بإرسال هذا التنبيه في شكل (trap message).



علاقات البروكسي الخارجية في (SNMPv2):

- يسمح (SNMPv2) باستخدام مجموعة بروتوكولات الـ (TCP/IP) بالإضافة على بروتوكولات أخرى، مثل مجموعة بروتوكولات الـ (OSI). و بالتالي يمكن استخدام (SNMPv2) لإدارة مجموعة واسعة من التهيئات الشبكية.
- فيما يتعلق بالـ (proxies)، فإن أي جهاز لا يقوم بتنفيذ (SNMPv2) يمكن فقط إدارته بواسطة الـ (proxy).
- إذا كان هناك جهاز ينفذ برمجية الـ (agent) الخاصة بـ (SNMPv1)، فيمكن الوصول إليه من مدير الـ (SNMPv2) فقط عن طريق جهاز الـ (proxy) الذي ينفذ الـ (SNMPv2 agent) و برمجية مدير الـ (SNMPv1).

علاقات البروكسي الأصلية في (SNMPv2):

- في هذه الحالة ، فإن الـ (proxied device) يدعم (SNMPv2).
- يقوم مدير الـ (SNMPv2) بالاتصال مع عقدة (node) من عقد الـ (SNMPv2) و التي تعمل كـ (agent).
- بعد ذلك تعمل هذه العقدة كمدير للوصول إلى الـ (proxied device)، و الذي يمثل الآن الـ (SNMPv2 agent).

الإصدار الثاني من بروتوكول إدارة الشبكات البسيط SNMPv2 :

- نعلم أن قوة بروتوكول الـ (SNMP) تكمن في بساطته.
- فهو يزود بمجموعة أساسية من أدوات إدارة الشبكة.
- و هذه الأدوات موضوعة في (package) سهلة الاستخدام و التهيئة.
- لكن مع ذلك فهناك عيوب و نقائص في هذا البروتوكول.

عيوب بروتوكول الـ (SNMP):

- نقص الدعم لإدارة الشبكات الموزعة (Distributed Network Management).
- نقائص وظيفية (Functional deficiencies).
- نقائص في السرية (Security deficiencies).

- النوعان الأولان من العيوب تم تلافيهما في (SNMPv2).
- أما النوع الثالث (النقائص في السرية) فقد تم تلافيها في (SNMPv3).
- لذا سنتطرق هنا للنوعين الأولين فقط.

أولاً :إدارة الشبكات الموزعة (Distributed Network Management):

سنتحدث أولاً عن إدارة الشبكة المركزية (Centralized Network Management)، وفيها يتم ما يلي:

- يقوم أحد الـ (host) بلعب دور الـ (Management Station) لهذه الشبكة. مع ملاحظة أنه قد يكون هناك أكثر من (host) يقوم بهذا الدور و ذلك فقط لعمل (Backup).
- بقية الأجهزة في هذه الشبكة تحتوي على برمجية (agent) و كذلك (MIB)، و ذلك حتى يمكن مراقبتها و التحكم فيها من قبل الـ (Management Station).
- مع نمو الشبكات و زيادة الـ (traffic)، أصبحت هذه الأنظمة غير ذات جدوى.

و كان الحل لهذه الإشكالية هو تطوير إدارة للشبكات الغير مركزية (Decentralized Network Management) ، أو ما نسميها بالشبكات الموزعة (Distributed Networks)، وفيها يتم ما يلي:

- قد يكون هناك العديد من الـ (Management Stations) العالية المستوى، والتي نشير إليها على أنها (Management Servers).
- كل (Server) منها يقوم بإدارة جزء مخصص من الـ (agents).
- مع ذلك فإنه في العديد من الـ (agents) يقوم الـ (Management Server) بتفويض المسئولية لمدير وسيط (Intermediate Manager).
- يلعب الـ (Intermediate Manager) دور المراقب و المتحكم بكل الـ (agents) الذين هم تحت مسئوليته.
- ويلعب الـ (Intermediate Manager) أيضاً دور الـ (agent) للتزويد بالمعلومات و استقبال التحكم من (Management Server) في المستوى الأعلى.

و نلاحظ أن (SNMPv2) يدعم الإدارة لكل من الـ (Centralized Networks) و كذلك الـ (Distributed Networks).

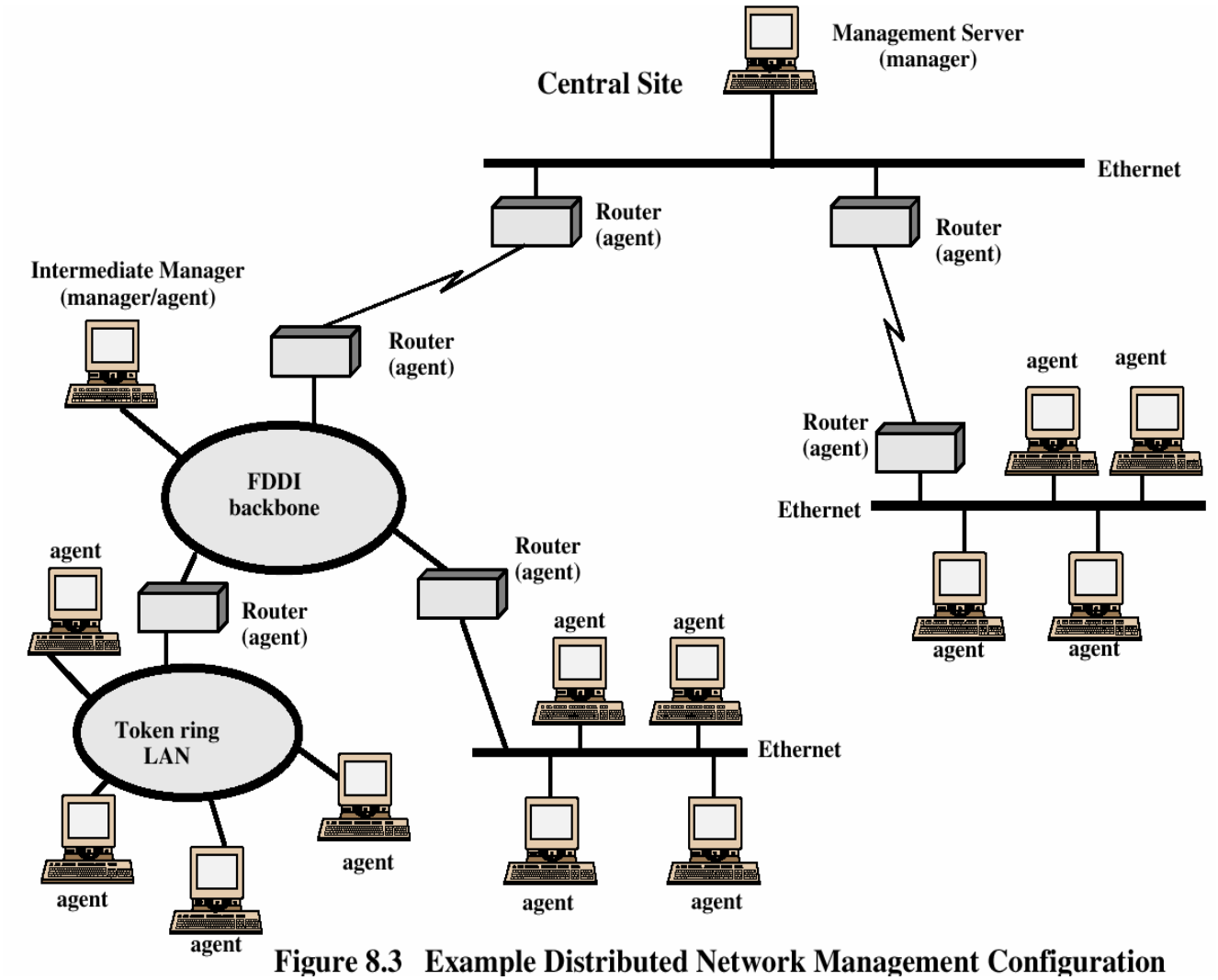


Figure 8.3 Example Distributed Network Management Configuration

ثانياً : التعزيزات الوظيفية (Functional Enhancement):

- يقدم الجدول التالي تطويرات وظيفية تم عملها في (SNMPv2).
- تم تعريف كلا البروتوكولين (SNMPv1 و SNMPv2) عن طريق مجموعة من الأوامر و التي نسيمها بوحدات بيانات البروتوكول (Protocol Data Units) أو اختصاراً (PDUs).

أولاً : الإصدار الأول (SNMPv1):

يوجد خمسة أوامر هي :

1- الأمر Get:

- ويتم إصداره من الـ manager إلى الـ agent و ذلك بغرض استعادة قيم الـ objects من الـ (MIB).

2- الأمر GetNext:

- و هو يستفيد من الحقيقة القائلة بأن الـ objects في الـ (MIB) تكون مرتبة في بنية شجرية (tree structure).
- إذا ما تم تسمية object في الأمر GetNext ، فأن الـ agent يقوم بإيجاد الـ object التالي في الشجرة و يرجع قيمته.

3- الأمر Set:

- يمكن الـ manager من تحديث القيم عند الـ agent.
- ويستخدم أيضا لخلق و حذف الصفوف من الجدول.

4- الأمر GetResponse:

- يستخدمه الـ agent بغرض الاستجابة لأمر الـ manager.

5- الأمر Trap:

- يمكن الـ agent من إرسال معلومة إلى الـ manager بدون الانتظار لطلب الـ manager.
- على سبيل المثال، قد يكون الـ agent معداً لإرسال Trap عند حصول فشل في ارتباط أو عندما يتجاوز المرور (traffic) حده.

ثانياً : الإصدار الثاني(SNMPv2):

يحتوي على كل الأوامر الموجودة في (SNMPv1) بالإضافة إلى أمرين جديدين:

1- الأمر Inform:

- و هو الأكثر أهمية.
- يتم إرساله من قبل (Management Station) إلى أخرى، وهو شبيه بالأمر Trap من حيث احتوائه على معلومات لها علاقة بشروط و أحداث في جهة المرسل.
- و من ميزاته أنه يستخدم في جعل العديد من الـ managers يتشاركون في تحمل مسئولية إدارة الشبكات الكبيرة.

2- الأمر GetBulk:

- هو يسمح للـ manager باسترجاع بلوك بيانات كبيرة في كل مرة.
- هذا الأمر صمم خصيصاً لإرسال كل الجداول باستخدام أمر واحد.

فرق أخير:

- الأمر Get في الـ (SNMPv1) غير قابل للتجزئة (atomic) بعكس الـ (SNMPv2).
- و نعني بذلك أنه إذا كان الأمر Get في الـ (SNMPv1) يحتوي على قائمة من الـ objects تكون قيمها مطلوبة ، وعلى الأقل لا يوجد أحد الـ objects عند الـ agent فإنه سيتم رفض الأمر تماماً.
- أما في الـ (SNMPv2) فإنه يمكن إرجاع نتائج جزئية.

مقارنة بين وحدات بيانات البروتوكول (PDUs) في كل من (SNMPv1) و (SNMPv2):

SNMPv1 PDU وحدات بيانات البروتوكول	SNMPv2 PDU وحدات بيانات البروتوكول	Direction (الاتجاه)	Description (الوصف)
GetRequest	GetRequest	Manager to agent من المدير إلى الوكيل	Request value for each listed object يتم طلب قيمة لكل كائن في القائمة
GetRequest	GetRequest	Manager to agent من المدير إلى الوكيل	Request next value for each listed object يتم طلب القيمة التالية لكل كائن في القائمة
------	GetBulkRequest	Manager to agent من المدير إلى الوكيل	Request multiple values يتم طلب قيم متعددة
SetRequest	SetRequest	Manager to agent من المدير إلى الوكيل	Set value for each listed object يتم وضع قيمة لكل كائن في القائمة
------	InformRequest	Manager to manager من المدير إلى المدير	Transmit unsolicited information يتم إرسال معلومة تطوعية
GetResponse	Response	Agent to manager or Manage to manager(SNMPv2) من الوكيل إلى المدير أو من المدير إلى المدير	Respond to manager request تتم الاستجابة لطلب المدير
Trap	SNMPv2-Trap	Agent to manager من الوكيل إلى المدير	Transmit unsolicited information يتم إرسال معلومة تطوعية

8.2 SNMPv1 Community Facility 2.8 تسهيل مجتمع الإصدار الأول من بروتوكول إدارة الشبكات البسيط

المجتمعات و أسماء المجتمع Communities and Community Names:

- تتشابه إدارة الشبكة (Network Management) مع التطبيقات الموزعة (Distributed Applications) في أنها تتضمن عدداً من كينونات التطبيق المدعومة من قبل الـ (Application Protocol).
- فمثلاً في حالة إدارة الشبكة بواسطة (SNMP) فإن التطبيقات المستخدمة هي: تطبيقات المدير (Manager applications) و تطبيقات الوكيل (Agent applications).

تتضمن إدارة الشبكة بواسطة (SNMP) على خصائص ليست موجودة في كل التطبيقات الموزعة:

- يتضمن التطبيق على علاقة (one-to-many) بين الـ manager و مجموعة من الـ agents: و هذا يعني أن الـ manager قادر على عمل set و get للـ objects لكل الـ agents ، و كذلك استقبال traps من الـ agents.
- يتضمن التطبيق على علاقة (one-to-many) بين الـ agent و مجموعة من الـ managers: حيث يتحكم كل agent بالـ (MIB) الخاصة به و يجب أن يكون قادراً على التحكم في استخدام هذه الـ (MIB) من قبل مجموعة من الـ managers.

أوجه تحكم الـ agent بالـ (MIB) المحلية الخاصة به:

هناك ثلاثة أوجه لهذا التحكم ، و هي:

خدمة التوثق Authentication Service:

- قد يريد الـ agent أن يجعل الوصول إلى الـ (MIB) مقصوراً على الـ managers الذين لديهم صلاحية.
- الغرض من هذه الخدمة في (SNMPv1) هو التأكيد للمستقبل أن رسالة الـ (SNMPv1) قادمة من المصدر الصحيح.
- و آلية عمل التوثق في (SNMPv1) هو أن كل رسالة من الـ manager إلى الـ agent يجب أن تتضمن على "اسم مجتمع" (Community Name)، هذا الاسم يعمل ككلمة مرور ، و سيكون الـ manager ذو موثوقية فقط إذا كان يعرف هذه الكلمة.

سياسة الوصول Access Policy:

- قد يريد الـ agent أن يعطي امتيازات وصول مختلفة للـ managers المختلفين.
- بعد تعريف الـ (Community) يقوم الـ agent بقصر الوصول للـ (MIB) الخاصة به على مجموعة من الـ managers.
- باستخدام أكثر من (Community) يمكن للـ agent أن يزود بتصنيفات مختلفة للوصول للـ (MIB) حسب تصنيف الـ managers.

هناك مجالين للتحكم بالوصول، و اثنين إضافيين:

الأول : (SNMP MIB view):

- مجموعة من الـ objects داخل الـ (MIB).
- يمكن تعريف (MIB views) مختلفة لكل (Community).
- ليس بالضرورة أن مجموعة الـ objects في الـ (view) تنتمي إلى شجرة فرعية واحدة في الـ (MIB).

الثاني : (SNMP access mode):

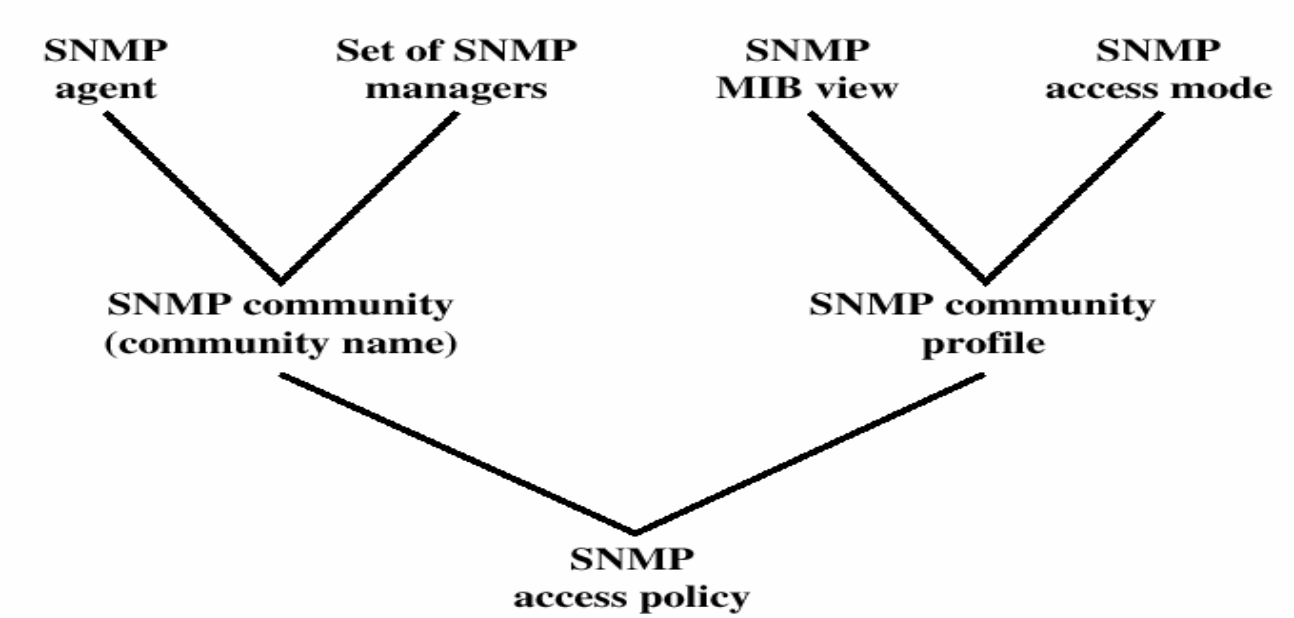
- عنصر من المجموعة (READ ONLY, READ WRITE).
- يتم تعريفه لكل (Community).

الثالث : (SNMP community profile):

- و هو عبارة عن تركيب من الـ (MIB view) و الـ (Access mode).
- يتكون من مجموعة جزئية معرفة من الـ (MIB) عند الـ agent + الـ access mode لهؤلاء الـ objects.

الرابع : (SNMP access policy):

- و هو عبارة عن تركيب من الـ (SNMP Community) و الـ (SNMP community profile).
- الشكل التالي يوضح كل هذه المفاهيم.



خدمة البروكسي (Proxy Service):

- يعد مفهوم الـ (Community) مهماً في دعم خدمة البروكسي.
- نعلم أن البروكسي هو عبارة عن (SNMP agent) يعمل من قبل أجهزة أخرى خارجية.
- في بعض الحالات ، قد يدعم النظام الخاضع لعمليات البروكسي بروتوكول الـ (SNMP) و لكن البروكسي يستخدم لتقليل التفاعل بين الـ (Proxied Device) وأنظمة إدارة الشبكات.

تم بحمد الله