بسم الله الرحمن الرحيم

جامعة السّودان المفتوحة

برنامج الحاسوب

استخدام وإدارة الشبكات (2)

رمز المقرر ورقمه: تقن 4033

إعداد المادة العلمية: أ.د. السيد محمود الربيعي

: أ.د. عبد الحميد محمد رجب

تصمـــيم تعلـــيمي : د. عبد الباسط محمد شريف

التدقيق اللغوي : أ. الهدي عبد الله محمد محمد أحمد

التصميم الفني : أ. أماني الأمين مبارك

منشورات جامعة السودان المفتوحة، الطبعة الأولى 2008م

مقدمة المقرر

الحمد لله رب العالمين والصلاة والسلام على رسوله الكريم، محمد صلى الله عليه وعلى آله وصحبه وسلم وبعد.

عزيزي الدارس،

بين يديك كتاب "استخدام وإدارة الشبكات 2".

لقد توسعت شبكات الحاسبات وزاد حجمها، واستخدمت في ربط مئات وآلاف الحاسبات بأنواعها المتعددة في شبكات متكاملة محلية وإقليمية ودولية. وقد ترتبط هذه الشبكات معاً إما سلكيا أو لاسلكيا خلال شبكة المعلومات الإنترنت. ونظراً للتزايد المستمر في بناء الشبكات وكذلك عدد الحاسبات التي تحتويها كل شبكة منها؛ فقد أصبح علم إدارة الشبكات مطلبا أساسيا يهدف إلى إدارة موارد الشبكات من عتاد وبرمجيات لتحقيق خدمة مثلى للمستخدمين المتصلين بالشبكة بتكلفة مناسبة وسرعة وأمان مناسبين.

ولقد أعدَّت جامعة السودان المفتوحة برنامج البكالوريوس في تقانة المعلومات بغرض تلبية الحاجة المتنامية لمتخصصين في مثل هذا المجال المتطور، وقد اشتمل هذا البرنامج على مقررين خاصين لاستخدام وإدارة الشبكات، الأول: استخدام وإدارة الشبكات (1)، والثاني: استخدام وإدارة الشبكات (2). يكمل بعضيهما الآخر، تم إعدادهما باللغة العربية ليكون أمام خريجي هذا البرنامج فرص عمل (مديرو إدارة شبكات أو مهندسو صيانة شبكات)، وهي من الوظائف التي من المتوقع زيادة الطلب عليها خلال السنوات القليلة المقبلة، خاصة في مجالات الشبكات بأحجامها وأنماطها المختلفة.

والمقرر الذي بين يديك الآن تحت عنوان "استخدام وإدارة الشبكات (2)" هو مقرر متقدم إلى حد كبير في استخدام وإدارة الشبكات بأنماطها المختلفة، وهو مكمل للمقرر الأول والذي تم نشره تحت عنوان استخدام وإدارة الشبكات (1) والذي يعتبر متطلباً أساسياً، ولا يمكن للطالب دراسة المقرر الثاني دون دراسة محتويات المقرر الأول.

وقد راعينا في صياغة هذا الكتاب أن يكون في صورة وحدات منفصلة متخصصة، كل وحده متكاملة تناقش فرعية معينة على نفس الطريقة التي اتبعناها في صياغة الجزء الأول من الكتاب.

والمتطلبات الأساسية لدراسة هذا الكتاب هو أن يكون لدى القارئ معرفة أساسية مسبقة بأساسيات وتقنيات اتصال البيانات في شبكات الحاسب الآلي، وكذلك الدراسة المتأنية للكتاب الأول"استخدام وإدارة الشبكات (1) " ويهدف هذا الكتاب في مجمله إلى تزويد الطالب بالمعرفة اللازمة والتهيئة لمستقبل مهني في مجالات استخدام وإدارة الشبكات المتقدمة، وما يدخل فيها من مفاهيم متعلقة بالإدارة المثلى لموارد الشبكة من عتاد وبرمجيات بغرض تقديم خدمة مثلى للمستخدمين المتصلين بالشبكة بتكلفة مناسبة وسرعة وأمان مناسبين، وهي مجموعة من المفاهيم تؤصل للدارس كيف يقوم بالتخطيط الجيد في المستقبل للشبكات.

ويشتمل هذا الكتاب على الوحدات التالية :

الوحدة الأولى: وعنوانها: " بروتوكول إدارة الشبكة البسيط الإصداران الأول والثاني"، نقدم فيها فكرة واضحة ودقيقة حول مجموعة من المفاهيم والتي من أهمها: أساليب تجميع البيانات من الشبكة، بروتوكول الإنترنيت الأمر بنج، تطوير البروتوكولات القياسية لإدارة الشبكة، برتوكول إدارة الشبكة البسيط "سنمب–ف1"، أنواع الرسائل والحصول على المعلومات وضبطها، الأمن في بروتوكول "سنمب–ف1"، مشاكل بروتوكول "سنمب–ف1"، برتوكول إدارة الشبكة البسيط "سنمب–ف2"، مميزات وخصائص "سنمب–ف2"، وسائل الأمن لبروتوكول"سنمب–ف2".

الوحدة الثانية: وعنوانها : " بروتوكول إدارة الشبكة البسيط الإصدار الثالث" ، وفيها: توضيح خصائص بروتوكول "سنمب–ف3" والبناء الهيكلي له، والعمليات التفاعلية بين آلة "سنمب–ف3" ومجموعة التطبيقات، نموذج أمن المستخدم USM، تحقيق التوثيق و الخصوصية وصحة الرسائل، توليد المفاتيح السرية والمحلية وإدارتها، التحقق من عدم تأخر الرسائل والتوقيت المتزامن، اختيار الآلات الموثقة، نموذج تحكم الوصول لرؤية

المعلومات VACM، معالجة تحكم الدخول لمرئية قاعدة المعلومات الإدارية، العمليات المنطقية في نموذج "فاكم" مكونات فورمات رسالة "سنمب--ف3".

الوحدة الثالثة : وعنوانها : " بروتوكول إدارة الخدمات المعلوماتية الشائعةCMIS/CMIP " ، وفيها تم بيان: خصائص بروتوكول CMIP، نموذج إدارة الشبكة باستخدام بروتوكول CMIP، وخدمات المعلومات الإدارية الشائعة CMIS ، الخدمات الإدارية المرافقة، و إدارة الإشعار، و إدارة العملية، المرافقات الإدارية و قوائم الدخول، مشاكل بروتوكول CMIS/CMIP ، بروتوكول CMOT، و بروتوكول LMMP ، مقارنة بين بروتوكول CMIP وبروتوكول SNMP.

الوحدة الرابعة : وعنوانها : "قواعد معلومات إدارة الشبكات (الجزء الأول)" ، وفيها تم توضيح كل من:الهيكل البنائي لقاعدة المعلومات الإدارية، محدد العنصر والشجرة المستعرضة وتطبيقاتها، قاعدة المعلومات الإدارية MIB-I لبروتوكول سنمب-ف1، المعلومات المعرفة لنظام SMI مع أمثلة تطبيقية، قاعدة المعلومات الإدارية لبروتوكول سنمب- ف2 وأقسامها، قاعدة المعلومات الإدارية الخاصة بالمديرين وأطراف الاتصال، التوافق Coexistence مع إصدارات بروتوكول سنمب، قاعدة المعلومات الإدارية MIB-II، وحساب معدل التغير للعنصر، مجموعة النظام واستخدامها لإدارة الأعطال وإدارة التهيئة مع أمثلة لها، مجموعة البينية واستخدامها في إدارة التهيئة والأداء والحسابات مع أمثلة لها، عناصر تحديد المستويات الفرعية و الدوائر الافتراضية والمعلومة والحرف، مجموعة ترجمة العنوان و هيكلها البنائي و طرق الترجمة مع أمثلة لها.

الوحدة الخامسة: وعنوانها: "قواعد معلومات إدارة الشبكات (الجزء الثاني) " ، وفيها تم بيان كل من:مجموعة بروتوكول الإنترنيت IP وبنائها الهيكلي، تطبيقات عناصر IP في إدارة الأعطال،التهيئة، الأداء، الحسابات مع أمثلة لها، مجموعة عناصر بروتوكول رسائل تحكم الإنترنيت ICMP، وتطبيقاتها، مجموعة عناصر بروتوكول النقل TCP وبنائها الهيكلي، تطبيقات عناصرTCP في إدارة التهيئة، الأداء، الحسابات، الأمن مع

أمثلة كافية عن ذلك، مجموعة بروتوكول UDP، وبناؤها الهيكلي، تطبيقات عناصر UDP في إدارة الأداء، الحسابات، التهيئة، الأمن مع أمثلة له، نبذة مختصرة عن مجموعة بروتوكول EGP، وعيوبه ومعالجتها بواسطةBGP . نبذة مختصرة عن مجموعة بروتوكول CMOT، مجموعة عناصر الإرسال، Transmission-Group، مجموعة بروتوكول SNMP وتطبيقاتها في إدارة الأعطال، الأداء،الحسابات، الأمن، التهيئة وأمثلة لكلّ ذلك.

الوحدة السادسة: وعنوانها: " رصد الشبكات عن بعد"، وفيها تم توضيح كل من: أجهزة رصد الشبكة عن بعد، أهداف قاعدة المعلومات الإدارية للرصد عن بعد، مجموعات عناصر قواعد المعلومات الإدارية RMON1, RMON2 ، مجموعة الإحصائيات وتطبيقاتها في إدارة الأعطال، التهيئة، والأداء، مجموعة التاريخ ومجموعة الإنذار وإدارة الأداء، مجموعة الحاسب المضيف وإدارة الأداء والحسابات، مجموعة القمة N للحاسب المضيف واستخداماتها، مجموعة المصفوفة وهيكلها البنائي واستخداماتها، مجموعة المرشحات وهيكلها البنائي واستخداماتها، مجموعة مسك الحزم ومجموعة الأحداث واستخداماتها، مجموعات قاعدة المعلومات الإدارية رمون-2 واستخداماتها،مقارنة بين بروتوكولات SNMP، CMIP، RMON.

الوحدة السابعة: وعنوانها: " الأدوات البرمجية المعاونة في إدارة الشبكات" وفيها: بيان: أدوات قاعدة المعلومات الإدارية، المترجم والمتصفح، وأداة الاستفسار، وأداة الأسماء المستعارة Alias أدوات العرض (السجل المركزي، وبرنامج كاتب التقرير، والحزم الرسومية)، أدوات حل المشاكل(نظام تتبع المشكلة، وأدوات تصميم الشبكة، والنظم الخبيرة)، تدريبات وتطبيقات عملية.

الوحدة الثامنة: وعنوانها : " تطبيقات في إدارة الشبكات " وفيها: بيانإدارة شبكات ويندوز Windows، تنصيب بروتوكول SNMP على نظام تشغيل النوافذ، خدمات SNMP في نظام النوافذ، قواعد المعلومات الإدارية MIBs لنظام النوافذ، إدارة شبكات يونيكسUnix، استخدام الوكيل التابع Proxy في نظم يونيكس، قاعدة المعلومات

الإدارية MIB لمحطة عمل يونيكس، إدارة شبكات IBM ،إدارة شبكات ATM ، نظام COBRA لإدارة الشبكات ، إدارة شبكات الويب Web.

عزيزي الدارس، كل وحدة من هذه الوحدات تحمل عنواناً جامعاً يعبر عن موضوعاتها، ولكل منها مقدمة وخلاصة، كما زودت كل وحدة بعدد من أسئلة التقويم الذاتي، وأحياناً بعدد من التدريبات والمناشط، وكذلك تشمل كل وحدة مسرد للمصطلحات والكلمات التي وردت فيها كما ذيلنا وحدات هذا المقرر بقائمة للمصادر والمراجع المتنوعة التي تم الاستعانة بها في بناء الوحدات، ليلجأ إليها الدارس إذا ما احتاج إلى تفاصيل أكثر.

عزيزي الدارس، لدى قراتك هذا الكتاب أرجو أن لا يغيب عن ذهنك أن مادة هذا الكتاب هي الحد الأدنى من المعرفة في موضوعه، الذي يسمح بإثرائه على الدوام بالرجوع إلى القراءات المساعدة والاطلاع عليها.

وختاماً نرجو أن نكون قد وفقنا في تقديم إضافة جديدة لمكتبة جامعة السودان المفتوحة من خلال هذا الكتاب ونسأل الله تعالى أن يكون هذا العمل خالصا لوجهه وأن يكون في ميزان حسناتنا وأن ينتفع به الجميع، ويغفر لنا ما سهونا عنه وعجزنا عن إدراكه.

ونحن نرحب بكل نقد بناء يسهم في تطوير هذا العمل إلى الصورة الأفضل على عناوين البريد الإلكتروني: **ahm_ragab@hotmail.com** ، أو **srabie1@yahoo.com** ، والله نسأل الأجر والثواب وآخر دعوانا أن الحمد لله رب العالمين إنه نعم المولى ونعم النصير.

وفيما يلي قائمة بعناوين الوحدات الواردة في هذا المقرر مع أرقام صفحاتها.

الأهداف العامة للمقرر

عزيزي الدارس، بعد فراغك من دراسة هذا المقرر يؤمل أن تكون لك القدرة على:

- **شرح** البروتوكولات البسيطة التي تستخدم في إدارة الشبكة بكفاءة عالية.
- **تذكُّر** خصائص بروتوكول "سنمب--ف3" و البناء الهيكلي له.
- **مناقشة** خصائص بروتوكول معلومات الإدارة الشائعة CMIS/ CMIP.
- **وصف** المعلومات المتاحة على أجهزة الشبكة التي يمكن الوصول إليها بواسطة بروتوكول إدارة الشبكة بدقة متناهية.
- **وصف** العناصر المكونة لقاعدة المعلومات الإدارية الشهيرة MIB-II، التي تستخدم كمكون أساسي في بروتوكولات إدارة الشبكات.
- **شرح** قواعد المعلومات الإدارية MIB الخاصة برصد الشبكات عن بعد RMON1, RMON2.
- **تعداد** الأدوات البرمجية المعاونة في إدارة الشبكات.
- **تحديد** المتطلبات اللازمة لكيفية تطبيق بروتوكول SNMP لإدارة أجهزة الشبكات.
- **تبيين** بعض الاتجاهات الحديثة لإدارة الشبكات .

محتويات المقرر


الوحدة الأولى
بروتوكول إدارة الشبكات البسيط
الإصداران الأول والثاني

محتويات الوحدة

المقدمة

تمهيد

عزيزي الدارس،

نرحب بك إلى الوحدة الأولى من مقرر " استخدام وإدارة الشبكات2" وموضوعها "بروتوكول إدارة الشبكات البسيط الإصداران الأول والثاني SNMPv1,v2 ".

تعلمنا من دراستنا للجزء الأول من كتاب استخدام وإدارة الشبكات، أن إدارة الشبكة بكفاءة تعتمد على قدرة مهندس الشبكة على الرصد والتحكم في شبكة البيانات وبدون هذه المعلومات؛ فإن مهندس الشبكة سوف يضطر لاتخاذ قرارات إدارة الشبكة بدون الاعتماد على الفوائد التي توفرها القياسات الكمية والجودة الملائمة Adequate Qualitative.

نشرح في هذه الوحدة الدراسية البروتوكولات البسيطة التي تستخدم في إدارة الشبكة بكفاءة عالية، كما نقدم الأساليب الأساسية المتاحة للحصول على المعلومات من شبكة البيانات، وكذلك ضبط قيمها، والذي بدونها تكون عملية تحقيق الأهداف من إدارة الشبكة مستحيلا. كما نستعرض في هذه الوحدة الأساليب المختلفة التي بواسطتها يستطيع مهندس الشبكة أن يحدد الطريقة المناسبة لإدارة شبكة المؤسسة التي يعمل فيها بكفاءة وقدرة عالية. وتشتمل هذه الوحدة على أربعة أقسام: القسم الأول منها يقدم نبذة تاريخية عن أساليب تجميع البيانات اللازمة لإدارة الشبكة، القسم الثاني يتناول تطوير البروتوكولات القياسية لإدارة الشبكات، القسم الثالث يتناول بروتوكول إدارة الشبكة البسيط (الإصدار الأول SNMPv1)، ونجد في هذا القسم أنواع الرسائل في SNMPv1 وكذلك الحصول على المعلومات وضبطها. القسم الرابع يتناول الإصدار الثاني للبروتوكول "سنمب" SNMPv2 حيث نجد في هذا القسم تحسين هيكل المعلومات الإدارية "SMI" ، كذلك يتناول القسم أنواع الرسائل في البروتوكول SNMPv2 ،

وأيضاً نجد في هذا القسم تدعيم البروتوكولات المتعددة Multiprotocol، حيث نجد أن سنمب–ف2" قد تم تصميمه ليعمل مع أربعة أنواع من البروتوكولات هي: (IP, AppleTalk, IPX, OSI CLNS) ، تناول القسم أيضاً وسائل الأمن في البروتوكول SNMPv2 ، وتناول مرئية قاعدة المعلومات الإدارية MIB View ، وتعرف مرئية قاعدة المعلومات الإدارية MIB View بأنها جزء قاعدة المعلومات الإدارية الذي يمكن الوصول إليه accessible بواسطة المدير Manager، وقد تناول القسم **أيضاً** السياق contexts. ويعرف السياق context في الإصدار الثاني للبروتوكول "سنمب–ف2" بأنه مجموعة العناصر الإدارية managed objects التي يمكن للمدير أو الوكيل أن يصل إليها.

أهداف الوحدة

عزيزي الدارس، بعد فراغك من دراسة هذه الوحدة ينبغي أن تكون قادراً على أن:

- **تكتب** نبذه تاريخية عن تطوير أساليب إدارة شبكة البيانات.
- **توضح** أساليب تجميع البيانات اللازمة لإدارة الشبكة.
- **تبيَّن** بروتوكول إدارة الشبكة البسيط، مميزاته وعيوبه.
- **تشرح** فوائد أنواع الرسائل المتعددة المستخدمة لإدارة الشبكة.
- **تذكر** الفرق بين بروتوكول سنمب–ف1، و سنمب–ف2.
- **توضح** كيفية عمل أساليب التوثيق والتشفير المستخدمة في تحقيق الأمن في بروتوكول سنمب–ف2.
- **تعدد** وظائف المدير والوكيل والوكيل المساعد في نموذج إدارة الشبكة.
- **تعدد** فوائد رسائل المصيدة وأنواعها ودورها في تحسين أداء الشبكة.
- **تستخدم** برتوكول سنمب–ف1، و سنمب– ف2 في إدارة الشبكات.
- **تصف** بعض وظائف إدارة الأمن.
- **توضح** كيفية إدارة شبكة البيانات بكفاءة عالية.

1. نبذة تاريخية عن أساليب تجميع البيانات اللازمة لإدارة الشبكة

يحتاج مهندسو الشبكات أن يتعلموا أساليب مختلفة لإجراء عملية تجميع المعلومات من أجهزة الشبكة. وكلما تَّم تطوير منتجات شبكية جديدة مصنعو هذه المنتجات تبتنصيب أساليب ملائمة كي يتم التمكن من تجميع البيانات من هذه المنتجات الشبكية. ينتج عن ذلك أنه يمكن لجهازين أن يكون لهما نفس الوظائف رغم أنهما صُنعَا في مصنعين مختلفين، وهذا ينتج عنه أساليب مختلفة جدا لتجميع البيانات.

وفيما يلي شرحٌ تفصيليّ لبعض هذه الأساليب:

1.1 نظام القائمة المنسدلة ونظام الأمر الخطي

يمكن أن يُستَخْدمَ نظامان في تجميع البيانات اللازمة لإدارة الشبكة، هما نظام القائمة المنسدلة، ونظام الأمر الخطي.

أولاً : نظام القائمة المنسدلة Menu-Driven System

في هذه الطريقة، كما هو موضح في الشكل 1.1، يتم استخدام جهاز الماوس المتصل بالحاسب والضغط على المفاتيح المناسبة لتظهر البيانات المطلوبة على شاشة النظام الإداري.

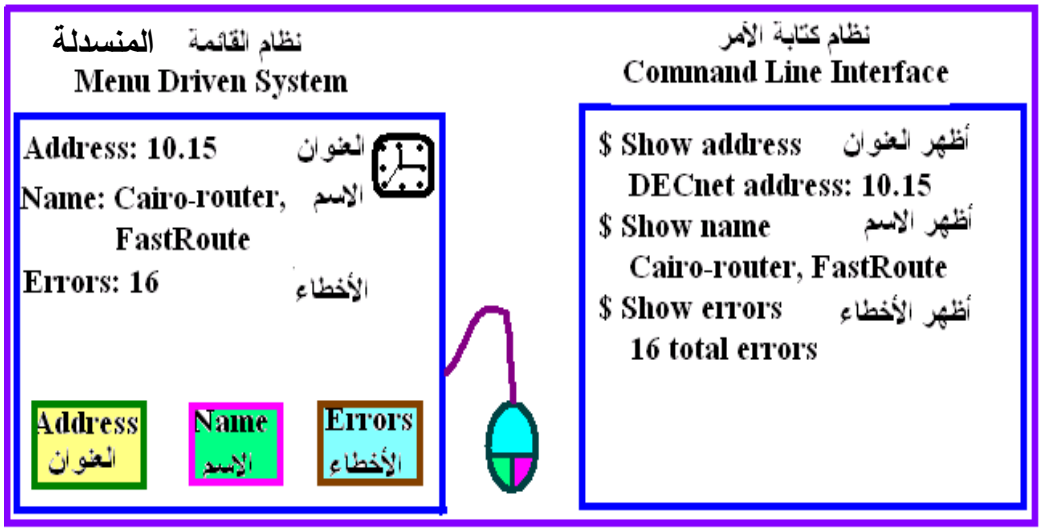
ثانياً : نظام الأمر الخطي: Command Line Interface

في هذه الطريقة يتم كتابة الأمر المناسب على شكل سطري على شاشة النظام الإداري، وبعد تنفيذ الأمر يتم ظهور المعلومات على شاشة العرض بالنظام.

على سبيل المثال، نفترض أن شبكة بيانات تستخدم نوعين من الموجهات Routers من نوع ديكنت DEC net لتوصيل أجهزة الحواسيب الرقمية بالشبكة. وأن الموجه الأول (A) قد تم إنتاجه من شركة الموجهات الفعالة، وأن الموجه الثاني (B) تم إنتاجه من

شركة أخرى تسمى شركة الموجهات السريعة. وأن كلا النوعين من الموجهات يسمحان أن يتم التوصيل بهما من خلال الدخول عن بعد Remote Login ، ولكن الوسيلة المستخدمة للوصول إلى البيانات تختلف تماما. للاستعلام من الموجه "A" عن عدد الوحدات البينية interfaces ومعاملات التشغيل Operating Parameters ينبغي أن نستخدم نظام القائمة المنسدلة Menu-Driven System . أما للاستعلام عن الموجه "B" ، يمكن أن يتم ذلك باستخدام ثلاثة أوامر من الوحدة البينية الخاصة بكتابة الأمر على شكل سطري Command Line . يوضح الشكل1.1 أمثلة لاثنين من الوحدات البينية المستخدمة، هما:

- الوحدة البينية الأولى لقائمة مشتقة Menu-Driven Interface
- الوحدة البينية الثانية لأمر خطي Command Line Interface



شكل1.1 نظم تجميع البيانات باستخدام بينية القائمة المنسدلة، وبينية الأمر الخطي.

1.1.1 عيوب هذه الطرق

تكون أساليب تجميع البيانات عن الشبكة باستخدام هذه الطرق، بطيئة ومتعبة، خاصة في بيئة الشبكات غير المتجانسة Heterogeneous وكذلك عند استخدام أساليب استفسار متعددة. لهذا السبب نحتاج إلى أسلوب موحد لتجميع البيانات عن كل مكونات شبكة البيانات، حيث إن مهندس الشبكة يطلب أدوات عامة ولكن قياسية standard tools. على الرغم من أن مصنعي منتجات الشبكات يوفرون أدوات متعددة تكون بسيطة الاستخدام، لكنها لا تصمم بالتحديد من أجل إدارة الشبكة وهذا يسبب مشكلة.

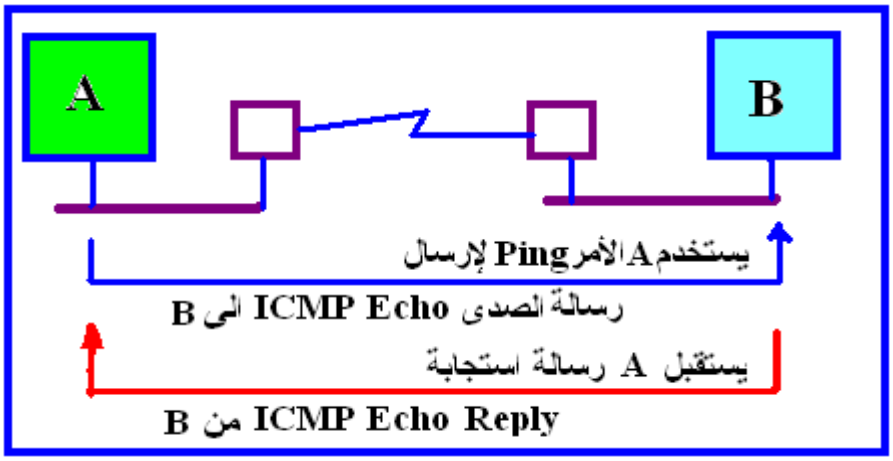
2.1 بروتوكول الإنترنيت Internet Protocol

يستطيع مهندس الشبكة استخدام رسائل الصدى Echo والاستجابة Echo Reply وذلك في شبكات البيانات التي تستخدم بروتوكول الإنترنيت Internet Protocol (IP)، لتجميع معلومات محددة تفيد في إدارة الشبكة، بواسطة بروتوكول رسائل تحكم الإنترنيت(ICMP) Internet Control Message Protocol، حيث إن هذا البروتوكول يستخدم أساسا في إرسال معلومات رسائل التحكم بين جهازين في الشبكة. وأن معظم رسائل البروتوكول ICMP يصعب تفسيرها interpret بواسطة الأشخاص. على الرغم من ذلك، فإن رسائل الصدى والاستجابة باستخدام بروتوكول ICMP توفر وسيلة سريعة لفحص توصيلة جهاز بالشبكة عن بعد.

وباستخدام هذه الرسائل، فإن جهاز الحاسب المضيف Host Computer الموجود بالشبكة والذي يستقبل رسالة الصدى ICMP Echo ينبغي أن يقوم بإرجاع رسالة استجابة ICMP Echo Reply إلى جهاز الحاسب المصدر المضيف. وأن عدم استقبال رسالة تم إرسالها بواسطة الحاسب المضيف، يمكن أن تبين وجود ضعف في توصيلة الشبكة بين الحاسبين المضيفين.

1.2.1 استخدام الأمر Ping

يعتبر الأمر بنج Ping ويعنى(Packet Inter Net Groper ، طريقة تلمس حزمة الإنترنيت)، هو أحد الأوامر التطبيقية شائعة الاستخدام في اختبار توصيلة جهاز متصل بالشبكة عن بعد. وذلك بواسطة إرسال رسالة صدى ICMP Echo إلى الجهاز المتصل بالشبكة عن بعد ، وبعد فترة انتظار يتم استقبال رسالة استجابة Echo Reply ICMP من الجهاز . يوضح الشكل1.2 الرسائل المرسلة والمستقبلة بواسطة الحاسوب المضيف باستخدام الأمر التطبيقي بنج Ping.



شكل1.2 الرسائل المرسلة والمستقبلة بواسطة الحاسب المضيفA,B باستخدام الأمر Ping.

إن معظم التطبيقات التي تستخدم الأمر بنج Ping يمكن أن تحدد أيضا إجمالي الفترة الزمنية للدورة turn around time بين رسالة الصدى المرسلة ورسالة الاستجابة بين حاسب المصدر source وحاسب الهدف destination، وتكون عادة بوحدة مللي/ ثانية. يوجد الأمر بنج ping أيضا في بروتوكولات أخرى عديدة بالإضافة إلى البروتوكول TCP/IP، وذلك مثل البروتوكولات نوفل Novel/IPX، وأبل Apple talk، وبانيان Banyan Vines، وزيروكس Xerox XNS.

2.2.1 من عيوب هذه الطريقة ما يلي:

أ ــ أنه لا يعتمد عليها في توصيل الرسائل.

ب ــ تحتاج لإجراء عملية التصويت Polling.

ج ــ توفر معلومات محدودة.

إن معظم حزم بيانات رسائل الصدى واستجابتها تستخدم مباشرة المستوى الشبكي Network Layer ، ولا يوجد ضمان كي يتم توصيلها بواسطة مستوى النقل Transport Layer . ولهذا السبب فإن الإخفاق في عدم وصول رسالة الصدى بين مكانين (جهازين متصلين بالشبكة) لا يعنى دائما بالضرورة وجود ضعف في توصيلة هذين الجهازين. ربما يكون ذلك بسبب أن الجهاز المتصل بالشبكة قد أسقط رسالة الصدى واستجابة الصدى بسبب نقصان مؤقت في حجم الذاكرة المؤقتة Buffer Space. أو أن حزمة البيانات قد أخفقت الوصول بسبب اختناق Congestion في دائرة البيانات أثناء الفترة الزمنية التي تم فيها عملية إرسالها.

لإيجاد المعلومات الحالية باستخدام الصدى والاستجابة، ينبغي إجراء عملية التصويت Polling المستمر لأجهزة الشبكة. إن إجراء عملية التصويت هذه هي وسيلة شائعة الاستخدام لعزل الأعطال Fault Isolation، حيث يمكن أن تتم بسرعة وسهولة، ولا تتطلب تجهيزات خاصة أو عتاد إضافي. عندما يتبين وجود نسبة عالية في فقدان استجابات رسائل الصدى يكون ذلك بياناً لوجود مشكلة في التوصيل. على الرغم من أن هذه الطريقة هي امتداد لتوفير الإمكانية لتشخيص الأعطال Trouble Shooting؛ فإن مهندس الشبكة يحتاج الاعتماد على وسائل أخرى لعزل وتصليح المشكلة. ينبغي على بروتوكول إدارة الشبكة توفير القدرة لامتلاك أجهزة ترسل رسائل تطوعية Unsolicited Messages لبيان وقوع أحداث معينة وتبليغها لنظام إدارة الشبكة. ويمكن أن يحدث ذلك بالإضافة إلى عملية التصويت، ولكنها تكون طريقة أكثر فاعلية لتجميع المعلومات المهمة لإدارة الشبكة.

أحد الأسباب الأساسية لهذا النقص هو بسبب أن رسائل الصدى واستجابتها لم يتم كتابتها بحيث توفر معلومات كافية، ولهذا السبب فإن المعلومات التي تنتج منها عادة تكون غير كافية ولا نستطيع استخدامها كأساس لاتخاذ قرارات حاسمة لإدارة الشبكة. لهذا الغرض فإنه من المفضل استخدام بروتوكول تم كتابته خصيصا لإدارة شبكات البيانات. وهو البروتوكول الذي يقوم بتوفير كثير من المعلومات الضرورية لإدارة الشبكة، وأن يعمل على نطاق واسع لأجهزة الشبكة. وبسبب هذا النقص، أصبح واضحا – في صناعة الشبكات – ضرورة الحاجة الماسة لوجود نظام قياسي. وبالتالي فإن جمعية تطوير الشبكات قد قامت بتطوير بروتوكول تم تصميمه خصيصا لإدارة الشبكة، وهو بروتوكول إدارة الشبكة البسيط Simple Network Management Protocol (SNMP). وقد صدر منه ثلاثة إصدارات Versions هي:

SNMPv1, SNMPv2, SNMPv3. ويقوم هذا البروتوكول بتوفير وسائل للحصول على المعلومات وكذلك إعطاء التعليمات لأجهزة الشبكة. وهذا البروتوكول متوافق مع النموذج المرجعيOpen Systems Interconnection (OSI) ، الذي يتكون من سبعة مستويات والذي تم تطويره من قبل الهيئات ISO, CCITT .

أسئلة تقويم ذاتي

اشرح، مع إعطاء مثال توضيحي، نظام القائمة المشتقة لتجميع البيانات عن بعد.

قارن بين طريقة القائمة المشتقة، وطريقة بينية الأمر الخطي.

اذكر بعض عيوب هذين الطريقتين.

اختر الإجابة الصحيحة للجمل التالية :

من عيوب طريقة استخدام الأمر ping في اختبار توصيلة جهاز متصل بالشبكة عن بعد ما يلي:

أ- أنه لا يعتمد عليها في توصيل الرسائل.

ب- تحتاج لإجراء عملية التصويت polling.

ج- توفر معلومات محدودة.

د- كل ما سبق.

هـ- لا شيء مما سبق.

2. تطوير البروتوكولات القياسية لإدارة الشبكات

إن الأمثلة والمشاكل التي تم مناقشتها في الفقرات السابقة، لا تحقق العدالة بخصوص المسائل المتعلقة بإدارة شبكات البيانات المركبة. حيث إنها تستبعد احتمال أن أي شبكة بيانات ينبغي أن تبنى كلية من منتجات يتم توفيرها بواسطة شركة تصنيع واحدة. أخيرا، فإن الحاجة يمكن أن تتزايد لمنتجات شبكية مثل المجمعات Hubs، والجسور Bridges، والموجهات Routers، والحاسبات المضيفة Hosts، من العديد من الشركات. وأنه ينبغي على مهندس الشبكة أن يخطط للتغيرات والنمو الذي قد يحدث للشبكة.

لقد أظهرت بروتوكولات إدارة الشبكة الحاجة لتوفير طريقة موحدة للوصول إلى أي جهاز شبكة يتم تصنيعه من قبل أي مصنع لتوفير مجموعة من القيم القياسية. إن

الاستفسارات queries عن أجهزة الشبكة ينبغي أن تشمل الآتي:

- اسم الجهاز.
- الإصدار البرمجي في الجهاز.
- عدد الوحدات البينية interfaces في الجهاز.
- عدد الحزم في الثانية للوحدة البينية للجهاز.

وأن معامِلات الإعداد settable parameters لأجهزة الشبكة ينبغي أن تشمل على الآتي:

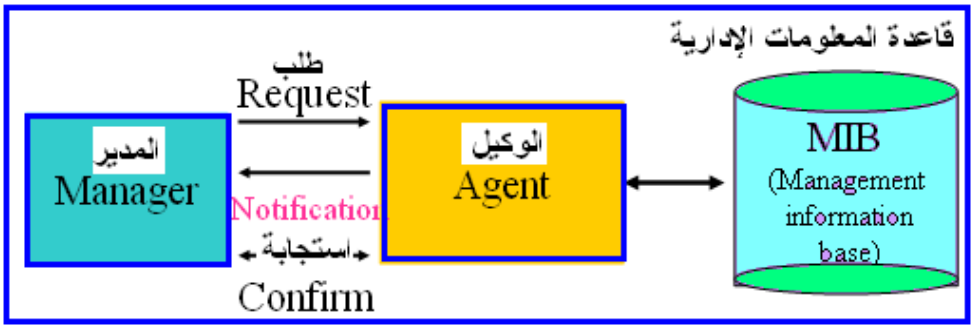
- اسم الجهاز.
- عنوان الوحدة البينية للشبكة.
- الحالة التشغيلية للوحدة البينية للشبكة.
- الحالة التشغيلية للجهاز.

كما توفر البروتوكولات القياسية لإدارة الشبكة فوائد إضافية أخرى مثل توفير إظهار بيانات موحدة يتم إرسالها وإرجاعها بواسطة أجهزة الشبكة.

3. بروتوكول إدارة الشبكة البسيط (الإصدار الأول SNMPv1)

إن بروتوكول إدارة الشبكة البسيط الإصدار الأول SNMPv1 (سوف نطلق عليه الاسم "سنمب–ف1")، هو بروتوكول قياسي تم تطويره لإدارة مراكز اتصالات شبكة البيانات. وهو أكثر بروتوكولات الشبكات شهرة واستخداما في إدارة العديد من الشبكات، وقد تم تصميمه للعمل في المستوي التطبيقي Application Layer، وذلك لتسهيل تبادل المعلومات الإدارية بين أجهزة الشبكة. ويشمل ذلك إدارة أجهزة الخادم – محطة العمل – الموجهات – مفاتيح الاتصال – المجمعات Hubs – وغيرها. حيث يمكن البروتوكول "سنمب" مهندس الشبكة من إدارة أداء الشبكة، وحل مشاكلها، والتخطيط لتوسعة وتطوير الشبكة.

يعتمد بروتوكول "سنمب–ف1" في عمله على استخدام نموذج "المدير/الوكيل" Manger/Agent Model الذي يتكون من ثلاثة أجزاء هي المدير، والوكيل ، وقاعدة المعلومات الإدارية MIB، كما هو موضح في الشكل1.3.



شكل 1.3 نموذج "المدير/الوكيل" **Manger/Agent Model** للبروتوكول **SNMP**.

1.3 طريقة عمل نموذج "المدير/الوكيل"

أولا: المدير

يمكن أن يكون المدير جزءاً من نظام إدارة الشبكة، ويمكن أن يكون الوكيل موجوداً داخل جهاز الشبكة (مثل الموجهrouter). يستطيع المدير الحصول على قيمة (أو تخزين قيمة) من الوكيل. عندما يتم تهيئة البروتوكول "سنمب" لإدارة موجه الشبكة فإن الوكيل يستطيع أن يستجيب للاستفسارات المتعلقة بقاعدة المعلومات الإدارية MIB التي يتم إرسالها بواسطة نظام إدارة الشبكة. يستخدم نظام إدارة الشبكة برامج إدارة الشبكة لضبط متغيرات الأجهزة وإجراء عملية التصويت للحصول على معلومات محددة. واستخدام نتائج عملية التصويت ورسمها وتحليلها لمساعدة مهندس الشبكة في حل المشاكل المتعلقة بتشخيص الأعطال وزيادة كفاءة أداء الشبكة والتحقق من تهيئة الأجهزة ورصد أحمال حركة مرور الرسائل داخل شبكة البيانات.

ثانيا: الوكيل

يقوم الوكيل بتجميع البيانات من قاعدة المعلومات الإدارية، والتي تمثل مستودع repository معلومات عن معاملات تشغيل الأجهزة وشبكة البيانات. كما يستطيع أيضا

أن يرسل رسائل Traps ليبين وقوع أحداث معينة وتبليغها إلى المدير.

جدول 1.1

أنواع الرسائل المستخدمة في بروتوكول "سنمب" ووظائفها

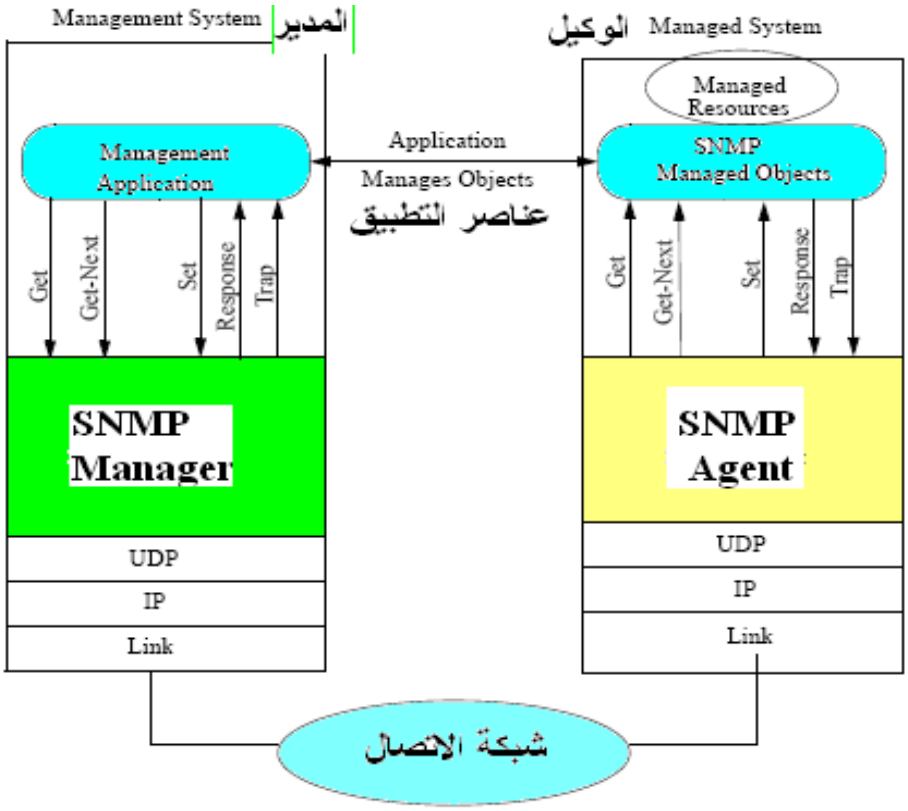
مسمى الرسالة	الوظيفة
Get-Request طلب أو رجاء	استرجاع قيمة لمتغير معين
Get-Next-Request طلب الرجاء التالي	استرجاع القيمة التالية لمسمى المتغير*
Get-Response طلب استجابة	استجابة طلبات الرجاء السابقة التي يتم إرسالها بواسطة نظام إدارة الشبكة
Set-Request	تخزين قيمة في متغير محدد
Trap	رسالة ترسل من الوكيل إلى المدير لبيان وقوع حدث معين

* غالبا تستخدم لاسترجاع المتغيرات من جدول

2.3 أنواع الرسائل والحصول على المعلومات وضبطها

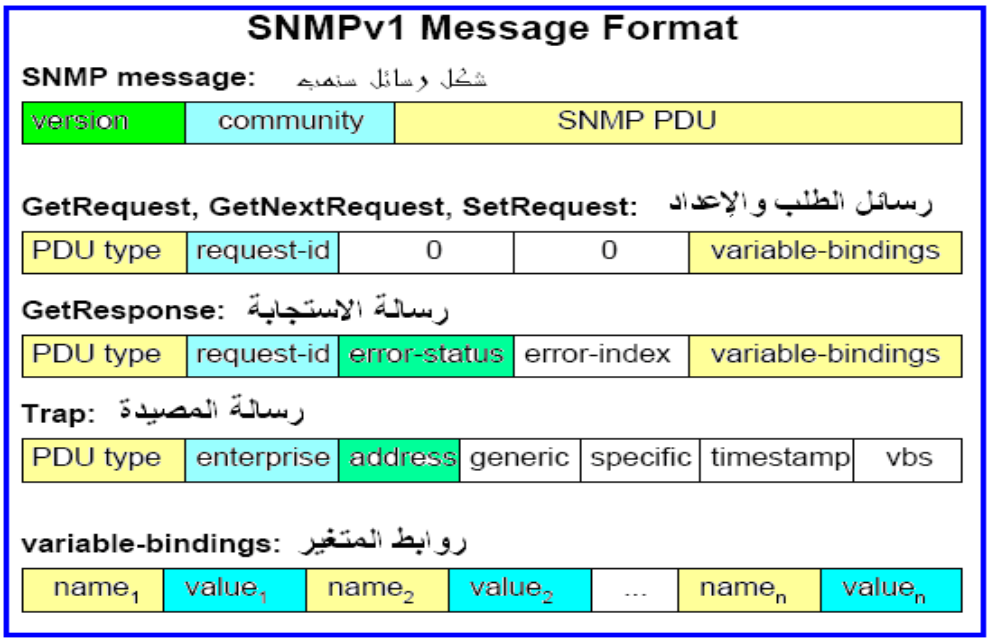
يقوم البروتوكول "سنمب- ف1" بتأدية وظائفه مستخدما خمسة أنواع من الرسائل القياسية المبينة في الجدول 1.1. ترسل الرسالة على شكل حزمة بيانية packet بين المدير والوكيل. تحتوي كل حزمة بيانية على جزء من البيانات يسمى بوحدة بيانات البرتوكول PDU (Protocol Data Unit). يستخدم سنمب بروتوكول داتاجرام للمستخدم UDP في المستوى الرابع، أو بروتوكول النقل. يتيح بروتوكول UDP خدمة عدم الربط connectionless (حيث إن رسالة داتاجرام بها عنوان المرسل والمستقبل، وبيانات تحديد المسار)، لذلك فإن بروتوكول سنمب ليس مجبرا بصيانة روابط الاتصال بين الوكيل والمدير من أجل إرسال الرسائل. يتيح بروتوكول UDP خدمة مستوى نقل

سريعة بأقل كمية من تخصيص المصادر resource allocation. لكنه لا يوفر طريقة اتصال معتمدة Reliable لتبادل الرسائل بين الوكيل والمدير. يوضح الشكل 1.4 النموذج المرجعي TCP/IP لبروتوكول "سنمب".

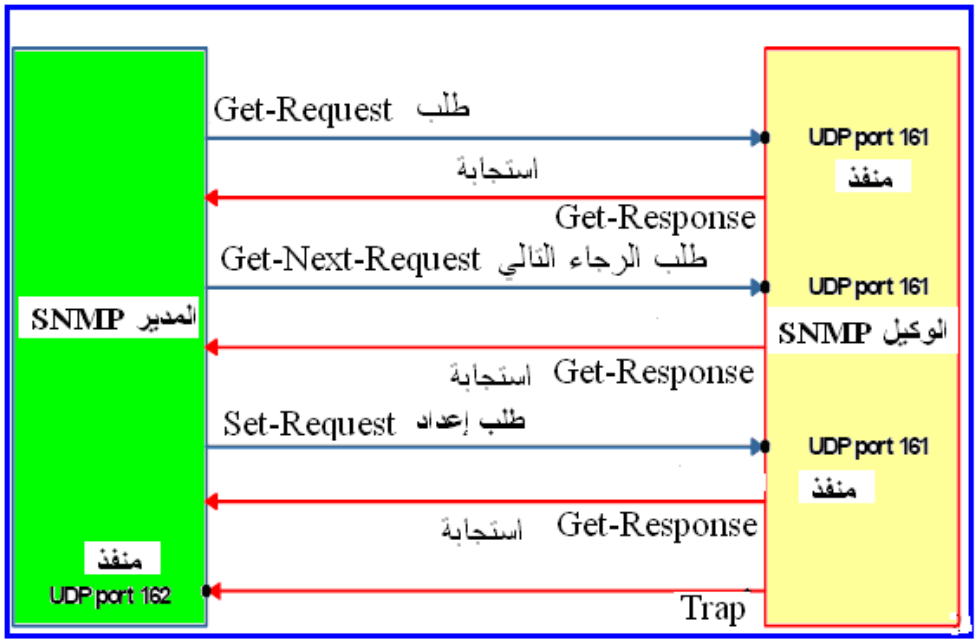


الشكل 1.4 النموذج المرجعي TCP/IP لبروتوكول "سنمب".

يوضح الشكل1.5 شكل رسائل سنمب- ف1. كما يوضح الشكل1.6 أنواع الرسائل المتبادلة بين المدير والوكيل.



الشكل1.5 شكل رسائل سنمب–ف1.



الشكل1.6 أنواع الرسائل المتبادلة بين المدير والوكيل.

1.2.3 استخدامات الرسائل القياسية لبروتوكول "سنمب– ف1"

- رسالة **Get-Request**:

يستخدم المدير "سنمب" رسالة Get-Request لاسترجاع معلومات من جهاز الشبكة الذي يوجد به الوكيل، لاسترجاع معلومات عن عنصر معين في الشبكة. يقوم الوكيل بدوره بإرسال استجابة بواسطة إرسال رسالة Get-Response. يمكن أن تشتمل هذه الاستجابة على اسم النظام، مدة بقاء النظام في التشغيل، وعدد وحدات الشبكة البينية الموجودة في النظام.

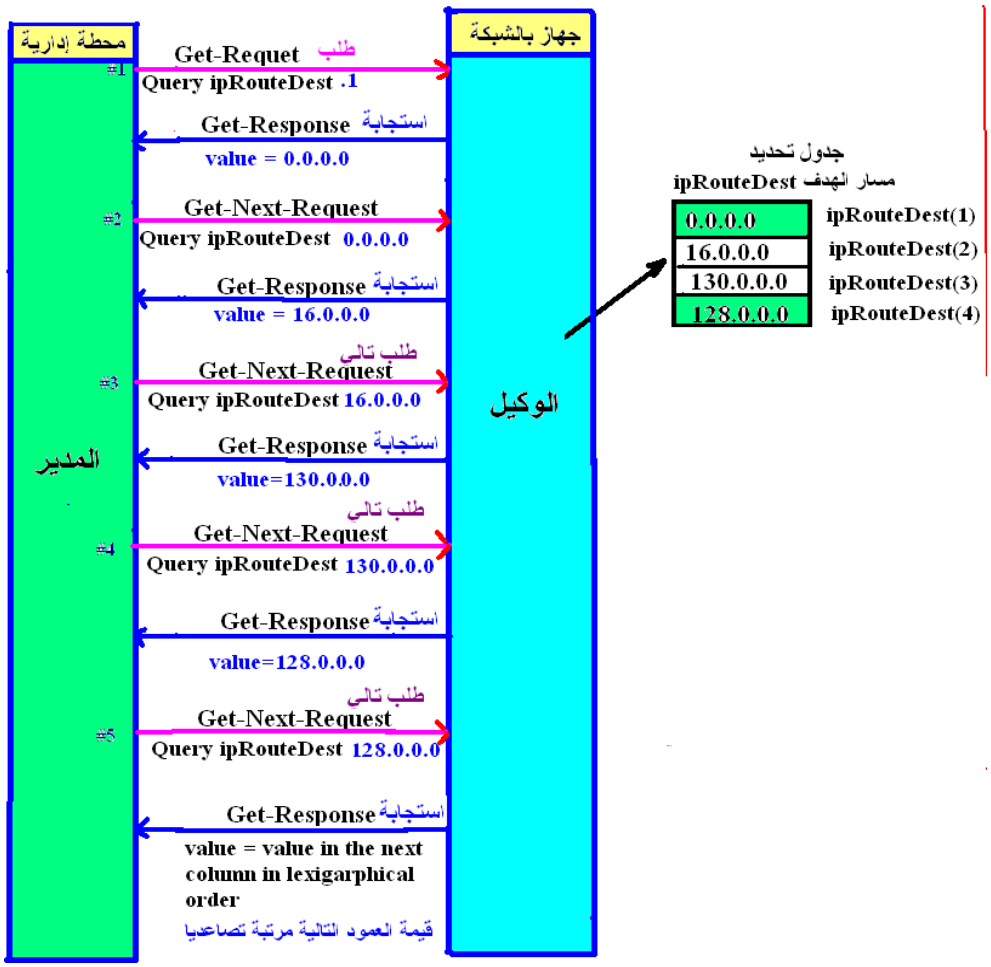
- رسالة **Get-Next-Request**:

تستخدم رسالة Get-Next-Request للحصول على جدول من العناصر، أو للسؤال عن عنصر محدد تالٍ في جدول البيانات. باستخدام هذه العملية، فإن المدير لا يحتاج أن يعرف اسم المتغير المطابق. حيث يتم إجراء عملية بحث متتالي لإيجاد المتغير المطلوب من قاعدة البيانات الإدارية MIB . يقوم الوكيل بالاستجابة إلي رسالة Get-Next-Request بواسطة إرسال رسالة Get-Response.

مثال تطبيقي: الاستفسار عن معلومات من جدول تحديد المسار في الشبكة:

يمكن استخدام نظام إدارة الشبكة للاستفسار عن جدول تحديد المسار IP Routing لجهاز متصل بالشبكة. حيث إن جدول تحديد المسار يتغير بطريقة ديناميكية، لهذا لا نعرف بالضبط عدد الصفوف الموجودة بهذا الجدول. لإيجاد القيمة في عمود الجدول المقابل لكل صف في الجدول، فإن المدير "سنمب" يرسل رسالة Get-Request إلى الوكيل في الجهاز المتصل بالشبكة، ويسأل عن العنصر الموجود في الصف الأول في الجدول. يتم اتباع هذه الرسالة برسائل Get-Next-Request بطريقة متتابعة "يطلق عليها "Lexigraphical order" (هي طريقة للبحث عن المعلومات بطريقة متتالية تنازليا أو تصاعديا)، لاسترجاع قيمة العمود التالي، حتى يتم الوصول إلى نهاية الجدول. وتحدد الأعمدة في جدول المسارات "مسار الهدف" IP Route Destination

وهو عنوان الحاسب المضيف ، أو عنوان جزء من الشبكة الفرعية subnet ، أو رقم الشبكة المدون في جدول مسارات ربط الشبكة. يوضح الشكل1.7 الاستفسارات المتتابعة التي يرسلها المدير إلى الوكيل لهذا العنصر.



الشكل1.7استخدام رسالة **Get-Next-Request** لاستعراض جدول بترتيب تصاعدي **Lexigraphical order**.

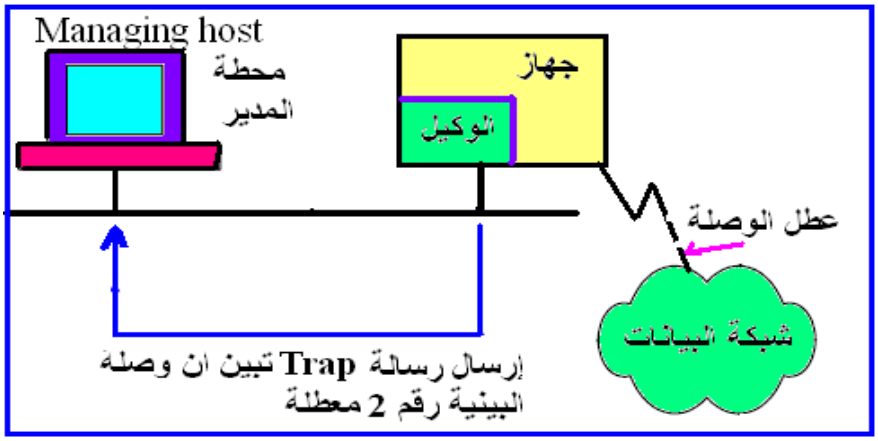
- رسالة **Set-Request**:

تسمح رسالة Set-Request بإجراء عمليات التهيئة عن بعد لمعاملات تشغيل أجهزة الشبكة. على سبيل المثال، يمكن أن تشمل رسائل Set-Request ضبط اسم الجهاز ،

غلق الوحدة البينية الإدارية، أو مسح عنوان خاص Address Resolution Table Entry . في هذا المثال، يستخدم نظام إدارة الشبكة الرسائل Get-Request ، Get-Next-Request لتحديد عدد الوحدات البينية interfaces لجهاز معين. عندما يقوم النظام بفحص حالة كل وحدة بينية، فإنه يستطيع معرفة أي وحدة منها لا تعمل. بواسطة مقارنة معاملات تشغيل الجهاز مع المعاملات المخزنة في الجدول الداخلي في قاعدة المعلومات الإدارية MIB؛ فإن النظام يستطيع أن يعرف أن الوحدة البينية العاطلة عن العمل يكون بسبب أن لها عنواناً غير صحيح. يمكن للنظام بعد ذلك استخدام رسالة Set-Request كي يغير عنوان الوحدة البينية لمحاولة إرجاعها إلى حالة التشغيل.

- رسالة **Trap**:

إن رسالة SNMP Trap هي رسالة تطوعية Unsolicited يقوم الوكيل بإرسالها إلى المدير، لإعلام الخادم بوقوع حدث معين. مثلا، يمكن استخدام رسالة Trap لإعلام نظام إدارة الشبكة عن حدوث عطل في الدائرة الكهربية بالجهاز، أو أن مساحة التخزين بقرص الجهاز المتصل بالشبكة أوشك على الامتلاء، أو أن أحد المستخدمين قد تم دخوله للتو على جهاز الحاسب المضيف. ينبغي أن يتم ضبط عنوان محطة الوكيل كي يعرف مكان إرسال رسائل traps. يوضح شكل1.8 كيفية التعامل بين المدير وبين الوكيل مع الجهاز الذي يقوم بإرسال رسالة SNMP Trap.



شكل1.8 إرسال رسالة trap إلى المضيف الإداري تبين وجود عطل وصلة.

2.2.3 أنواع رسائل SNMP Traps

يوجد سبعة أنواع من رسائل SNMP Traps يتم تعريفها كجزء من قاعدة المعلومات الإدارية MIB II. يوضح الجدول1.2 مسميات أنواع هذه الرسائل، ووظيفة كل نوع منها.

الجدول1.2

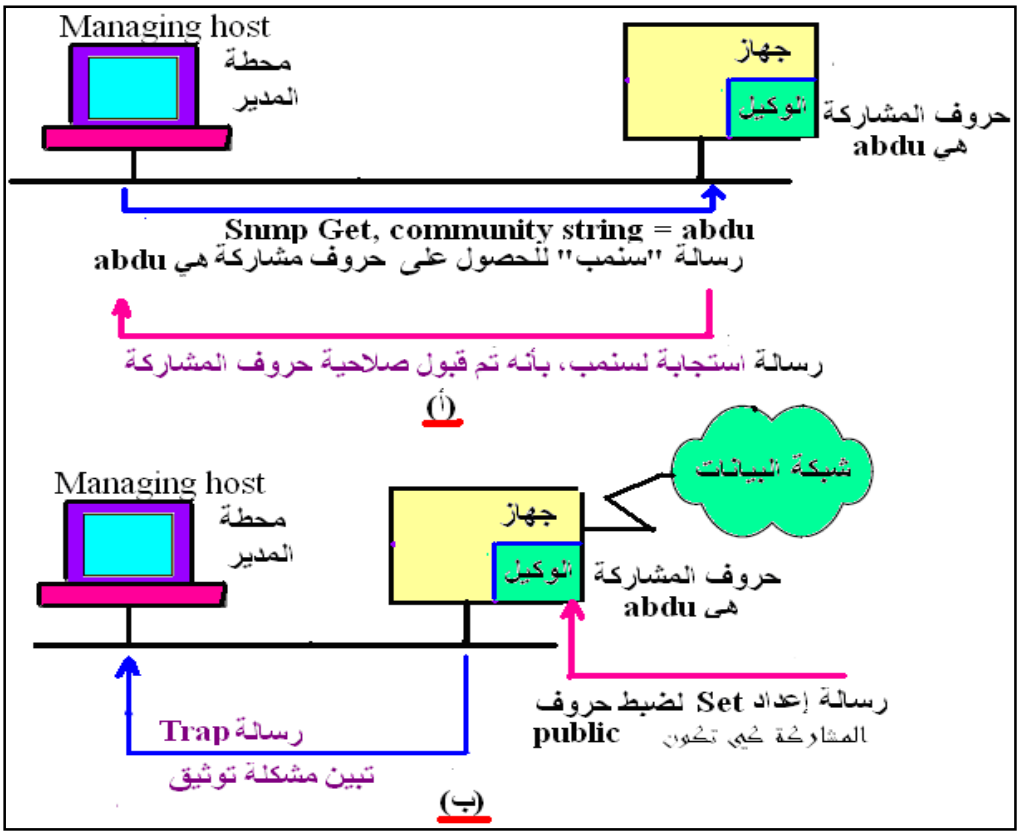
نوع ومسمي رسالة trap	الوظيفة التي تؤديها
Cold start التشغيل البارد	يتم إرسالها عند بدء تشغيل الجهاز. وهي تبين أن الوكيل يرسل إشارة trap لإعادة بدء تشغيل نفسه كما في حالة التهيئة configuration، أو أن تنفيذ البروتوكول قد تغير.
Warm start التشغيل الدافئ	عندما يقوم الوكيل Snmp في جهاز الشبكة بعملية إعادة التشغيل reset، فإن ذلك يؤدي إلى إصدار رسالة warm start trap، ويحدث هذا عادة بسبب تدخل يدوي. وتبين رسالة warm start trap أن الجهاز الذي يرسل هذه الرسالة يقوم بإعادة بدء تشغيل نفسه دون تغير التهيئة، أو تغير تنفيذ البروتوكول.
Link down الوصلة معطلة	تبين وقوع عطل وصلة معينة في جهاز المنبع.
	تبين إتمام إصلاح وصلة معينة في جهاز المنبع.
Authentication failure عطل توثيق	يتم إرسالها إلى نظام إدارة الشبكة، عندما يقوم

	الوكيل SNMP بالتحقق من أن طلب الرجاء request ليس به توثيق صحيح. مثال: إذا قام الوكيل بإرسال رسالة بها خطأ في الشكل string، يمكن لهذه المعلومات أن تطلب تنفيذ إدارة الأمن security management.
EGP neighbor loss فقد برتوكول مجاور	تستخدم بواسطة الوكيل SNMP لتدوين فقدان في EGP neighbor . يستخدم البروتوكولEGP بين شبكات البيانات. سيتم شرحه فيما بعد في وحدات الكتاب.
Enterprise specific تحديد مؤسسة	هي رسالة يتم بناؤها بواسطة المصنع لتوفير وظائف إضافية عمومية. وذلك لتبيان معدلات الاستخدام outnumbers بقيم متعددة. مثل: استخدامات القرص في محطة العمل، العدد الأكبر للمستخدمين، الحمل العالي للمعالج، وهكذا. تستطيع أجهزة الشبكة المختلفة إرسال traps بناء على المعدل العالي للاستخدام utilization، معدلات الخطأ الموجودة بوصلات الشبكة، أو أعطال منبع القدرة الزائد.

3.3 الأمن Security في البروتوكول "سنمب–ف1"

يستطيع الوكيل SNMP agent في جهاز الشبكة أن يطلب من المدير SNMP manager إرسال كلمة سر معينة مع كل رسالة. يقوم الوكيل بعد ذلك بالتحقق من قاعدة المعلومات الإدارية MIB عن توثيق عملية السماح بالاتصال. ويطلق على كلمة

السر هذه مسمى "حروف المشاركة" Community String. يوضح شكل1.9 كيفية تفاعل الوكيل لاستقبال "حروف مشاركة" صالحة أو غير صالحة.



شكل1.9 كيفية تفاعل الوكيل لاستقبال "حروف المشاركة".

(أ): حروف مشاركة صالحة Valid.

(ب) حروف مشاركة غير صالحة Invalid.

يمكن بناء وتنفيذ وكلاء "سنمب" كي تسمح بمستويات أمن مختلفة باستخدام "حروف المشاركة". مثال، يمكن للوكيل أن يحدد "حروف المشاركة" كي يسمح لرسائل Get-Request، Get-Next-Request من مجموعة من المديرين بأن تتصل للقراءة فقط للمعلومات الموجودة في قاعدة المعلومات الإدارية MIB. يمكن أيضا للوكيل أن يحدد "حروف المشاركة" للرسائل Set-Request، Get-Next-Request، Get-Request،

لمجموعة أخرى من المديرين بالوصول إلى الوكلاء وإتمام عمليات كاملة للقراءة والكتابة للمعلومات الموجودة في قاعدة المعلومات الإدارية MIB.

يتم إرسال "حروف المشاركة" من خلال حزم بيانات بروتوكول "سنمب" على شكل شفرة أسكي ASCII بصيغة واضحة. يستطيع المستخدم بقليل من الجهد تعلم "حروف المشاركة" المستخدمة بواسطة الوكيل "سنمب".

4.3 بعض مشاكل البروتوكول "سنمب–ف1"

على الرغم من كفاءة البروتوكول "سنمب–ف1" في إدارة الشبكة، لكن يوجد به ثلاث مشاكل هي:

- بروتوكول قياسي للاستخدام، فقط لشبكات IP.
- غير كفء في حالة استرجاع المعلومات من الجداول الكبيرة.
- يستخدم كلمات نصية واضحة للأمن، مما يجعلها نسبيا غير آمنة.

- المشكلة الأولى:

يمكن حل المشكلة الأولي بواسطة استخدام وكلاء معاونين SNMP Proxy Agents تقوم بتجميع المعلومات من أجهزة الشبكة التي لا تتعامل مع شبكات IP ويحولها إلى معلومات يمكن إدارتها بواسطة المدير "سنمب–ف1". يوضح الشكل1.10 استخدام وكيل مساعد لتحويل بروتوكول النقل من سنمب فوق يعمل على TCP/IP إلى سنمب فوق بروتوكولات IPX,OSI .

الشكل1.10

وبذلك يمكن إدارة أجهزة الشبكات التي لا تتعامل مع IP ، و أن تدار بواسطة البروتوكول "سنمب–ف1". ويتطلب ذلك كتابة برامج خاصة تكتب لكل جهاز شبكة يستخدم لوكلاء SNMP proxy.

- المشكلة الثانية:

المشكلة الثانية في البروتوكول "سنمب–ف1" هي أنه غير كفء في استرجاع البيانات من الجداول الضخمة. مثال: بفرض أننا نريد أن نحصل على جدول له 2000 سجل دخول للحسابات من الجهاز. فإن كل صف في جدول الحسابات يكون له أربعة مداخل entries، هي عنوان المصدر، عنوان الهدف، حرف العد byte count، وحزمة العد packet count. باستخدام الرسائل Get-Next-Request، في حالتها الأحسن (عدم إعادة إرسال)، سوف نحصل على 2 * 4 * 2000 = 16,000 حزمة بيانات packets.

تم حساب هذه القيمة بواسطة ضرب عدد أربعة رسائل "رجاء request" لكل صف في 2000 صف، ثم ضرب الناتج في عدد رسائل Get-Request, Get-Response المصاحبة لهذه العملية. عندما يقوم المدير بطلب الأربعة بنود كلها لكل صف في حزمة البيانات الواحدة، فإن إجمالي عدد حزم البيانات يساوي 2000 * 2 = 4000 حزمة بيانات في الشبكة. حتى مع هذا العدد القليل الملحوظ في حركة حزم البيانات، فإن الوكيل "سنمب" الموجود في جهاز الهدف يظل عليه أن يحقق 16,000 عملية بحث look ups في جدول الحسابات Accounting Table.

- المشكلة الثالثة:

هي استخدام البروتوكول "سنمب–ف1" حروف مشاركة Community String نصية صريحة للأمن. يستطيع أحد المستخدمين قراءتها. وإذا حدث ذلك يستطيع هذا الشخص تغيير تهيئة أجهزة الشبكة التي يستخدمها البروتوكول "سنمب–ف1" وذلك باستخدام رسالة SNMP Set-Request.

أسئلة تقويم ذاتي

عدد خصائص بروتوكول SNMPv1.

أكمل ما يلي :

يعتمد بروتوكول إدارة الشبكة البسيط SNMP على استخدام نموذج يسمى..... وهذا النموذج يتكون من ثلاثة أجزاء هي: ..... ، ..... ، ..... .

ما هي مشاكل بروتوكول SNMPv1.

يبين الجدول التالي أنواع الرسائل المستخدمة في بروتوكول SNMPv1 ووظائفها. قم بتوفيق مسميات الرسائل مع ما يقابله من الوظائف :

رقم	نوع الرسالة	وظيفتها	رقم الإجابة
1	Get - Request	تخزين قيمة لمتغير	
2	Get –Next - Request	بيان وقوع حدث معين	
3	Get – Response	استرجاع قيمة لمتغير	
4	Set - Request	استرجاع القيمة التالية لمتغير	
5	Trap	استجابة طلبات الرجاء السابقة	

ما وظيفة رسالة المصيدة Trap؟

اذكر خمسة أنواع من رسائل المصيدة، موضحاً وظيفة كل منها.

ما حروف المشاركة Community String ؟

كيف تستخدم حروف المشاركة في تحقيق الأمن ؟

4. الإصدار الثاني للبروتوكول "سنمب" SNMPv2

يؤدي الإصدار الثاني للبروتوكول "سنمب" الذي سوف نرمز له بالاسم "سـنمب–ف2" ، نفس الوظائف الأساسية التي يؤديها الإصدار الأول للبروتوكول "سنمب–ف1" التي تـم شرحها سابقا، والخاصة بالاستفسار وتغيير البيانات في قاعدة المعلومات الإدارية عـن أجهزة الشبكة. وقد تم تطوير هذا الإصدار كي يتغلب على المشاكل التي يعـاني منهـا الإصدار الأول للبروتوكول "سنمب–ف1". ويتميز الإصدار الثاني للبروتوكول "سنمب–ف2" بعدة خصائص هي:

1. يوجد به إضافات لتحسين هيكل المعلومات الإدارية "SMI".
2. يوجد به أنواع جديدة من الرسائل.
3. يدعم بروتوكولات متعددة قياسية.
4. تحسين الأمن بفعالية عالية significantly.
5. يوجد به عناصر لقاعدة معلومات إدارية جديدة.
6. يمكن أن يتعاون مع الإصدار الأول للبروتوكول "سنمب–ف1".

1.4 تحسين هيكل المعلومات الإدارية "SMI"

إن هيكل المعلومات الإدارية "SMI" القياسية المستخدم في الإصدار الأول للبروتوكـول "سنمب–ف1" يوجد به بعض العيوب drawbacks. من ضمن هذه العيـوب أنـه يـتم تمثيل الرمز بعدد طوله 32 معلومة bit ، ولهذا فإن هذا البروتوكـول يحتـوي علـى أقصى قيمة عدد صحيح "غير رمزي unsigned" تكون قيمتـه تسـاوي " $2^{32}-1$" ، ولا يميز بين الأعداد الصحيحة "الرمزية signed" وغير رمزية "unsigned"، وهو يستخدم فقط للتعبير عن عنوان الشبكات التي تستخدم بروتوكول IP. بينمـا الإصـدار الثـاني

للبروتوكول "سنمب–ف2" يسمح لأعداد صحيحة طولها 64 معلومة bits، وبذلك تـزداد القيمة العظمى للأعداد الصحيحة غير رمزية "unsigned لتصبح قيمتهـا " $2^{64}-1$ " ، ويطلق عليها اسم 64 counter . وتكون هذه القيمة كبيرة وكافية للتعامل مع معلومـات العد information count والتي تسبب مشـاكل فـي الإصـدار الأول للبروتوكـول "سنمب–ف1" (حيث إنه يخصص 32 bits لتمثيل طول الرمز).

مثال: نفترض وحدة بينية لبيانات الألياف الضوئية الموزعة FDDI لشبكة حلقية Ring سرعتها 100 ميجا بايت. وأن بها قاعدة معلومات إدارية MIB، ونريد حساب عـدد العناصر لمعرفة عدد الحروف. نفرض أن متوسط معدل الاسـتخدام utilization فـي الحلقة هو 30% ، وأن 32 معلومة bits سـوف تسـتغرق دورة wrap حـوالي 19 دقيقة.

- خطوات الحل:

(1) 30% of 100 Mbits / second = 30 Mbits / sec

= 30 x 1024 x 1024 = 3,750,000 bytes/sec.

(2) $2^{32} - 1 = 4,294,967,295$ bytes

4,294,967,295 bytes / 3,750,000 bytes/sec = 1145 seconds

1145 seconds / 60 seconds (minute) = 19.09 minutes

باستخدام bits 64 عدد صحيح غير رمزي unsigned لإجراء عملية العد، فإن العداد يستغرق حدوث دورة زمنية مدتها تساوي

(3) 82,000,000,000 minutes

30% of 100 Mbits / second = 30 Mbits / sec

= 3,750,000 bytes/sec.

(4) $2^{64} - 1 = 1.8446744E19$ bytes

(5) 1.8446744E19 bytes / 3,750,000 bytes/sec = 4.92×10^{12} sec

4.92×10^{12} sec / 60 seconds (minute) = 8.20×10^{10} minutes.

- **حل المشكلة الأولي لبروتوكول سنمب–ف1:**

تحتاج قاعدة المعلومات الإدارية MIB التي تستخدم الإصدار الثاني للبروتوكول "سنمب–ف2" لكي تقوم بتنفيذ عنصر طوله 64 bit عداداً صحيحاً و ذاكرة حجمها ضعف الذاكرة المستخدمة في حالة قاعدة المعلومات الإدارية، التي يستخدمها الإصدار الأول للبروتوكول "سنمب–ف1"، والذي يستخدم عنصر ذاكرة طوله 32 بيت لتمثيل الأعداد الصحيحة اللازمة للعناوين. وهذا قد يسبب مشكلة خاصة لبعض الوحدات البينية التي قد يكون بها ذاكرة محدودة ، مثل أجهزة المودم وبطاقات وحدات المواجهة interface boards . لهذا السبب فإن العديد من قواعد المعلومات الإدارية القياسية تستخدم أعداداً محدودةً فقط من العناصر ليتم تمثيلها بأعداد صحيحة طولها 64 خانة.

- **حل المشكلة الثانية لبروتوكول سنمب–ف1:**

إن هيكل المعلومات الإدارية SMI للإصدار الأول للبروتوكول "سنمب–ف1" هي عدم المقدرة على تعبير عن كل من الأرقام الرمزية signed وغير الرمزية unsigned. إن المعلومة الرمزية sign bit في الأعداد الثنائية يمكن أن تستخدم للتعبير عن الأعداد الموجبة أو السالبة أو ربما تستخدم كمعلومة إضافية لاقتناء القيم (وذلك لزيادة القيمة العظمى للعدد). على سبيل المثال، إن العدد الصحيح غير الرمزي الذي طوله 32 خانة، يمكن أن يعبر عن قيمة عظمى $(2^{32} - 1)$ وهذه القيمة العددية تكافئ (4,294,967,295). وأن العدد الصحيح الرمزي signed يمكن أن يعبر عن قيمة عظمى $(2^{31} - 1)$، وهي تكافئ القيمة العددية 2,147,483,647 . عندما تحتاج عناصر قاعدة المعلومات الإدارية MIB أن تعبر فقط عن قيمة صحيحة موجبة، فإن المعلومة الرمزية sign bit يمكن أن تستخدم لزيادة عدد المعلومات للتعبير عن هذه القيمة.

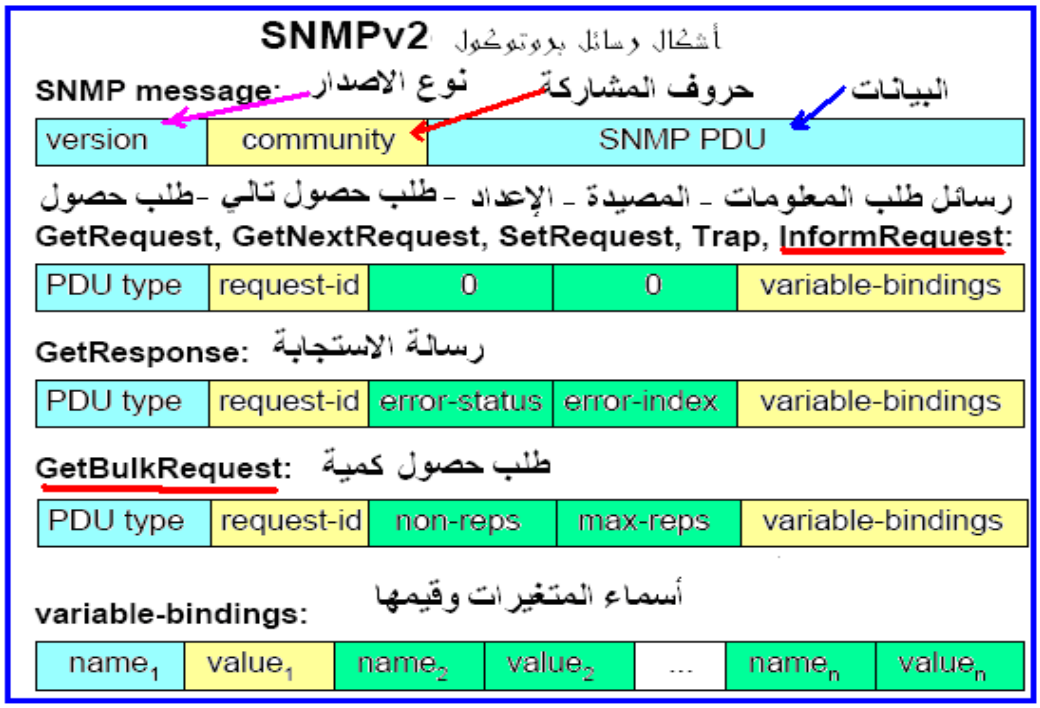
يتميز الإصدار الثاني للبروتوكول "سنمب–ف2" بأنه أضاف لهيكل المعلومات الإدارية SMI نوع بيانات Data Type جديداً لتمثيل نقط اتصال الخدمة الشبكية للعناوين Network Service Access Point (NSAP). وهو عنوان شبكي هرمي Hierarchical، يستخدم بواسطة مستويات الشبكة المتوافقة مع النظام OSI.

2.4 أنواع الرسائل و ضبط المعلومات والحصول عليها

تستخدم الأنواع المتعددة للرسائل الموجودة في الإصدار الأول للبروتوكول "سنمب–ف1" مع الإصدار الثاني. أحد الاختلافات الأساسية بين هذين البروتوكولين هو أن الإصدار الأول يستخدم شكل رسالة واحداً لكل الرسائل ماعدا الرسائل Traps، Get-Response، بينما الإصدار الثاني يستخدم شكل رسالة مميزاً لكل الرسائل ماعدا الرسائل Get Response, Get Bulk Request. الفرق الآخر بين الإصداران هو في كيفية تعامل كل إصدار في إنشاء جداول البيانات ورسائل الخطأ.

1.2.4 أنواع الرسائل في البروتوكول SNMPv2

يوجد نوعان جديدان من الرسائل التي يستخدمها الإصدار الثاني للبروتوكول "سنمب–ف2"، هما: InformRequest, GetBulkRequest . كلاهما يؤدي وظائف قيمة للوكيل والمدير. إن أسماء أنواع الرسائل في الإصدار الأول للبروتوكول "سنمب–ف1" يتم توصيلها بواسطة شرطة Hyphenated بين الكلمات. بينما في الإصدار الثاني فإن أسماء الرسائل تكتب بدون وصلات بين الكلمات. يوضح الشكل 1.11 شكل هذه الرسائل، ونشرح فيما يلي وظائفها بالتفصيل.



الشكل 1.11

(أ) رسالة InformRequest:

يتم إرسال رسالة InformRequest من مدير لمدير آخر. ويسمح ذلك لأحد التطبيقات الإدارية بأن ترسل معلومات إلى مدير آخر، وذلك بهدف تحقيق اتصال بين مديرين في الشبكة. وتتيح رسالة InformRequest طريقة قياسية لإجراء عمليات الاتصال للنظم الإدارية في الشبكات الهرمية أو الموزعة. حيث يمكن للمؤسسة أن تختار نظام الإدارة الهرمي أو نظام الإدارة الموزع، لتوزيع إنذارات alarms الشبكة، وإجراء عمليات التصويت Polling، وتقسيم إدارة الأجهزة المختلفة بين النظم. كما يمكن أن تسمح لمديرين متعددين لإجراء عملية التهيئة، أو تغيير خريطة الشبكة في نفس التوقيت simultaneously. وقبل أن يصدر الإصدار الثاني وكذلك رسالة InformRequest ، كانت معظم الاتصالات بين تطبيقات نظام إدارة الشبكة تتم بواسطة وسائل أخرى خاصة.

(ب) رسالة **GetBulkRequest** :

تستخدم رسالة GetBulkRequest للمساعدة في تحسين عملية استرجاع كمية كبيرة من المعلومات الإدارية MIB، وهى بذلك تحل أحدي المشاكل المتعلقة بالإصدار الأول للبروتوكول "سنمب–ف1". إن التطبيق الذي يستخدم الإصدار الأول للبروتوكول "سنمب–ف1" الذي يتطلب استرجاع كمية كبيرة من المعلومات الإدارية، كان يستخدم رسالة Get-Next-Request بطريقة مجهدة، بواسطة إرسال طلب استرجاع معلومات لكل عنصر. ويعمل الأمر GetBulkRequest بنفس الطريقة التي يعمل بها الأمر Get-Next-Request لاسترجاع القيمة التالية من قاعدة المعلومات الإدارية MIB ، وذلك عندما يستعرض traversing قاعدة المعلومات الإدارية بطريقة منتظمة in order. لكن باستخدام الأمر GetBulkRequest، يستطيع البروتوكول "سنمب–ف2" طلب استرجاعات متعددة للعنصر، وذلك بإرسال رسالة واحدة فقط. وأن كل استرجاع retrieval يمثل القيمة التالية للعنصر، كلما تم استعراض شجرة قاعدة المعلومات الإدارية. فبدلا من السؤال عن قيمة العنصر التالي في الجدول، يمكن للبروتوكول أن يسأل عن مجموعة قيم "س" في الجدول ، حيث "س" هي أي قيمة عددية صحيحة. تقوم الرسالة GetBulkRequest باسترجاع أكبر قدر ممكن من المعلومات من قاعدة المعلومات الإدارية بواسطة طلب معين. بالإضافة إلى ذلك يمكن للبروتوكول "سنمب–ف2" أن يطلب قيمة واحدة لمجموعة عناصر، يتم طلبها بواسطة الرسالة GetBulkRequest .

تطبيقات: لتوضيح العمليات السابقة، نفترض تعريف المتغيرات التالية:

(أ) L = إجمالي عدد أسماء المتغيرات للعناصر في قاعدة المعلومات الإدارية MIBفي الطلب.

(ب) N = عدد أسماء المتغيرات من بداية قائمة أسماء المتغيرات .

(ج) R = عدد المتغيرات التالية لأول عدد N يتم تكراره، والذي نريد عنده إجراء استرجاعات متعددة.

(د) M=عدد المرات التي نريد استعراض (تصفح) شجرة قاعدة المعلومات الإدارية لكل قيمة R من المتغيرات.

(هـ)من التعريفات السابقة نستنتج أن :

$$R = L - N$$

أي أن إجمالي عدد المتغيرات التي تتطلب استفسارات من قاعدة المعلومات الإدارية، يساوى إجمالي عدد المتغيرات في الطلب مطروحا منها المتغيرات التي تتطلب استفسارا واحدا فقط.

(و) نلاحظ أيضا أن إجمالي عدد قيم المتغيرات المطلوبة في الرسالة GetBulkRequest يساوى القيمة:

$$N + (M * R)$$

أي أن إجمالي عدد قيم المتغيرات المطلوبة في الرسالة GetBulkRequest يساوي إجمالي عدد الطلبات المنفردة N مضافاً إليها إجمالي عدد الطلبات المتكررة M مضروبا في عدد مرات التكرار R .

عندما يتم استقبال الرسالة GetBulkRequest، فإن الوكيل agent ينبغي عليه أن يقوم بتحديد عدد العناصر المطلوبة L وإيجاد عدد العناصر التي تتطلب استفساراً واحداً فقط Single Query وهي N ، وكذلك إيجاد عدد العناصر التي سوف تتطلب استفسارات متكررة R ، وتحديد عدد الاستفسارات التي تم طلبها في الرسالة لكل عنصر R وهي M. يقوم الوكيل بعد ذلك بمعالجة الاستفسارات ومحاولة ترجيع القيم للعناصر في قاعدة المعلومات الإدارية بكفاءة.

مثال: عندما يقوم جهاز الوكيل باستقبال الأمر GetBulkRequest بالقيم التالية:

L = 5, N = 2, R = 3, M =10

فسوف يوجد خمسة عناصر L يتم طلبها في الرسالة GetBulkRequest ، وأن

العنصرين الأولين N يكونان غير مكررين ، وأن العناصر الثلاثة التالية R تكون مكررة . وأن الوكيل سوف يحاول أن يجعل عشرة طلبات M مكررة لكل عنصر محدد في R.

3.4 تدعيم البروتوكولات المتعددة Multiprotocol

شرحنا سابقا أن الإصدار الأول للبروتوكول "سنمب–ف1" يعمل مع الشبكات التي تستخدم فقط بروتوكول IP، مثل شبكات شركة أبل، ونوفيل. وأن هذه الشبكات يجب أن يتم تهيئتها بواسطة استخدام برامج خاصة كي تستخدم البروتوكول IP كي تتمكن من استخدام البروتوكول "سنمب–ف1".

أما الإصدار الثاني للبروتوكول "سنمب–ف2" فقد تم تصميمه ليعمل مع أربعة أنواع من البروتوكولات هي:

1. الشبكات التي تستخدم بروتوكول IP.
2. شبكات أبل التي تستخدم بروتوكول AppleTalk.
3. شبكات نوفل التي تستخدم بروتوكول IPX.
4. شبكات OSI التي تستخدم خدمة شبكة CLNS .

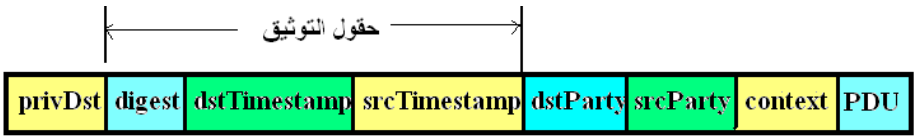
ولهذا فإن رسالة الإصدار الثاني للبروتوكول "سنمب–ف2"، ينبغي أن تكون قادرة على العمل مع الشبكات التي تستخدم هذه الأنواع الأربعة (IP, AppleTalk, IPX, OSI CLNS). يتم تسكين reside هذه البروتوكولات عند المستوى الشبكي Network Layer. في النموذج المرجعي OSI بينما البروتوكول "سنمب–ف2" يكون موجودا في المستوى التطبيقي Application Layer.

4.4 وسائل الأمن في البروتوكول SNMPv2

شرحنا سابقا أن تقنية الأمن في الإصدار الأول للبروتوكول "سنمب–ف1" تتم بواسطة استخدام "حروف المشاركة Community String". وعلى الرغم من أن هذه الطريقة لا تمنع إذن الدخول access غير المميز من رصد وتغيير قاعدة المعلومات الإدارية؛ فإنه يمكن لمهندس الشبكة مشكوراً أن يخصص جهازاً أو برمجيات مناسبة تحدد "حروف المشاركة" التي تستخدم في الشبكة.

بسبب أن استخدام حروف المشاركة في تأمين إذن الدخول إلى الشبكة لا يوفر مستوىً أمنياً قوياً؛ فإن هذا يعتبر نقطة ضعف في بروتوكول الإصدار الأول SNMPv1.

يحتوي الإصدار الثاني **SNMPv2** تقنيات أمن شاملة يمكنها إجراء عمليات التوثيق Authentication وعمليات التشفير Encryption لرسائل هذا الإصدار. وتوجد معلومات الأمن Security Information خارج رسائل هذا البروتوكول، وهي موضحة في الشكل 1.12.

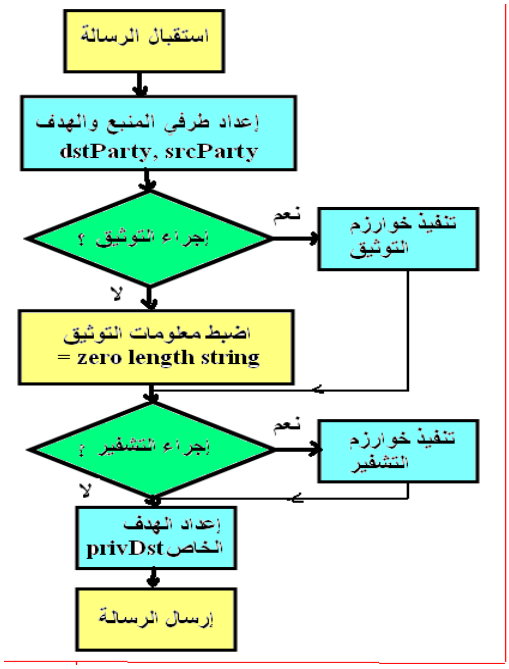


الشكل 1.12 حقول التوثيق المطلوبة لتحقيق تقنيات الأمن لسنمب–ف2.

تمثل الحروف srcParty في شكل رسالة سنمب– ف2 المجال الذي يحدد المدير المصدر manager source أو الوكيل Agent الذي يقوم بإرسال هذه الرسالة. أما الحروف dstParty فهي تحدد مجال المدير الهدف Destination Manager أو الوكيل الهدف، الذي يقوم بإعادة حروف المجالprivDst. تكون هذه الإعادة repetition ضرورية بسبب أن رسالة سنمب–ف2 ربما يكون جميع حروفها مشفرة، ويليها حروف مجال privDst الذي يظل نصا واضحا clear text، وذلك كي يتم تحديد محطة الهدف بسهولة.

عندما تطلب الرسالة عملية التوثيق، فإنه أيضا تحتوي على حروف استيعاب digest، وحروف ختم زمني للمنبع srcTimestamp، وختم زمني للهدف dstTimestamp. تكون هذه المعلومات ضرورية بحيث يمكن للوكيل في بروتوكول سنمب–ف2 من تحديد الاتصال المناسب بالمحطة الطرفية party وتوزيع الرسالة إلي صاحبها. وتحقيق الأمن المناسب للرسالة عندما يتم إرسالها أو استقبالها.

يعرف طرف الاتصال في البروتوكول سنمب–ف2 SNMPv2 Party بأنه عبارة عن مجموعة تتكون من اثنين أو أكثر، وترغب في إجراء عملية الاتصال من أجل إدارة المعلومات فيما بينها. كل طرف اتصال Party يكون له مجموعة من الخواص التي تحكم منح امتيازاته privileges بإذن الدخول إلى قاعدة المعلومات الإدارية. وتشمل هذه الخواص: التوثيق، التشفير، تصفح قاعدة المعلومات الإدارية، وسياق مجري النص (الكتابة) context. يوضح شكل1.13 خريطة خط سير العمليات لإرسال رسالة، يمكن توثيقها وتشفيرها، باستخدام البروتوكول سنمب–ف2 .



شكل1.13 عمليات إرسال رسالة (موثقة ومشفرة) باستخدام سنمب–ف2.

1.7.5 التوثيق Authentication

يوفر بروتوكول سنمب–ف2 طريقة آمنة للتوثيق تسمى التوثيق الاستيعابي Digest Authentication . وتعرف عملية الاستيعاب digest بأنها عملية حسابية تتم على رسالة البروتوكول سنمب–ف2 للتأكد من أن الرسالة المستقبلة هي نفسها المرسلة، وأن مصدر الرسالة قد قام بتوثيقها.

لتحقيق هاتين الوظيفتين، فإن المصدر يقوم بحساب الرسالة الاستيعابية message digest لرسالة بروتوكول سنمب–ف2، وذلك باستخدام بروتوكول يسمى MD5 ، ويعني message digest 5 ، وذلك باستخدام مفتاح توثيق authentication key . ثم يتم إرسال رسالة بروتوكول سنمب–ف2 ورسالة الاستيعاب. ولا يتم إرسال مفتاح التوثيق مع الرسالة. عندما يقوم الهدف باستقبال الرسالة، يقوم بإعادة حساب رسالة الاستيعاب، باستخدام النسخة المحلية لمفتاح التوثيق التي يمتلكها. عندما يتحقق توافق بين الرسالة الاستيعابية المحسوبة مع الرسالة الاستيعابية الموجودة بالرسالة، فإنه يتم توثيق الرسالة. إن استخدام الرسالة الاستيعابية يؤكد أن الرسالة المستقبلة هي التي تم إرسالها، وأن مفتاح التوثيق يثبت أن المصدر يكون موثقاً (مفوضاً).

كما يوجد خاصية توثيق إضافية وهي أن MD5 يستخدم أختاماً زمنيةً time stamps في الرسالة لضمان أن الرسالة لم يتم الاستيلاء عليها captured ، وإعادة تشغيلها replayed للحصول على إذن دخول غير موثق (غير مفوض). إن كل طرف للبروتوكول سنمب–ف2 له أقصى عمر maximum age، يطلق عليه العمر الزمني lifetime لكل رسالة، وأن الأختام الزمنية في الرسالة تضمن أن العمر الزمني للرسالة لم يتم تجاوزه.

أحد المشاكل المتعلقة باستخدام بروتوكول التوثيق الاستيعابي هو توزيع مفاتيح التوثيق على النظم المتعددة داخل أطراف party البروتوكول سنمب–ف2. وكما تعلمنا سابقا في إدارة الأمن Management security، أن استخدام المفاتيح العامة Public Keys

يعالج هذه المشكلة. لكن في واقع الأمر أن البروتوكول "سنمب–ف2" لا يستخدم خوارزم المفتاح العام لتوزيع مفاتيح التوثيق اللازمة لإجراء خوارزم رسالة الاستيعاب.

- التشفير Encryption

عندما يرغب عضوان في دائرة الاتصال بالشبكة (يطلق عليه مسمى Party)، بتحديد أن الرسالة ينبغي إجراء تشفير لها، فإنه يتم استخدام خوارزم تشفير البيانات DES. مثل كل خوارزميات التشفير فإن الخوارزم يمكن أن يتم كسر شفرته، وهذا قد يحدث كل 1×10^{72}، وهي فرصة ضعيفة جدا. وعندما يتم تخصيص عملية التشفير لإجراء الاتصال، فإن كل رسالة في البروتوكول "سنمب–ف2" ؛ ما عدا حروف حقل privDst؛ يتم تشفيرها قبل إجراء عملية الإرسال. وأن الطرف الهدف Destination Party يقوم بفك شفرة decrypt الرسالة بواسطة نفس الخوارزم.

5.4 مرئية قاعدة المعلومات الإدارية MIB View

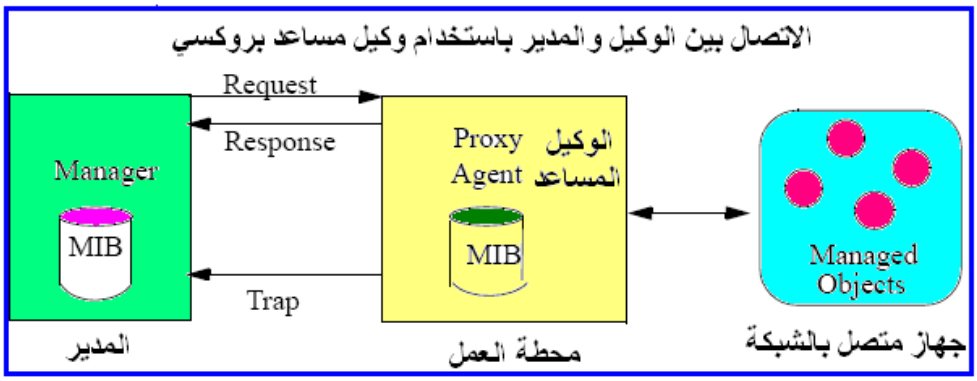
تعرف مرئية قاعدة المعلومات الإدارية MIB View بأنها جزء قاعدة المعلومات الإدارية الذي يمكن الوصول إليه accessible بواسطة المدير Manager. كما يستطيع طرف اتصال Party أن يتحكم في إذن الدخول access لجزء من قاعدة المعلومات الإدارية في جهاز الوكيل Agent. حيث يمكن للوكيل أن يسمح بإذن الدخول لمجموعة معينة فقط من المديرين لتصفح أجزاء محددة فقط من قاعدة المعلومات المحلية الخاصة بإدارة المعلومات. على سبيل المثال، في حالات عديدة ربما يكون من المرغوب فيه، أن يوجد مجموعة قليلة مختارة من المديرين يسمح لها بإذن الدخول إلى أجزاء معينة في قاعدة المعلومات الإدارية MIB لتهيئة جهاز (وهو عنصر يتم طلبه بواسطة الرسالة Set-Request)، أو أن يسمح لمجموعة أخرى من المديرين بإذن الدخول لتصفح عناصر معلوماتية فقط.

إن العمليات التي قد يحتاجها نظام إدارة معين يمكن أن تقتصر فقط على تصفح خواص properties جهاز محدد. في حين أن مهندس نظام إدارة الشبكة، ربما يحتاج أن يكون

قادرا على تغيير قيم العناصر الموجودة في قاعدة المعلومات الإدارية. إن تصفح مرئية قاعدة المعلومات الإدارية يسمح بإجراء هذه الوظائف. يمكن لكل وكيل أن يتصل بمدير ويحدد احتياجاته عندما يرغب الخروج من دائرة الاتصال party ، وكذلك احتياجاته لتصفح المعلومات الإدارية المصاحبة.

6.4 السياق contexts

يعرف السياق context في الإصدار الثاني للبروتوكول "سنمب–ف2"، بأنه مجموعة العناصر الإدارية managed objects التي يمكن للمدير أو الوكيل أن يصل إليها. على سبيل المثال، يمكن أن نعتبر عملية تصفح مرئية قاعدة المعلومات الإدارية هي سياق لكيان entity محلي معطى للبروتوكول "سنمب–ف2". حيث إن هذا السياق المحلي يعرّف عناصر قاعدة المعلومات الإدارية التي يستطيع المدير أو الوكيل الوصول إليها. يمكن إجراء الاتصال عن بعد بين سياق للبروتوكول "سنمب–ف2" للمدير والوكيل من خلال وكيل مساعد "proxy agent"، كما هو موضح في الشكل1.14.



الشكل1.14 الاتصال عن بعد بين سياق "سنمب–ف2" للمدير والوكيل من خلال وكيل مساعد.

يحتاج الوكيل المساعد "proxy agent" أن يفهم العناصر الإدارية للعمليات التي يطلبها المدير ويرغب في تصفحها. بهذه الطريقة فإن السياق context يعتبر عملية مجردة abstraction يكون لها علاقة بالتحكم في الوصول إلى المعلومات وإلى تصفح مرئية

قاعدة المعلومات الإدارية، التي من خلالها يتم الاستفسار عن المعلومات. يحتاج كل طرف اتصال party إلى سياق، لتمكين المدير والوكيل من تحديد العمليات المسموحة لمجموعة محددة من العناصر الإدارية.

أسئلة تقويم ذاتي

عدد خصائص بروتوكول SNMPv2 .

اذكر وظائف الرسائل التالية التي يستخدمها بروتوكول SNMPv2 :

أ- InformRequest.

ب- GetBulkRequest.

الإصدار الثاني للبروتوكول SNMPv2 تم تصميمه ليعمل مـــع أربعـــة أنواع من البروتوكولات ما هي ؟

ضع علامة (√) أو (×) .

يستخدم التوثيق الاستيعابي Digest Authentication في SNMPv2:

أ- للتأكد من أن الرسالة المستقبلة هي نفسها المرسلة.

ب- لدعم بروتوكولات قياسية متعددة.

ج- لتحسين هيكل المعلومات الإدارية.

د- كل ما سبق.

هـــ - لا شيء مما سبق.

الخلاصة

عزيزي الدارس،

أوضحت الوحدة عيوب استخدام نظامي: القائمة المنسدلة، ونظام الأمر الخطي حيث ذكرت الوحدة أن هذه الطرق عادة تكون بطيئة ومتعبة، خاصة في بنية الشبكات غير المتجانسة، وكذلك عند استخدام أساليب استفسار متعددة، كذلك تناولت الوحدة بروتوكول الإنترنت والأمر ping، ولخصت الوحدة عيوب هذه الطريقة في ثلاث نقاط هي :

- أنه لا يعتمد عليها في توصيل الرسائل .
- تحتاج لإجراء عملية التصويت polling .
- توفر معلومات محدودة .

ثم تناولت الوحدة بروتوكول إدارة الشبكة البسيط الإصدار الأول SNMPv1 ، وهو بروتوكول قياسي تم تطويره لإدارة مراكز اتصالات شبكة البيانات.وتم تصميمه للعمل في المستوى التطبيقي Application Layer، وذلك لتسهيل تبادل المعلومات الإدارية بين أجهزة الشبكة. حيث يمكّن البروتوكول مهندس الشبكة من إدارة أداء الشبكة، وحل مشاكلها، والتخطيط لتوسعة وتطوير الشبكة.

يعتمد بروتوكول SNMPv1 في عمله على استخدام نموذج "المدير/الوكيل" Manger/Agent Model، ويقوم البروتوكول SNMPv1 بتأدية وظائفه مستخدما خمسة أنواع من الرسائل القياسية:

Get – Request
Get-Response
Get - Next Request
Set- Request
Trap

وأوضحت الوحدة أنه على الرغم من كفاءة البروتوكول SNMPv1 في إدارة الشبكة إلاَّ أنه توجد به ثلاث مشاكل هي:

- هو بروتوكول قياسي للاستخدام فقط لشبكات IP.
- هو غير كفء في حالة استرجاع المعلومات من الجداول الكبيرة.
- يستخدم كلمات نصية واضحة للأمن، مما يجعلها نسبيا غير آمنة.

ومن ثم تناولت الوحدة الإصدار الثاني للبروتوكول SNMPv2، وأوضحت الوحدة أن الإصدار الثاني يؤدي نفس الوظائف الأساسية التي يؤديها الإصدار الأول للبروتوكول SNMPv1 التي تم شرحها سابقا، والخاصة بالاستفسار وتغيير البيانات في قاعدة المعلومات الإدارية عن أجهزة الشبكة. وقد تم تطوير هذا الإصدار كي يتغلب على المشاكل التي يعاني منها الإصدار الأول للبروتوكول SNMPv1 ويتميز الإصدار الثاني للبروتوكول SNMPv2 بعدة خصائص هي:

- يوجد به إضافات لتحسين هيكل المعلومات الإدارية "SMI" .
- يوجد به أنواع جديدة من الرسائل .
- يدعم بروتوكولات متعددة قياسية Multiprotocol.
- تحسين الأمن بفعالية عالية Significantly .
- يوجد به عناصر لقاعدة معلومات إدارية جديدة .
- يمكن أن يتعاون مع الإصدار الأول للبروتوكول SNMPv1 .

كما بينت الوحدة أنواع الرسائل في البروتوكول SNMPv2، حيث يوجد نوعان جديدان من الرسائل التي يستخدمها الإصدار الثاني للبروتوكول SNMPv2، هما: InformRequest, GetBulkRequest . كلاهما يؤدي وظائف قيمة للوكيل والمدير .

لمحة مسبقة عن الوحدة التالية

تأتي الوحدة التالية بعنوان " بروتوكول إدارة الشبكة البسيط الإصدار الثالث"، حيث توضح هذه الوحدة خصائص بروتوكول "سنمب--ف3" والبناء الهيكلي له، كما توضح الوحدة العمليات التفاعلية بين آلة "سنمب--ف3" ومجموعة التطبيقات، كما تجد في هذه الوحدة نموذج أمن المستخدم USM الذي يوفر للبروتوكول "سنمب--ف3"خدمات التوثيق وخدمات الخصوصية ، وأيضاً تجد نموذج تحكم الوصول لرؤية المعلومات VACM، وكذلك معالجة تحكم الدخول لمرئية قاعدة المعلومات الإدارية، و العمليات المنطقية في نموذج "فاكم".

مسرد المصطلحات

نظام القائمة المنسدلة Menu-Driven System

أحد أساليب أوطرق تجميع البيانات، وفي هذه الطريقة يتم استخدام جهاز الماوس المتصل بالحاسب، والضغط على المفاتيح المناسبة لتظهر البيانات المطلوبة على شاشة النظام الإداري.

نظام الأمر الخطي Command Line Interface

أحد أساليب أوطرق تجميع البيانات، وفي هذه الطريقة يتم كتابة الأمر المناسب على شكل سطري على شاشة النظام الإداري، وبعد تنفيذ الأمر يتم ظهور المعلومات على شاشة العرض بالنظام.

الأمر بنج Ping

ويعنى Packet Inter Net Groper "طريقة تلمس حزمة الإنترنيت" هو أحد الأوامر التطبيقية الشائعة الاستخدام في اختبار توصيلة جهازٍ متصل بالشبكة عن بعد.

بروتوكول إدارة الشبكة البسيط(SNMP) Simple Network Management Protocol.

ويقوم هذا البروتوكول بتوفير وسائل للحصول على المعلومات، وكذلك إعطاء التعليمات لأجهزة الشبكة. وهذا البروتوكول متوافق مع النموذج المرجعي Open Systems Interconnection (OSI)الذي يتكون من سبعة مستويات والذي تم تطويره من قبل الهيئات ISO, CCITT ، وقد صدر منه ثلاثة إصدارات Versions هي:

SNMPv1, SNMPv2, SNMPv3، وتشترك هذه الإصدارات الثلاثة بأن لها نفس تركيب ومكونات البناء الهيكلي الأساسي.

بروتوكول إدارة الشبكة البسيط (الإصدار الأول SNMPv1**):**

هو بروتوكول قياسي تم تطويره لإدارة مراكز اتصالات شبكة البيانات. و تم تصميمه للعمل في المستوى التطبيقي Application Layer، وذلك لتسهيل تبادل المعلومات الإدارية بين أجهزة الشبكة. ويشمل ذلك إدارة أجهزة الخادم – محطة العمل –

الموجهات – مفاتيح الاتصال – المجمعات Hubs – وغيرها.

بروتوكول إدارة الشبكة البسيط (الإصدار الثاني SNMPv2) :

يؤدي الإصدار الثاني للبروتوكول SNMP نفس الوظائف الأساسية التي يؤديها الإصدار الأول والخاصة بالاستفسار وتغيير البيانات في قاعدة المعلومات الإدارية عن أجهزة الشبكة. وقد تم تطوير هذا الإصدار كي يتغلب على المشاكل التي يعاني منها الإصدار الأول .

التوثيق الاستيعابي Digest Authentication

طريقة آمنة للتوثيق يوفرها بروتوكول SNMPv2 ، وتعرف عملية الاستيعاب digest بأنها عملية حسابية تتم على رسالة البروتوكول سنمب–ف2 للتأكد من أن الرسالة المستقبلة هي نفسها المرسلة، وأن مصدر الرسالة قد قام بتوثيقها.

الأختام الزمنية time stamps

خاصية توثيق إضافية يوفرها بروتوكول SNMPv2 من خلال استخدام بروتوكول MD5، حيث يستخدم MD5 أختاماً زمنيةً time stamps في الرسالة لضمان أن الرسالة لم يتم الاستيلاء عليها captured ، وإعادة بثها replayed للحصول على إذن دخول غير موثق (غير مفوض).

مرئية قاعدة المعلومات الإدارية MIB View

هو ذلك الجزء من قاعدة المعلومات الإدارية الذي يمكن الوصول إليه accessible بواسطة المدير Manager. كما يستطيع طرف اتصال Party أن يتحكم في إذن الدخول access لجزء من قاعدة المعلومات الإدارية في جهاز الوكيل Agent.

السياق contexts

يعرف السياق context في الإصدار الثاني للبروتوكول SNMPv2 بأنه مجموعة العناصر الإدارية managed objects التي يمكن للمدير أو الوكيل أن يصل إليها.

المصطلح بالإنجليزية	معناه بالعربية
Abstraction	عملية مجردة
Access	الدخول
Accessible	يمكن الوصول إليه
Adequate Qualitative	كمية الجودة الملائمة
Agent	وكيل
Alarm	إنذار
Authentication failure	عطل توثيق
ASCII	شفرة أسكي
Application Layer	المستوى التطبيقي
Bridges	الجسور
Buffer Space	حجم الذاكرة المؤقتة
Captured	الاستيلاء
Connectionless	الإرسال بعدم الربط
Cold start	التشغيل البارد
Community String	حروف المشاركة
Context	سياق مجرى النص
Congestion	اختناق
Command Line Interface	بينية الأمر الخطي
Digest Authentication	التوثيق الاستيعابي
Drawbacks	العيوب
Data typ	نوع بيانات
Destination	الهدف

المصطلح بالإنجليزية	معناه بالعربية
Echo	رسائل الصدى
Echo Reply	استجابة الصدى
Encryption	التشفير
Enterprise specific	تحديد مؤسسة
Entries	مداخل
Fault Isolation	عزل الأعطال
Get-Request	رسالة طلب–رجاء
Get-Next-Request	رسالة طلب تالي
Get-Response	رسالة استجابة
GetBulkRequest	طلب استرجاع كمية كبيرة من المعلومات
Hubs	المجمعات
Heterogeneous	غير متجانسة
Host Computer	الحاسب المضيف
Hyphenated	شرطة بين الكلمات
Hierarchical	هرمي
Internet Protocol (IP)	بروتوكول الإنترنيت
Interfaces	الوحدات البينية
Interpret	تفسير
Invalid	غير صالحة
InformRequest	رسالة إعلام
Lexigraphical order	ترتيب المعلومات بطريقة متتالية تنازليا أو تصاعديا .

المصطلح بالإنجليزية	معناه بالعربية
Lifetime	العمر الزمني
Manger/Agent Mode	نموذج "المدير/الوكيل"
Managed objects	العناصر الإدارية
Management Information Base (MIB)	قاعدة المعلومات الإدارية
Multiprotocol	البروتوكولات المتعددة
Network Service Access Point	نقطة اتصال الخدمة الشبكية
Network layer	طبقة الشبكي
Operating Parameters	معاملات التشغيل
Open Systems Interconnection (OSI)	الاتصال البيني للنظم المفتوحة
Party	طرف اتصال
Properties	خواص
Privileges	امتيازاته
Internet Control Message Protocol (ICMP)	بروتوكول رسائل تحكم الإنترنيت
Proxy Agents	وكلاء معاونون
Polling	عملية التصويت
Protocol Data Unit (PDU)	وحدة بيانات البروتوكول
Queries	استفسارات
Repository	مستودع
Replayed	إعادة بث

المصطلح بالإنجليزية	معناه بالعربية
Resource allocation	تخصيص مصادر
Reside	تسكين
Retrieval	استرجاع
Routing	تحديد المسار
Routers	الموجهات
Security	الأمن
Settable parameters	معاملات الإعداد
Standard tools	أدوات قياسية
Source	المصدر
Simultaneously	نفس التوقيت
Significantly	فعالية عالية
Signed	الأعداد الصحيحة الرمزية
Structure management Information(SMI)	هيكل المعلومات الإدارية
Traversing	يستعرض
Transport Layer	مستوى النقل
Trap	رسالة المصيدة
Trouble Shooting	تشخيص الأعطال
Turn around time	الفترة الزمنية للدورة
Unsolicited Messages	رسائل تطوعية
Unsigned	عدد صحيح "غير رمزي"
Valid	صالحة
Warm Start	التشغيل الدافئ

قائمة المراجع

1- Essential SNMP, 2nd Edition by Douglas R Mauro, Kevin J Schmidt Published by O'Reilly Media, Publication date: September 21, 2005, ISBN: 0596008406.

2- Hands-On SNMP, (McGraw-Hill Series on Computer Communications) by Paul Simoneau, Published by Computing McGraw-Hill, Publication date: June 1, 1997, ISBN: 0079130755.

3- How to Manage Your Network Using SNMP: The Networking Management Practicum, by Marshall T. Rose, Keith McCloghrie Published by Prentice Hall, Publication date: January 1995, ISBN: 0131415174.

4- Managing Internetworks With SNMP: The Definitive Guide to the Simple Network Management Protocol (SNMP and SNMP Version 2) by Mark A. Miller, P.E., Published by M & T Books; Book & CD-ROM edition Publication date: June 1997, ISBN: 1558515615.

5- Network Management: A Practical Perspective ,by Allan Leinwand, Karen Fang-Conroy. Info at Addison-Wesley, 1997.

6- SNMP at the Edge: Building Effective Service Management Systems by Jonathan Saperia, Published by McGraw-Hill Professional, Publication, date: June 28, 2002, ISBN: 0071396896.

7- SNMP Network Management, (McGraw-Hill Computer Communications Series), Book & CD-ROM Edition by Paul Simoneau, Published by McGraw-Hill Companies, Publication date: May 20, 1999, ISBN: 0079130755.

8- SNMP Over Wi-Fi Wireless Networks, by Jiradett Kerdsri, Published by Storming Media, Publication date: 2003, ISBN: 1423503287.

9- SNMP, SNMPv2c, SNMPv3, and RMON 1 and 2, 3rd Edition, by William Stallings, Published by Addison-Wesley Pub Co Publication date: December 1998, ISBN: 0201485346.

10- SNMP: Versions 1 & 2 Simple Network Management Protocol Theory and Practice, by Mathias Hein, David Griffiths, Published by Van Nostrand Reinhold, Publication date: September 1995, ISBN: 1850321396.

11- Total SNMP: Exploring the Simple Network Management Protocol 2nd Edition, by Sean J. Harnedy, Published by Prentice Hall, Publication date: July 1, 1997, ISBN: 0136469949.

12- SNMP & Network Web Sites:

- RFCs: Requests for Comments, http://ietf.org/rfc.html

- IETF: The Internet Engineering Task Force, http://www.ietf.cnri.reston.va.us/

- mibDepot is an online SNMP MIB reference site,http://www.mibdepot.com/index.shtml

- The Simple Times is a quarterly newsletter.http://www.simple-times.org/

- The Simple Web is a Web site created and maintained by the SNMP group at the University of Twente in Holland. http://www.simpleweb.org/

- SNMP World is a Web site created and maintained by a group of Network Management Engineers. http://www.snmpworld.com/


الوحدة الثانية
بروتوكول إدارة الشبكات البسيط
الإصدار الثالث SNMPv3

محتويات الوحدة

المقدمة

تمهيد

عزيزي الدارس،

مرحباً بك إلى الوحدة الثانية من مقرر " **استخدام وإدارة الشبكات (2)** "، وتأتي هذه الوحدة بعنوان " **بروتوكول إدارة الشبكة البسيط الإصدار الثالث SNMP-v3** "، و تشتمل هذه الوحدة على ستة أقسام: القسم الأول يوضح خصائص بروتوكول "سنمب--ف3" والذي اشتمل على خصائص أمنية تسمح بإتمام تهيئتها باستقلالية Independent، القسم الثاني من الوحدة يتناول البناء الهيكلي لبروتوكول "سنمب--ف3"، كما يتناول القسم أيضاً العمليات التفاعلية بين آلة "سنمب--ف3" ومجموعة التطبيقات، أما القسم الثالث فيتناول نموذج أمن المستخدم USM، حيث يوفر نموذج أمن المستخدم USM للبروتوكول "سنمب-ف3": خدمات التوثيق Authentication، وخدمات الخصوصية Privacy. فقد تم تصميم نموذج USM للحماية من التهديدات Threats الرئيسية التي سنوضحها من خلال دراستك للوحدة. القسم الرابع يتناول نموذج تحكم الوصول لرؤية المعلومات VACM، والذي يستخدم للتحكم في الدخول لإدارة العناصر في قاعدة المعلومات الإدارية MIB. أما القسم الخامس فيأتي متناولاً معالجة تحكم الدخول Access Control Processing وأيضاً يتناول القسم العمليات المنطقية في نموذج "فاكم"، و تحقيق العمليات المنطقية داخل نظام "فاكم"، ثم مقارنة مع سنمب-ف1 و سنمب-ف2. ونختم هذه الوحدة بالقسم السادس والذي يأتي متناولاً مكونات شكل رسالة "سنمب--ف3" .

أهداف الوحدة

عزيزي الدارس، بعد فراغك من دراسة هذه الوحدة ينبغي أن تكون قادراً على أن:

- **تذكر** خصائص بروتوكول "سنمب--ف3" و البناء الهيكلي له.
- **تشرح** العمليات التفاعلية بين آلة "سنمب--ف3" ومجموعة التطبيقات.
- **توضح** وظائف وكيفية عمل نموذج أمن المستخدم USM.
- **تشرح** طرق تحقيق التوثيق والخصوصية وصحة الرسائل.
- **تصف** كيفية توليد المفاتيح السرية والمحلية وإدارتها.
- **تشرح** عمليات التحقق من عدم تأخر الرسائل والتوقيت المتزامن.
- **تصف** طريقة عمل واختيار الآلات الموثقة.
- **تشرح** نموذج تحكم الوصول لرؤية المعلومات VACM.
- **تصف** كيفية معالجة تحكم الدخول لمرئية قاعدة المعلومات الإدارية.
- **تتتبع** وصف العمليات المنطقية في نموذج "فاكم".
- **تعدد** مكونات فورمات رسالة "سنمب--ف3".
- **تستخدم** برتوكول سنمب-ف3 في إدارة شبكات البيانات.

1 . خصائص بروتوكول "سنمب--ف3"

لقد تم اشتقاق وتطوير الإصدار الثالث لبروتوكول إدارة الشبكات البسيط "سنمب–ف3" من كلا الإصدارين الأول والثاني. وتشترك هذه الإصدارات الثلاثة بأن لها نفس تركيب ومكونات البناء الهيكلي الأساسي. وأن التعديلات الأساسية التي حدثت في بروتوكول "سنمب–ف3"، شملت الأمن Security، وعمليات الإدارة Administration. وذلك بهدف بناء تصميم عام يتميز بنظام أمني مرن يجعل من الممكن إجراء عمليات التفاعل بين المدير وأجهزة الإدارة تحقق عمليات الأمن التي تطلبها المؤسسة. الهدف الآخر هو أن يتم تصميم نظام عمليات إدارة الأمن بسهولة.

ولتحقيق الأهداف السابقة، فإن "سنمب–ف3" اشتمل على خصائص أمنية تسمح بإتمام تهيئتها باستقلالية Independent ، وهي كما يلي:

– يدعم "سنمب–ف3" عملية توثيق الرسائل Message Authentication لضمان أن تكون التعليمات صادرة من مدير معتمد Valid.

– تحقيق الخصوصية Privacy، لضمان عدم استطاعة أحد من قراءة الرسائل أثناء عبورها بين محطة المدير وأجهزة الإدارة.

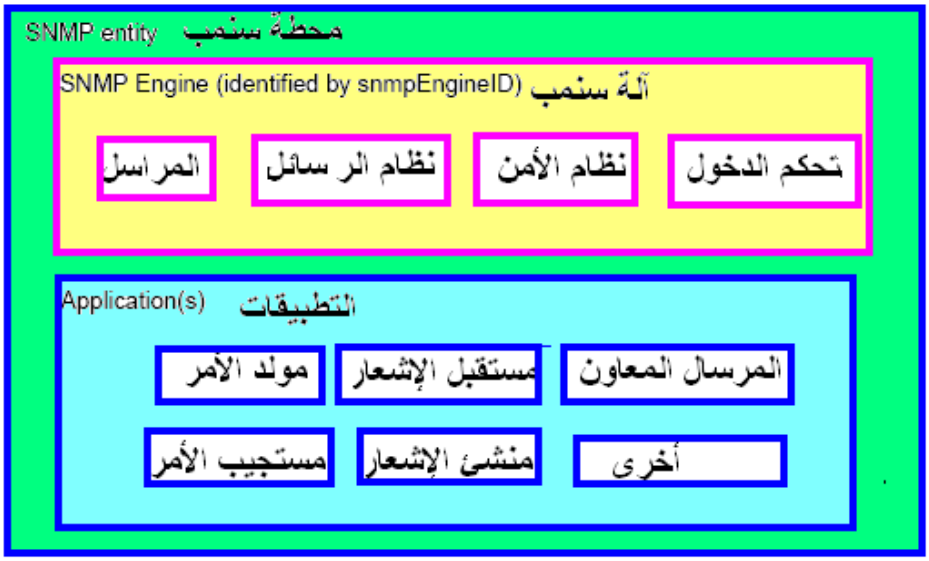
– تحقيق عملية التفويض Authorization ، والتحكم في الوصول لتصفح المعلومات View Based Access Control للسماح فقط للمديرين المفوضين بالدخول، وتصفح بنود محددة في قاعدة المعلومات الإدارية.

– يسمح "سنمب–ف3" بإجراء عمليات التهيئة عن بعد Remote Configuration ، وهذا يمكن المدير المفوض من أن يقوم بتغيير تهيئة قائمة بنود الأمن عن بعد بدون الحاجة لأن يكون موجودا فعليا داخل الجهاز.

2 . البناء الهيكلي لبروتوكول "سنمب--ف3"

عزيزي الدارس،

يتكون البناء الهيكلي لبروتوكول "سنمب-ف3"، كما هو موضح في الشكل2.1، من مكونين أساسيين هما: آلة سنمب-ف3 ، و مجموعة التطبيقات، وسوف نطلق عليهما اسم محطة التشغيل، أو "كينونة سنمب-ف3 SNMP Entity".



الشكل2.1 البناء الهيكلي لبروتوكول سنمب-ف3.

1.2 آلة "سنمب--ف3" SNMPv3 Engine

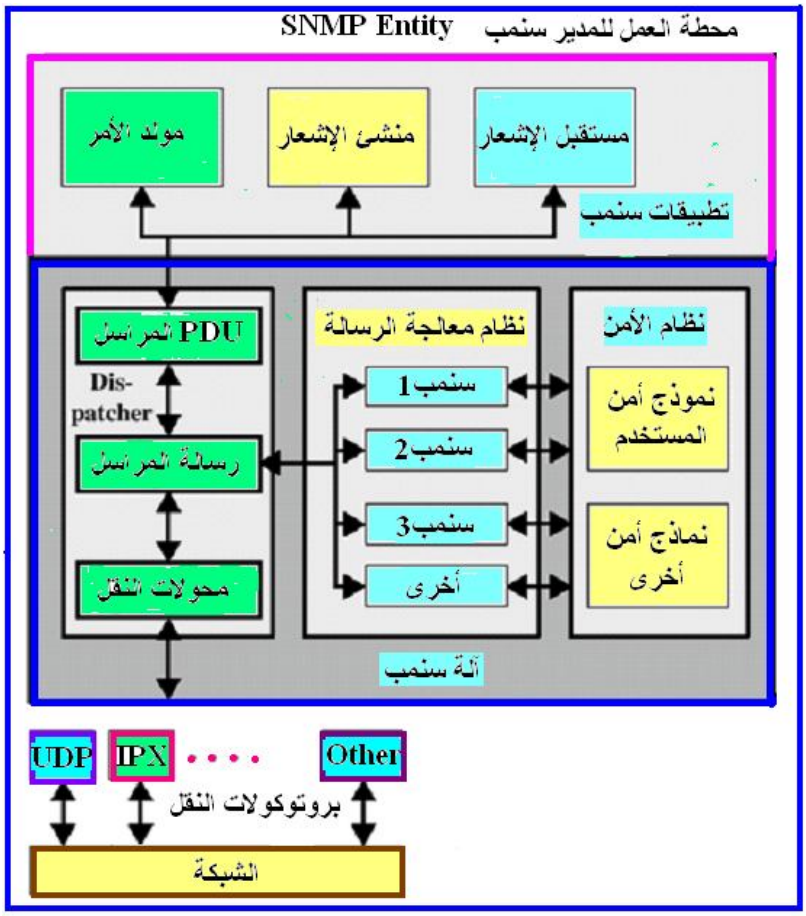
تتكون آلة "سنمب-ف3" من أربعة مكونات هم: المنجز Dispatcher ، ونظام الرسائل، ونظام الأمن، ونظام تحكم الدخول.

- **المنجز** Dispatcher هو الذي يختص بعمليات إرسال واستقبال الرسائل. وتحديد نوع إصدار الرسالة التي يستقبلها سنمب-ف1، سنمب-ف2،سنمب-ف3. عندما تتم عملية تحديد الإصدار ومعالجته، يقوم المنجز بتسليم الرسالة إلى نظام معالجة الرسالة، وكذلك إلى الكيانات الأخرى (الوكلاء والمديرين في محطة التشغيل).

- **نظام الرسائل** Message Subsystem ويختص بمعالجة الرسائل الصادرة من الإصدارات الثلاثة لبروتوكول "سنمب–ف3"، وأي نماذج رسائل لبروتوكولات أخرى.
- **نظام الأمن** Security Subsystem ، يختص بمعالجة الأمن مستخدما نموذج أمن المستخدم User Based Security Mode (USM)، الخاص بالبروتوكول "سنمب–ف3" . كما يستخدم نموذج أمن المشاركة Community Based Security Model ، الذي يتعامل مع الإصدارين الأول والثاني للبروتوكول "سنمب–ف3". وأي نماذج أمنية إضافية جديدة يتم تحديدها.
- **نظام تحكم الدخول** Access Control System وهو يختص بمنح أو منع عمليات الدخول إلى عناصر إدارية محددة في قاعدة المعلومات الإدارية MIB. على سبيل المثال، يمكن تحديد عمليات الكتابة والقراءة لمستخدم يرغب الدخول إلى قطاع معين في شجرة قاعدة المعلومات الإدارية، بينما يمكن أن يسمح لباقي المستخدمين بإجراء الدخول إلى عمليات قراءة فقط لكامل محتويات شجرة قاعدة المعلومات الإدارية.

2.2 مجموعة التطبيقات SNMP Applications

يوجد خمسة أنواع من التطبيقات للبروتوكول "سنمب–ف3" ، كما هو موضح في الشكل2.1 ، والشكل 2.2 وهي:



الشكل2.2 محطة العمل للمدير سنمب–ف3 والتطبيقات.

أ- **مولد الأوامر** Command Generator، ووظيفته إنشاء الأنواع المختلفة لرسائل بروتوكول "سنمب–ف3".

ب- **مستجيب الأوامر** Command Responder، ووظيفته الرد على رسائل بروتوكول "سنمب–ف3".

ج- **منشئ الإشعار** Notification Originator، ووظيفته إرسال رسالة مصيدة Trap ، أو إرسال رسالة إشعار (إعلام) Inform.

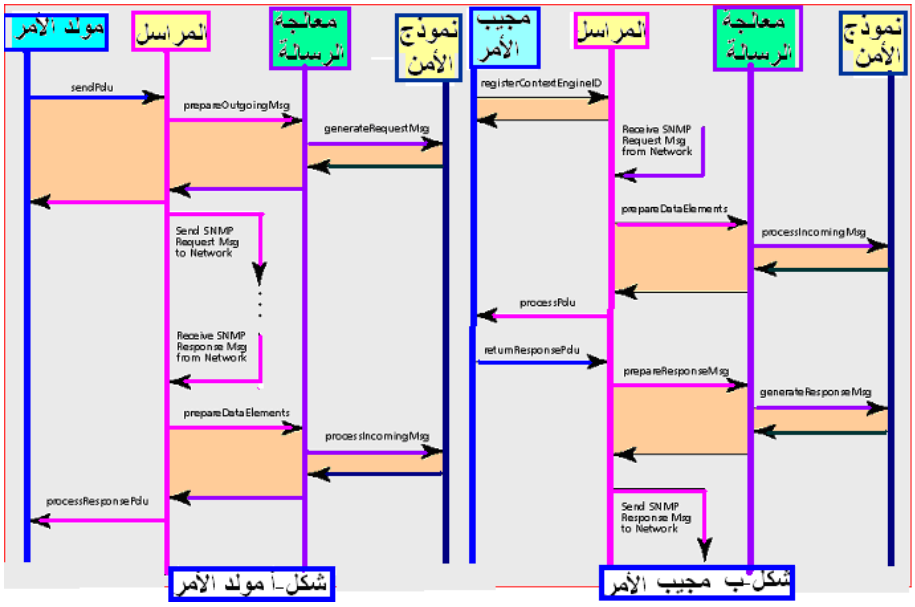
د- **مستقبل الإشعار** Notification Receiver، ووظيفته استقبال ومعالجة رسائل المصيدة Trap ، أو الإشعار Inform.

هـ- **الوكيل المعاون** Proxy Forwarder، ووظيفته توصيل الرسائل بين مكونات محطة "سنمب-ف3" (Entity).

وسنشرح العمليات التفاعلية التي تتم بين هذه التطبيقات في الفقرات التالية تباعا.

3.2 العمليات التفاعلية بين آلة "سنمب--ف3" ومجموعة التطبيقات

يتم إجراء الخدمات Services بين وحدات برامج التشغيل Modules في محطة التشغيل Entity في بروتوكول "سنمب-ف3" بواسطة معاملات Parameters، ودوال أولية . تستخدم المعاملات لتمرير بيانات ومعلومات التحكم، بينما تستخدم الدوال لتحديد الوظائف المطلوب تحقيقها. يوضح الشكل2.3 (أ) مخطط تتابع الأحداث التي يقوم فيها تطبيق مولد الأمر (أو منشئ الإشعار) برجاء إرسال وحدة بيانات بروتوكول PDU، وطريقة استرجاع الرد الموافق لهذا التطبيق، وهذه الأعمال تحدث عند وحدة المدير Manager. يوضح الشكل2.3 (ب) الأحداث Events المقابلة التي تتم عند وحدة الوكيل Agent. عندما يقوم المنجز Dispatcher باستقبال رسالة قادمة إليه من وحدة PDU فإنه يقوم بالرد عليها. تبين الأسهم التي يوجد عليها ملصق Label اسم الدوال المعبرة عن هذا النداء Call الخاص بهذا التطبيق. وتبين الأسهم التي لا يوجد عليها ملصق الاستجابات الصادرة من هذا النداء. يبين الجزء المظلل عملية التوافق Matching بين دالة النداء والاستجابة العائدة Return.



الشكل2.3 العمليات التفاعلية بين آلة "سنمب--ف3" ومجموعة التطبيقات

- **<u>تطبيق مولد الأمر</u>:**

يقوم باستخدام رسالة sendPDU، وينشئ رسالة processResponsePDU من دالة المنجز. تزود دالة النداء sendPDU المنجز بمعلومات عن الهدف Destination، ومعاملات الأمن، ووحدة بيانات البروتوكول PDU المطلوب إرسالها. يقوم المنجز بعد ذلك ببدء تشغيل Invoke نموذج معالجة الرسالة الذي بدوره يقوم ببدء تشغيل نموذج الأمن لتجهيز الرسالة.

يقوم المنجز بعد ذلك بتسليم الرسالة المجهزة إلى مستوى النقل Transport Layer (مثلا UDP) للإرسال. إذا فشلت عملية تجهيز الرسالة، يظهر المنجز بيان وقوع خطأ، وذلك في قيمة دالة نداء العودة sendPDU . عندما تنجح عملية تجهيز الرسالة، يخصص مراسل محدد sendPDUHandle إلى وحدة PDU، و يتم ترجيع هذه القيمة إلى مولد الأمر. يخزن مولد الأمر القيمة sendPDUHandle لكي يستطيع توفيق الاستجابة المتتابعة من وحدة PDU مع الطلب الأصلي originalRequest. يرسل

المنجز كل استجابة من وحدة PDU إلى تطبيق مولد الأمر الصحيح بواسطة استخدام الدالة processResponsePDU.

- **تطبيق مستجيب الأمر:**

يستخدم أربعة دوال من المنجز هي:

- registerContextEngineID, مسجل سياق آلة الهوية
- unregisterContextEngineID, سياق آلة هوية غير مسجل
- processPDU, معالجة وحدة بيانات البروتوكول
- returnResponsePDU. إرجاع استجابة لوحدة بيانات البروتوكول

بالإضافة إلى دالة واحدة للتعامل مع نظام تحكم الوصول هي isAccessAllowed.

تقوم دالة مسجل سياق آلة الهوية بتشغيل تطبيق مستجيب الأمر كي تشترك مع آلة "سنمب–ف3" لغرض معالجة أنواع وحدات بيانات بروتوكول PDU معينة لسياق الآلة. يقوم المنجز بتوصيل طلب الرجاء القادم من وحدة PDU إلى تطبيق مستجيب الأمر الصحيح، مستخدما دالة المعالجة processPDU .

يقوم مستجيب الأمر بعد ذلك بتنفيذ الخطوات الآتية:

– يفحص محتويات طلب وحدة PDU. ينبغي أن يتوافق نوع العملية مع الأنواع المسجلة سابقا بواسطة هذا التطبيق.

– يحدد إذا كان دخول هذه العملية الإدارية المطلوبة لوحدة PDU مسموحة أم لا. ولهذا الغرض يتم استدعاء الدالة accessAllowed .

يبين معامل نموذج الأمن securityModelParameters عملية الاستجابة على هذه الدالة، وذلك بواسطة تحديد نموذج الأمن الذي ينبغي استخدامه، بواسطة نظام تحكم الوصول Access Control Subsystem. يتحقق نظام تحكم الدخول من سماحية الطلب الرئيسي requesting Principal (بواسطة فحص الاسم الأمني security-Name)، عند هذا المستوى الأمني (securityLevel) من طلب عملية إدارية

(view-Type) لعنصـــــر إداري (variableName)، فـــــي هـــــذا الســـــياق (contextName).

- إذا تمت سماحية الدخول، يقوم مستجيب الأمر بتنفيذ العملية الإدارية، وتجهيز الاستجابة (الرد) على وحدة PDU. إذا أخفقت سماحية الدخول، يقوم مستجيب الأمر بتجهيز استجابة ملائمة لوحدة PDU لتبيان هذا الإخفاق.
- يقوم مسجل الأمر بمخاطبة المنجز، بواسطة الدالة returnResponsePDU لإرسال استجابة لوحدة PDU.

- **تطبيق مولد الإشعار:**

يتبع نفس الخطوات المستخدمة في تطبيق مولد الأمر. عندما يطلب إرسال طلب إعلام لوحدة PDU، فإنه يستخدم دالة sendPDU، ودالة processResponsePDU بنفس الطريقة المتبعة في تطبيق مولد الأمر. عندما يطلب إرسال رسالة trap PDU يتم فقط استخدام الدالة sendPDU.

- **تطبيق مستقبل الإشعار:**

يَتَّبِعُ جزءاً من الخطوات التي يقوم بها تطبيق مستجيب الأمر. ينبغي على مستقبل الإشعار أن يقوم بالتسجيل أولا، لكي يستقبل الإشعار Inform أو المصيدة Trapمن وحدات PDU. يتم استقبال أنواع وحدات بيانات البروتوكول PDUs بواسطة الدالة processPDU. يتم الاستجابة على رسالة الإشعار Inform PDU بواسطة استخدام رسالة الاستجابة returnResponsePDU.

- **تطبيق الوكيل المعاون:**

يستخدم دوال المنجز لكي يرسل رسائل "سنمب–ف3". يقوم الوكيل المعاون بمعالجة أربعة أنواع من الرسائل هي:

أ – رسائل تحتوي على أنواع وحدات PDU من تطبيق مولد الأمر. ويحدد آلة "سنمب–ف3" الهدف أو الآلة الأقرب للهدف ويرسل الطلب requestPDU المناسب.

ب – رسائل تحتوي على أنواع وحدات PDU من تطبيق منشئ الإشعار، ويحدد آلة "سنمب–ف3" التي ينبغي أن تستقبل الإشعار، ويرسل الإشعار المناسب لوحدات PDUs.

ج – رسائل تحتوي على نوع استجابة response PDU. ويحدد الطلب المرسل سابقا أو الإشعار. عندما يتوافق مع هذه الاستجابة، يرسل استجابة مناسبة لوحدة PDU.

د – رسائل تحتوي على مبين تقرير report indicator . إن وحدات مبين التقرير تحقق الاتصالات بين آلات بروتوكول "سنمب–ف3". يحدد الوكيل المعاون الطلب المرسل سابقا أو الإشعار، عندما يحدث توافق مع مبين التقرير، يقوم بإرجاع مبين التقرير إلى مرسل initiator الطلب أو الإشعار.

أسئلة تقويم ذاتي

عدد الخصائص الأمنية التي اشتمل عليها بروتوكول SNMPv3.

اذكر مكونات آلة SNMPv3.

يوجد خمسة أنواع من التطبيقات للبروتوكول SNMPv3 اذكرها.

ارسم شكلاً يوضح العمليات التفاعلية بين آلة SNMPv3 ومجموعة التطبيقات ؟.

اذكر أنواع الرسائل المتبادلة بينهما ووظيفة كل منها.

أكمل ما يلي: يستخدم تطبيق مستجيب الأمر أربعة دوال من المراسل ما هي؟

أ) ..... ب) .....

ج) ..... د) .....

يقوم المرسل المعاون بمعالجة أربعة أنواع من الرسائل ما هي ؟

3. نموذج أمن المستخدم USM

يوفر نموذج أمن المستخدم USM للبروتوكول "سنمب–ف3" خدمات التوثيق Authentication، وخدمات الخصوصية Privacy. فقد تم تصميم نموذج USM للحماية من التهديدات Threats الرئيسية ،الموضحة في الشكل2.4 وهي :

- **تعديل المعلومات:**

وذلك لأنه يمكن أن يتم تغيير الرسالة المتولدة أثناء مرورها في محطة التشغيل Entity بواسطة محطة تشغيل أخرى غير مفوضة، ممَّا يؤثر على العمليات الإدارية، ويشمل ذلك تهيئة قيم العناصر (الأجهزة). و تكمن خطورة هذا التهديد في أنه يمكن لمحطة التشغيل غير المفوضة أن تغير أي معاملات إدارية، وقد يشمل ذلك معاملات التهيئة، والتشغيل، والحسابات.

- **التنكر Masquerade:**

حيث يمكن لبعض العمليات الإدارية غير المفوضة لبعض محطات التشغيل، أن تحاول من خلال هذه المحطات فرض هوية Identity المحطة المفوضة.

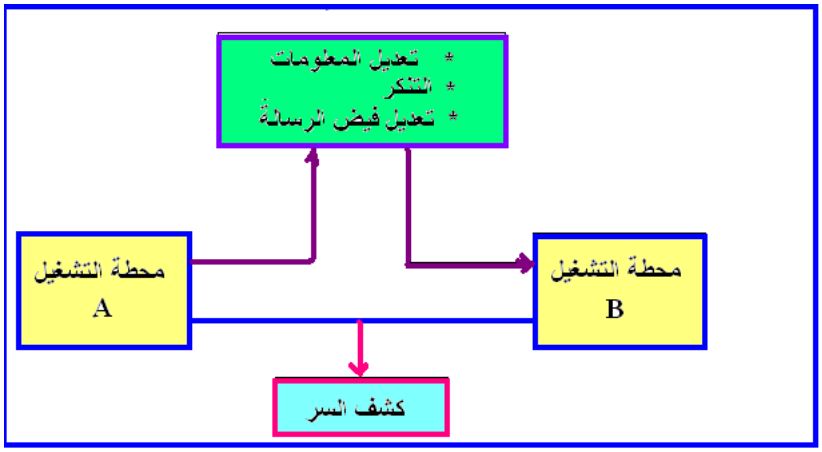
- **تعديل فيض الرسالة Message Stream:**

لقد تم تصميم بروتوكول"سنمب–ف3" لكي يعمل فوق طبقة بروتوكول النقل Transport Protocol في نمط عدم الربط Connectionless. وقد يسبب هذا تهديدا لرسائل بروتوكول "سنمب–ف3" ' إذ يمكن إعادة طلبها Reordered أو تأخيرها، أو عمل نسخة إضافية منها Duplicated ، وتحدث عمليات إدارية غير مفوضة. على سبيل المثال، يمكن أن يتم نسخٍ الرسالة التي تقوم بإعادة تشغيل (Reboot) جهاز، وإعادة تشغيلها Replayed لاحقا.

- **كشف السر Disclosure:**

يمكن لمحطة التشغيل Entity أن تلاحظ المبادلات Exchanges بين المدير والوكيل لكي تتعلم قيم العناصر الإدارية التي يجب أن يتم الإبلاغ عنها. على سبيل المثال، إن

ملاحظة أمر الإعداد set الذي يغير كلمات السر ربما يمكن المقتحم Attacker من تعلم (معرفة) كلمات السر الجديدة.



شكل2.4 تهديدات أمن إدارة المعلومات.

تهديدات أخرى:

يوجد بعض التهديدات الأخرى التي لم يتم تصميم نموذج USM لإجراء عمليات الحماية منها وهي:

- **إنكار الخدمة Denial of Service:**

المقصود بهذا التهديد هو أن يقوم المهاجم بمحاولة منع المستخدم الشرعي من استخدام الشبكة. حيث يقوم المهاجم هنا بمحاولة منع المبادلات التي تتم بين المدير والوكيل. ويحتاج هذا النوع من التهديدات وجود وسائل أمنية أخرى، خلاف الموجودة في بروتوكول إدارة الشبكة.

- **تحليل الحركة Traffic Analysis:**

قد يتمكن المهاجم من مراقبة النموذج العام لحركة مرور الرسائل بين المديرين والوكلاء. إن نماذج تحليل حركة مرور الرسائل يمكن معرفته بواسطة بروتوكول إدارة الشبكة، باستخدام أوامر "سنمب–ف3" على فترات منتظمة. ولذلك لا يوجد ميزة هامة للحماية ضد ملاحظة المهاجم نماذج حركة مرور الرسائل.

وسائل الحماية:

للحماية من التهديدات السابقة فإن نموذج أمن المستخدم USM في بروتوكول "سنمب–ف3" يستخدم بروتوكولين مختلفين للتوثيق هما بروتوكول HMAC-MD5-96 وبروتوكول HMAC-SHA-96. ويستخدم نموذج USM مفتاحين، أحدهما خاص لتحقيق الخصوصية هو privKey، والمفتاح الآخر لتحقيق التوثيق وهو authKey. ويستخدم هذان المفتاحان للمستخدمين المحليين Local Users ، والمستخدمين عن بعد Remote Users. وأن هذين المفتاحين لا يتم تخزينهما في قاعدة المعلومات الإدارية MIB في الشبكة. ولذلك من غير الممكن الوصول إليهما مباشرة من خلال رسائل "سنمب–ف3 get, set ". وسيتم شرح ذلك بالتفصيل في الفقرات التالية.

أسئلة تقويم ذاتي

يوفر نموذج أمن المستخدم USM للبروتوكول "سنمب–ف3" خدمات..... ، وخدمات .....

اذكر التهديدات Threats الرئيسية التي تم تصميم نموذج USM للحماية منها .

أكمل ما يلي :

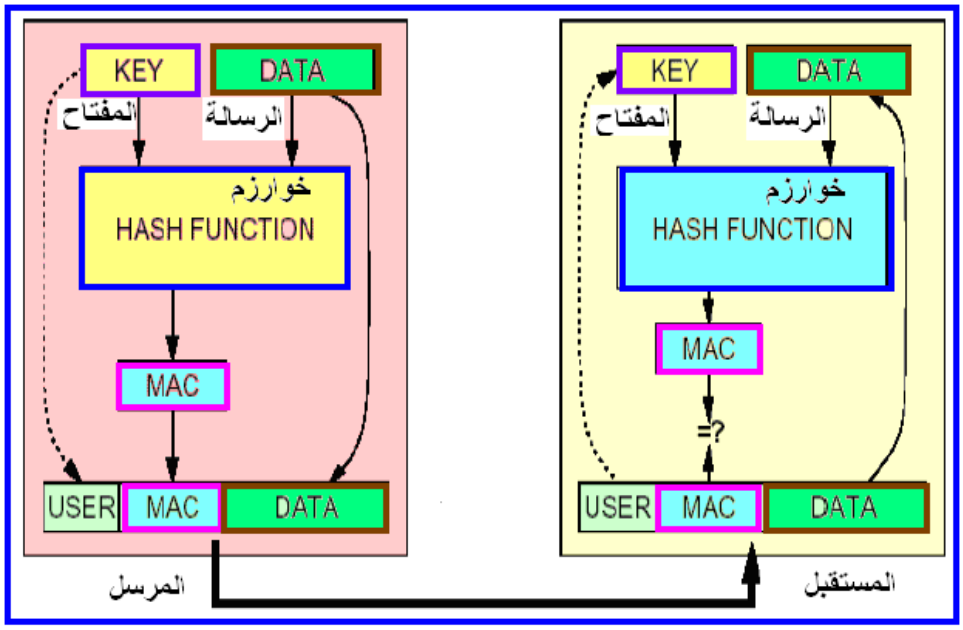
للحماية من التهديدات، فإن نموذج أمن المستخدم USM في بروتوكول SNMPv3 يستخدم بروتوكولين مختلفين للتوثيق هما بروتوكول ..... وبروتوكول ..... ويستخدم نموذج USM مفتاحين، أحدهما خاص لتحقيق الخصوصية هو ..... ، والمفتاح الآخر لتحقيق ..... وهو authKey. ويستخدم هذان المفتاحان للمستخدمين ..... والمستخدمين .....

يوجد بعض التهديدات الأخرى التي لم يتم تصميم نموذج USM لإجراء عمليات الحماية منها:

أحد هذه التهديدات إنكار الخدمة Denial of Service . ما المقصود بهذا التهديد.

1.3 تحقيق التوثيق والتكامل Authentication and Integrity

تحقق طريقة توثيق الرسائل إجراء عمليات الاتصال بين طرفي الاتصال من استقبال رسائل موثقة . وذلك لضمان أن محتويات الرسالة لم يتم تعديلها وأن مصدر الرسالة موثق. وتستخدم تقنية شفرة توثيق الرسالة Message Authentication Code (MAC) لتحقيق عملية توثيق الرسالة. يوضح الشكل 2.5 عملية توثيق الرسالة باستخدام شفرة التوثيق MAC .



شكل2.5 توثيق الرسالة باستخدام شفرة التوثيق MAC.

يستخدم نموذج USM بروتوكول التوثيق HMAC-MD5-96 الذي يستعمل دالة Hash وهي DM5. بينما البروتوكول HMAC-SHA-96 تكون دالة Hash هي SHA-1. يكون مدخل دالة Hash الرسالة المطلوب إرسالها، ومفتاح التوثيق authKey من المستخدم. يكون الخرج الناتج هو شفرة توثيق الرسالة MAC يكون طولها 12 حرف Octets يتم إرسالها مع الرسالة الأصلية.

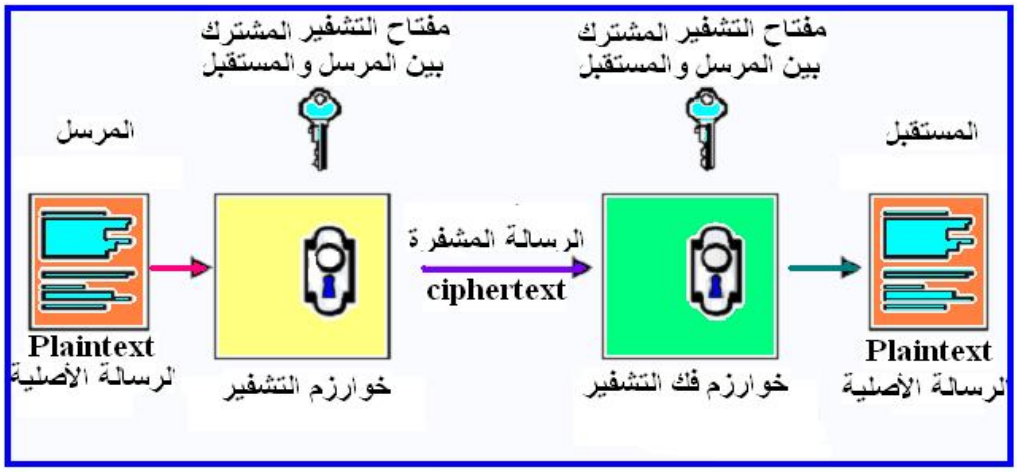
عند طرف الاستقبال، تستخدم الرسالة المستقبلة ومفتاح التوثيق كمدخلات للخوارزم HMAC وذلك لحساب القيمة MAC مثلما تم في مرحلة الإرسال. إذا كانت القيمة المحسوبة MAC هي نفسها القيمة MAC التي تم استلامها مع الرسالة المستقبلة؛ فإن المستقبل يطمئن من شيئين هما:

- صحة وكمال الرسالة، وأنها لم تتغير أثناء عملية الإرسال. حيث إنه ينبغي على المهاجم أن يعرف مفتاح التوثيق كي يستطيع تغيير الرسالة بدون أن يُلاَحظَ.
- التوثيق: لحساب قيمة MAC الصحيحة، فإن المرسل ينبغي أن يعرف المفتاح السري. وعندما يتم معرفة المفتاح السري فقط بواسطة المرسل والمستقبل، فإن أحدهما يستطيع أن يتأكد أن الرسالة المرسلة تم إرسالها بواسطة الطرف المفوض.

2.3 تحقيق الخصوصية بواسطة التشفير

Privacy Through Encryption

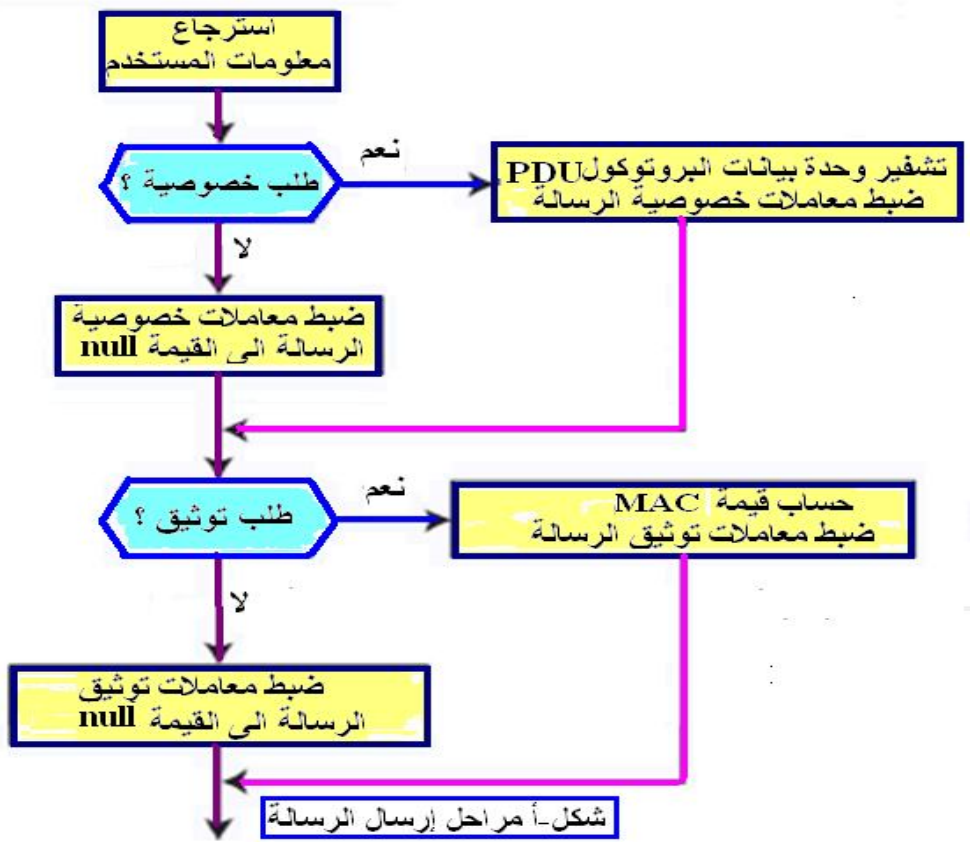
يستخدم نموذج USM الخوارزم القياسي لتشفير البيانات Data Encryption Standard (DES) في تشفير الرسائل وذلك لضمان تحقيق الخصوصية Privacy. ويستخدم مفتاح سري privKey طوله ثمانية حروف لإجراء عملية التشفير . ويوضح الشكل2.6 مراحل إجراء عملية التشفيرEncryption للرسالة الأصلية Plaintext عند الطرف المرسل، وعملية فك التشفير Decryption عند الطرف المستقبل.



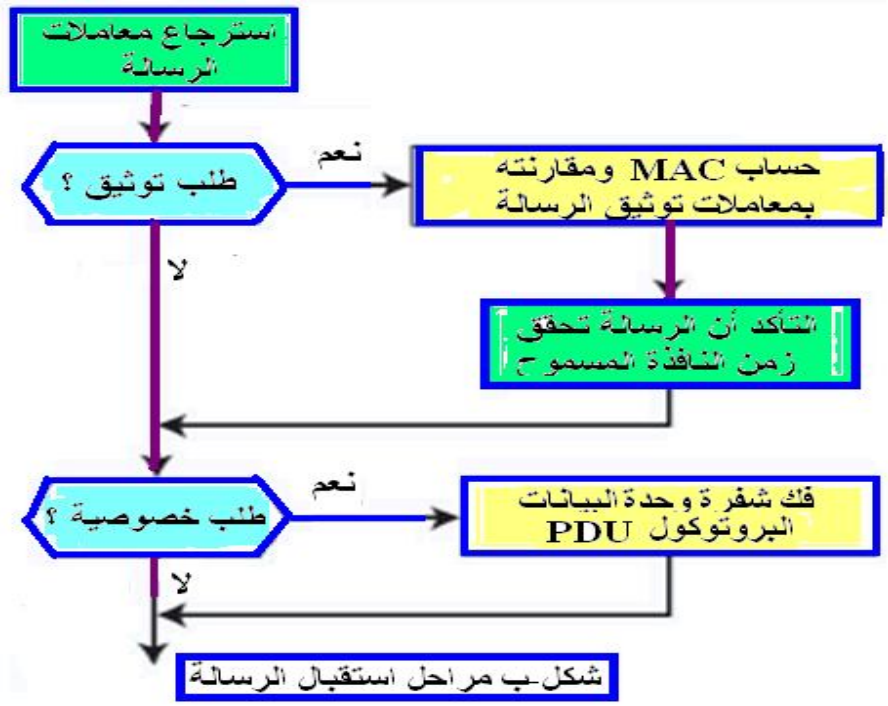
الشكل2.6 مراحل إجراء عملية التشفير.

3.3 معالجة الرسالة في نموذج USM

يوضح الشكل2.7، والشكل 2.8 خريطة التدفق لبيان سير العمليات التي تمر بها الرسالة أثناء معالجتها في نموذج USM في مرحلتي الإرسال والاستقبال، على الترتيب. عندما تمر رسالة خرج outgoing إلى نموذج USM بواسطة معالج الرسالة، فإن USM يضع بها معاملات الأمن ذات العلاقة في مقدمة الرسالة Message Header . وعندما تمر رسالة دخل incoming إلى نموذج USM بواسطة معالج الرسالة، فإن نموذج USM يقوم بمعالجة القيم الموجودة في هذه الحقول البيانية للرسالة، وتشمل معاملات الأمن ذات العلاقة. تكون قيمة معامل الخصوصية هي القيمة المبدئية IV (متجه مبدئي Initial Vector)في خوارزم DES CBC.



شكل2.7 مراحل إرسال الرسالة في نموذج USM.



شكل2.8 مراحل استقبال الرسالة في نموذج USM.

عند إرسال الرسالة إلى نموذج USM يتم تحقيق التشفير أولاً، عند الاحتياج. يتم تشفير وحدة بيانات البروتوكول PDU المستهدفة، ويتم وضعها في حمولة الرسالة. ويتم ضبط قيمة معاملات خصوصية الرسالة إلى القيمة التي تحتاجها لتوليد المعامل IV . بعد ذلك يتم تحقيق التوثيق، عند الحاجة. تعتبر الرسالة بأكملها شاملة وحدة PDU المستهدفة مدخلا إلى HMAC، وتوضع شفرة التوثيق الناتجة في معاملات توثيق الرسالة. ويلخص الجدول2.1 بيان هذه المعاملات.

بخصوص الرسالة القادمة incoming، يتم تحقيق التوثيق أولاً عند الحاجة. يختبر USM أولا الدالة MAC القادمة مع قيمة MAC التي تم حسابها، عندما يحدث توافق بين القيمتين، يدل ذلك على أن الرسالة مفوضة (آتية من مصدر صحيح ولم يتم تعديلها أثناء عملية الإرسال). بعد ذلك يفحص USM ما إذا كانت الرسالة وصلت خلال المدة الزمنية المسموحة بزمن النافذة (للتأكد من عدم تأخير الرسالة بسبب اقتحام مفترض).

إذا لم تكن الرسالة وصلت خلال المدة الزمنية المسموح بها لزمن النافذة، يتم إهمالها، حيث إنها تكون غير مفوضة. أخيراً، إذا تم تشفير وحدة PDU المستهدفة، يقوم نموذج USM بتحقيق فك التشفير وترجيع أصل نص الرسالة Plaintext.

الجدول2.1 معاملات توثيق الرسالة المستخدمة في نموذج USM.

مسلسل	مسمى المعامِل Parameter	وظيفته
1	هوية آلة توثيق الرسالة msgAuthoritativeEngineID	تحدد المصدر المرسل لرسائل سنمب–ف3، وكذلك الهدف المستقبل لها.
2	إعادة تشغيل آلة توثيق الرسالة msgAuthoritativeEngineBoots	يحدد عدد المرات التي يتم فيها إعادة تشغيل آلة سنمب–ف3 منذ بداية تهيئتها.
3	زمن آلة توثيق الرسالة msgAuthoritativeEngineTime	تحدد عدد الثواني منذ توثيق آلة سنمب–ف3 لحظة آخر زيادة لزمن إعادة التشغيل.
4	اسم مستخدم الرسالة msgUserName	المستخدم الرئيسي Principal الذي نيابة عنه يتم تبادل الرسالة.
5	معاملات توثيق الرسالة msgAuthoritativeParameters	تحدد شفرة توثيق الرسالة HMAC. وهي لا تستخدم في حالة عدم التوثيق.
6	معاملات خصوصية الرسالة msgPrivacyParameters	يحدد الخصوصية الموجودة في نموذج USM وقيمته تحدد القيمة المبدئية للمتجه IV المستخدمة في خوارزم التشفير DES CBC.

4.3 توليد المفاتيح السرية

يحتاج خوارزم DES متجهاً مبدئياً Initial Vector (IV) يماثل الحرف الثمانية الأخيرة لمفتاح التشفير privKey . وتكون عملية تشفير الرسائل اختيارية. يتم إرسال مفتاح التشفير محليا عند محطة الإدارة. عندما تستخدم محطات الإدارة مفاتيح سرية مختلفة، فإن المدير ينبغي عليه أن يمتلك نفس عدد هذه المفاتيح. في هذه الحالة، قد تسبب عملية إدارة هذه المفاتيح بسرعة مشكلة. إذا تم اقتحام محطة الإدارة وتعرضت مفاتيح السرية إلى شبهة Compromise، فإن كل مراكز الاتصال في الشبكة nodes ينبغي إعادة تهيئتها يدويا. من ناحية أخرى، يمكن استخدام مفتاح وحيد لكل مراكز اتصال الشبكة التي يتم إدارتها. لكن تكمن مشكلة خطورة إدارة نظام الأمن كله بمفتاح سري وحيد.

في نموذج USM يتم حل هذه المشكلة بواسطة توليد مفتاح محلي Localized Key . حيث يتم إنشاء هذه المفاتيح المحلية وتحديثها وإدارتها لكل مستخدم بواسطة آلة "سنمب–ف3"، وذلك باستخدام كلمة السر المستخدمة من المستخدم، مع هوية آلة سنمب–ف3 snmpEngineID، وهي الهوية الهدف Target لآلة سنمب–ف3.

5.3 توليد المفاتيح المحلية Localized Key

إن المفتاح المحلي هو مفتاح سري يتم مشاركته بين المستخدم U وآلة سنمب–ف3 المفوضة E. عندما يكون للمستخدم كلمة سر واحدة فقط ومفتاح واحد لكل الشبكة؛ فإن الأسرار الفعلية المشتركة بين المستخدم وآلة سنمب–ف3 المفوضة سوف تكون مختلفة. يتم تحقيق ذلك بواسطة المفتاح المحلي.

– عندما يستعمل المستخدم كلمة سر، فإنه يتم تحويل كلمة السر إلى مفتاح Ku باستخدام خوارزم HMAC-DM5 أو خوارزم HMAC-SHA . وذلك لتحويل المفتاح Ku إلى مفتاح محلي Kul للمستخدم U عند آلة سنمب–ف3 المفوضة E.

- يتم إلحاق append هوية آلة سنمب-ف3 snmpEngineID لآلة سنمب-ف3 المفوضة إلى المفتاح Ku . بعد ذلك يتم إلحاق المفتاح Ku إلى الناتج.

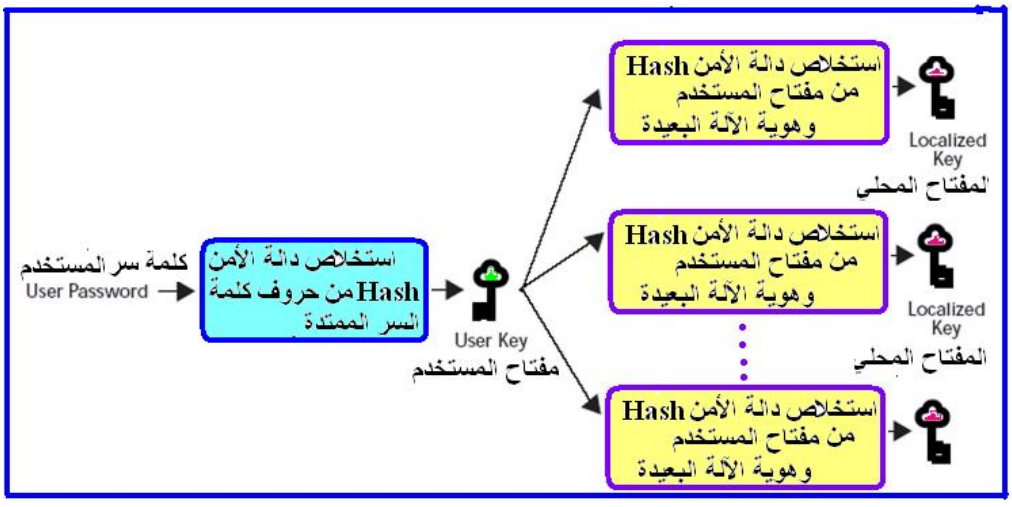
- يتم تغليف هوية آلة سنمب-ف3 من خلال نسختين من مفتاح المستخدم Ku. يتم تشغيل دالة الأمن Hash (التي تعتمد على بروتوكول التوثيق المعرف للمستخدم U عند محطة سنمب-ف3 المفوضة E ، وهما دالة MD5 ودالة SHA.

- يكون خرج دالة الأمن Hash هو المفتاح المحلي Kul للمستخدم U عند محطة سنمب-ف3 المفوضة. يوضح الشكل2.9 المراحل المستخدمة لتوليد المفتاح المحلي.

- **<u>مميزات توليد المفاتيح المحلية:</u>**

- تتميز هذه الطريقة بأنها تبطئ بقيمة كبيرة جدا قوة المعجم الشرس Brute-Force Dictionary الذي يحاول فيه المهاجم العديد من كلمات السر المجهدة، وذلك كي يحصل على المفتاح السري للمستخدم.

- الميزة الأخرى، هي أنها تفك ارتباط Decouple مفاتيح المستخدم من أي نظام إدارة شبكة NMS. حيث لا حاجة لتخزين قيم مفاتيح المستخدم في داخل نظام إدارة شبكة NMS. فبدلا من ذلك - عند الحاجة- يتم توليد مفتاح المستخدم من كلمات سر المستخدم.



شكل2.9 توليد المفاتيح المحلية.

6.3 إدارة المفاتيح السرية

يوجد حلٌّ آخر لتخزين المفتاح السري ،بدلاً من توليده من كلمة السر، وهو الاحتفاظ بمستودع مركزي Centralized Repository للمفاتيح السرية.

لكن هذا يؤثر عدائياً على إجمالي الاعتمادية Reliability ويصعب عملية تشخيص الأعطال Troubleshooting نفسها، حيث يكون المستودع نفسه غير ممكن الوصول إليه عند الحاجة.
من ناحية أخرى، عندما يتم مضاعفة Duplicate مستودعات التخزين، فهذا يعرض إجمالي الأمن للخطر، بسبب توفير أكثر من هدف يمكن مهاجمته.

عندما تستخدم طريقة المستودع المركزي، أو طريقة مضاعفة العديد من المستودعات، فإنه ينبغي أن يتم الاحتفاظ بها في أماكن آمنة.

ينبغي استخدام كلمة سر وحيدة لتوليد مفتاح واحد لكل من التوثيق والتشفير. إن استخدام اثنين من كلمات السر يكون أكثر أمانا ، أحدهما يستخدم لتوليد مفتاح التوثيق، والآخر لتوليد مفتاح تشفير مميز.

إن المفتاح المحلي يحدد مفتاحاً سرياً مشتركاً بين المستخدم وآلة سنمب–ف3 المفوضة. والهدف هو أن المستخدم يحتاج فقط الاحتفاظ بمفتاح واحد (أو مفتاحين لكل من التوثيق والخصوصية) وبذلك يحتاج فقط لتذكر كلمة سر واحدة (أو اثنتين). إن الأسرار الفعلية المشتركة بين مستخدم محدد وآلة سنمب–ف3 المفوضة، يكون مختلفا. إن المعالجة التي

بواسطتها يتم تحويل المفتاح الواحد للمستخدم إلى مفاتيح متميزة عديدة، مفتاحا لكل آلة سنمب–ف3 بعيدة، ترجع إلى المفتاح المحلى.

مما سبق شرحه، يمكن تحديد الأهداف التالية لإدارة المفاتيح:

– إن كل نظام آلة سنمب–ف3 في الشبكة الموزعة يمتلك مفتاحا مميزا لكل مستخدم مفوض لإدارته.

– عندما يوجد العديد من المستخدمين المفوضين للعمل كمديرين، فإن الوكيل يمتلك مفتاحا موثقا مميزا، ومفتاح تشفير مميز لكل مستخدم. بذلك، عندما يتم احتواء المفتاح لمستخدم واحد، فإن مفاتيح المستخدمين الآخرين لا يتم احتواؤها.

– إن مفاتيح المستخدم عند الوكلاء المختلفين تكون مختلفة. بذلك عندما يتم احتواء الوكيل، فإنه يتم فقط احتواء مفاتيح المستخدم لهذا الوكيل وليس مفاتيح المستخدم المستعملة للوكلاء الآخرين.

– يمكن إجراء إدارة الشبكة من أي نقطة في الشبكة، بغض النظر عن الإتاحة المهيأة سابقا في نظام إدارة الشبكة NMS. إن ذلك، يسمح للمستخدم أن ينفذ الأعمال الإدارية من أي محطة إدارة. يتم توفير هذه الإمكانية بواسطة خوارزم تحويل الكلمات السرية إلى مفتاح Password-to-key algorithm ، الذي تم شرحه سابقا.

نستطيع أيضا تحديد النقاط التي ينبغي تجنبها وهي:

– ينبغي على المستخدم أن يتذكر (أو يدير) عدداً ضخماً من المفاتيح ، وهذا العدد ينمو مع إضافة وكلاء إداريين جدد.

– إن العدو Adversary الذي يتعلم مفتاحا لأحد الوكلاء يكون الآن قادرا على تمثيل شخصية Impersonate أي وكيل آخر لأي مستخدم، أو أي مستخدم لأي وكيل آخر.

- **استخدام دالة الطريق الواحد غير العكسي:**

لأخذ الأهداف السابقة بعين الاعتبار، فإنه يتم استخدام مفتاحً واحداً للمستخدم يتم تحويله إلى مفاتيح محلية مختلفة لآلات (وكلاء) مفوضين مختلفين باستخدام "دالة الطريق الواحد غير العكسي" nonreversible-one way function .

وتتم هذه الطريقة كما يلي:

– تكوين حروف digest2 بواسطة سلسلة concatenating لحرف digest1، مع قيمة هوية آلة سنمب–ف3 لآلة مفوضة ، مع digest1 .

– عندما نرغب في مفتاح طوله 16 حرفاً، نأخذ دالة الأمن MD5 من digest2.

وعندما نرغب في مفتاح طوله 20 حرفاً، نأخذ دالة الأمن SHA-1 من digest2.

يكون الخرج بعد ذلك هو المفتاح المحلى.

نستطيع بعد ذلك، تهيئة المفتاح المحلي الناتج في نظام الوكيل بطريقة آمنة. بسبب طبيعة الطريق الأوحد one-way للدالة MD5 والدالة SHA-1 ، فإنه يكون غير مرئي للعدو أن يتعلم مفتاح المستخدم، حتى إذا كان العدو يدبر لاكتشاف المفتاح المحلي.

أسئلة تقويم ذاتي

اشرح مع الاستعانة بالرسم ،كلما أمكنك ذلك، كيف يتم تحقيق توثيق الرسائل والتحقق من صحتها، عندما نستخدم بروتوكول إدارة الشبكة البسيط SNMPv3.

اشرح مع الاستعانة بالرسم، كيف يتم تحقيق الخصوصية Privacy بواسطة التشفير، عندما نستخدم بروتوكول إدارة الشبكة البسيط SNMPv3.

7.3 التحقق من عدم تأخر الرسائل Message Timeliness Verification

إن دالة الأمن Hash المستخدمة في عملية التوثيق التي تم شرحها سابقاً، لا تمنع تأخير الرسائل أو إعادة بثها نتيجة حدوث اقتحام. حيث إنه لا يوجد شيء غير عادي يحدث عادة عند إعادة إرسال الرسائل. لحماية بروتوكول "سنمب–ف3" من هذا النوع من الهجوم، فإن نموذج USM يستخدم طريقة لتحقق من عدم تأخر الرسائل. حيث تتطلب هذه الطريقة أن يقوم بروتوكول "سنمب–ف3" باستلام الرسائل خلال نافذة زمنية Time Window مناسبة.

- **النافذة الزمنية Time Window:**

يحدد بروتوكول "سنمب–ف3" نافذة زمنية مناسبة لاستقبال الرسالة، وذلك لتجنب التأخير، ومهاجمات إعادة بث الرسائل replay attacks. وتعرف بأنها القيمة التي يتم فيها توليد الرسالة نيابة عن أي مستخدم مفوض. وهذه القيمة تكون 150 ثانيةً لكل المستخدمين.

تستخدم طريقة عدم تأخر الرسائل عدادين مصاحبين لكل آلة سنمب–ف3 هما: عداد إعادة تشغيل الآلة snmpEngineBoots ، وعداد زمن الآلة snmpEngineTime. عندما يتم تنصيب آلة سنمب–ف3 (بواسطة برنامج بروتوكول "سنمب–ف3" في المركز الإداري للشبكة)، فإنه يتم ضبط قيم العدادين على القيمة صفر. عندما تبدأ آلة سنمب–ف3 في العمل، فإن عداد زمن آلة سنمب–ف3 يبدأ في الزيادة قيمة واحدة لكل ثانية. عندما يصل عداد آلة سنمب–ف3 للقيمة العظمى وهي $(2^{31} - 1)$ ، فإن عداد إعادة تشغيل آلة سنمب–ف3 يتم زيادته قيمة واحدة أيضا. بعد ذلك يتم ضبط عداد آلة سنمب–ف3 إلى القيمة صفر، وتستمر هذه الدورة.

- **الطريقة التزامنية المركبة:**

تستخدم آلة سنمب–ف3 طريقة تزامنية مركبة عند مركز الاتصال الإداري بالشبكة، لحساب القيم الزمنية لكل مركز اتصال شبكي يتم إدارته بواسطة المدير، الذي يتم إجراء الاتصال معه. ويتم إدراج هذه القيم الزمنية المحسوبة مع كل رسالة خرج. عندما يتم استقبال هذه الرسائل بواسطة آلة سنمب–ف3 في مركز الإدارة، فإنها تقوم بتحديد ما إذا كانت الرسالة القادمة قد استغرقت الوقت المسموح به في النافذة الزمنية (وهو150 ثانية) . إذا استغرقت الرسالة القادمة فترة زمنية أطول من المسموح بها في النافذة الزمنية، فإنه ببساطة يتم إهمال هذه الرسالة.

يجب اختيار زمن النافذة صغيرا كلما أمكن ذلك، بشرط أن تكون الساعة clock المستخدمة دقيقة ،وكذلك التأخير الناتج عن رحلة الاتصال Round-trip Communication Delay، وكذلك التردد الذي يتم عنده تزامن الساعات clocks. إذا تم ضبط زمن النافذة ليصبح أصغر من اللازم، فإن الرسائل الموثقة سوف يتم رفضها مثل الرسائل غير الموثقة. من ناحية أخرى، إذا تم اختيار زمن النافذة كبيراً جداً، فإن ذلك يزيد من تعرض الرسائل للتأخير بسبب مهاجمات سهلة ماكرة Vulnerability to Malicious.

- **شروط إهمال الرسالة:**

تعتبر الرسالة القادمة Incoming Message خارجة عن زمن النافذة، وتعتبر غير موثقة وبالتالي يتم إهمالها ، إذا تحقق أحد الشروط التالية:

أ– أن يكون زمن إعادة تشغيل الآلة قد وصل إلى القيمة العظمي وهى $(2^{31} - 1)$.

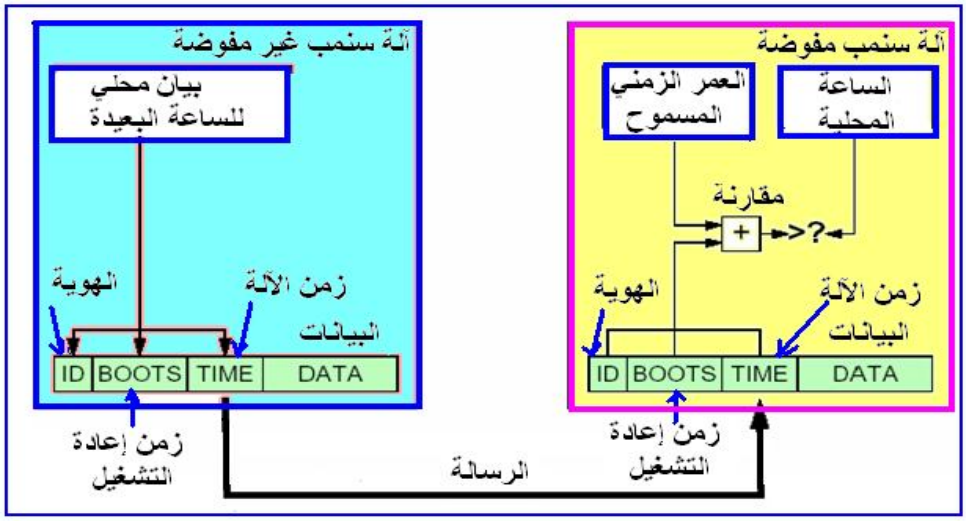
ب– أن يكون زمن إعادة تشغيل الآلة في الرسالة الموثقة غير مطابق لزمن إعادة التشغيل المحلي. على سبيل المثال، إذا تم إعادة تشغيل الآلة المحلية، و لم يتم تزامنها مع الآلة البعيدة عند لحظة إعادة التشغيل.

ج- أن يكون زمن آلة سنمب-ف3 في الرسالة الموثقة القادمة يختلف عن زمن آلة سنمب-ف3 المحلي بقيمة أكبر من أو أصغر من 150 ثانية.

في هذه الحالات السابقة تكون الرسالة خارج النافذة الزمنية، وتعتبر الرسالة غير موثقة، ويتم إرجاع بيان خطأ notInTimeWindow إلى برنامج الاتصال calling module.

8.3 التوقيت المتزامن Time Synchronization

تحتاج آلة سنمب-ف3 غير المفوضة إجراء تزامن للتوقيت لكي تستمر في اتصالاتها المفوضة، وذلك عندما تحصل على بيان محلي Local Notion لكل من زمن إعادة تشغيل آلة سنمب-ف3، وزمن آلة سنمب-ف3 من محطة مفوضة. وأن تكون هذه الأزمنة مطابقة للقيمة المسموح بها في النافذة الزمنية لآلة سنمب-ف3 المفوضة، كما موضح في الشكل2.10. كما ينبغي أن يكون بيان هذه القيم الزمنية المحلية متزامناً بحرية Loosely مع القيم المخزنة في آلة سنمب-ف3 المفوضة. بالإضافة إلى احتفاظ آلة سنمب-ف3 غير المفوضة بنسخة محلية من أزمنة إعادة التشغيل ، وزمن الآلة من آلة سنمب-ف3 المفوضة. كما أنها يجب أن تحتفظ بقيمة متغير آخر أيضا هو آخر زمن استقبال للآلة latestReceivedEngineTime. تسجل هذه القيمة أعلى زمن لآلة سنمب-ف3 من محطة مفوضة. ويستخدم لمنع إمكانية إعادة تشغيل Replaying الرسائل التي قد تمنع بيان زمن آلة سنمب-ف3 غير المفوضة من التقدم Advancing. بما أن كل آلة سنمب-ف3 مفوضة تكون مميزة ومحددة بواسطة معامل هوية الآلة snmpEngineID، فإن آلة سنمب-ف3 غير المفوضة قد تستعمل هذه الهوية كمفتاح لتخزين to cache القيم المحلية لزمن إعادة التشغيل، وزمن الآلة.



شكل2.10 عملية "تزامن التوقيت" اللازم لاتصال آلة مفوضة وآلة غير مفوضة.

يحدث تزامن التوقيت كجزء من عملية استقبال رسائل سنمب–ف3. ولا يقتضي الأمر وجود طريقة تزامن محددة كي تستخدمها لآلة سنمب–ف3 غير المفوضة. إذا تم تغيير القيمة المحلية لهوية آلة سنمب–ف3، فإن القيم المحلية لأزمنة إعادة التشغيل، وآخر زمن استقبال، يجب ضبطهما على القيمة صفر. وهذا يسبب إجراء عملية التزامن ، ويتم ذلك عند استقبال رسالة موثقة تالية. لتمكين آلة سنمب–ف3 غير المفوضة من إجراء التزامن؛ فإن كل آلة مفوضة تضع قيمها الحالية لأزمنة إعادة التشغيل، وزمن الآلة، وكذلك الهوية ID في كل رسالة استجابة، أو تقرير، أو مصيدة تكون قادمة، كما موضح في الشكل2.10. وذلك داخل حقول الرسالة الخاصة بهذه المعاملات، **والتي تشمل ما يلي:**

أ– **زمن إعادة التشغيل** في رسالة آلة سنمب المفوضة
. msgAuthoritativeEngineBoots

ب – **زمن الآلة** في رسالة سنمب– ف3 المفوضة
.msgAuthoritativeEngineTime

ج – **هوية الآلة** في رسالة سنمب– ف3 المفوضة msgAuthoritativeEngineID

إذا كانت الرسالة موثقة، وأن هذه القيم الزمنية مطابقة لزمن النافذة، فإنه يتم تحديث update هذه القيم عندما يتم استقبالها من آلة غير مفوضة. **يتم إجراء تحديث update هذه القيم طبقا للقواعد التالية:**

- **عندما يتحقق على الأقل أحد الشرطين التاليين:**

أ- إذا كانت قيمة زمن إعادة التشغيل في رسالة آلة سنمب-ف3 المفوضة قد زاد منذ التحديث الأخير.

ب- إذا كانت قيمة زمن إعادة التشغيل في رسالة آلة سنمب-ف3 المفوضة يساوي زمن إعادة التشغيل لآلة سنمب-ف3، وأن يكون زمن الآلة القادم في رسالة آلة سنمب-ف3 المفوضة أكبر من زمن الآلة المستقبل أخيراً.

يكون زمن الآلة القادم أصغر من زمن الآلة المستقبل أخيرا، عندما تصل رسالتان قادمتان غير نظامية out of order (وهذا يمكن أن يحدث)، أو عند عودة هجوم attack قادم في كلا الحالتين فإن آلة الاستقبال سوف لا تنجز التحديث.

- **- عندما يطلب إجراء التحديث، فإنه يتم تنفيذ التغييرات التالية:**

أ- ضبط زمن إعادة تشغيل الآلة كي يساوى القيمة الموجودة في زمن إعادة تشغيل الرسالة الموثقة.

ب- ضبط زمن الآلة إلى القيمة الموجودة في زمن آلة الرسالة الموثقة.

ج- ضبط زمن الآلة لآخر قيمة مستقبلة إلى قيمة زمن آلة الرسالة الموثقة.

بفرض أنه تم تغيير الشروط المنطقية السابقة، أي عندما يكون زمن إعادة التشغيل في رسالة آلة سنمب-ف3 المفوضة أصغر من زمن إعادة تشغيل آلة سنمب-ف3، في هذه الحالة لا يحدث تحديث. وأن هذه الرسالة تعتبر غير موثقة ويجب إهمالها. عندما يكون زمن إعادة التشغيل في رسالة آلة سنمب-ف3 المفوضة يساوي زمن إعادة تشغيل آلة سنمب-ف3، ولكن زمن إعادة التشغيل في رسالة آلة سنمب-ف3 المفوضة يكون أصغر من زمن آلة سنمب-ف3 المستقبل أخيراً، في هذه الحالة أيضاً لا يتم تنفيذ

التحديث. ربما تكون الرسالة؛ في هذه الحالة موثقة، لكنها ربما تكون غير منظمة Disordered، وبالتالي يكون تحديث زمن آلة سنمب–ف3 غير مباح.

تذكر أنه، يتم تطبيق التزامن فقط، عندما تكون خدمة التوثيق مستخدمة في الرسالة، وأن الرسالة تم توثيقها من خلال بروتوكول التوثيق HMAC. وهذا القيد restriction ضروريٌ لأن مجال التوثيق يحتوي على معاملات تشمل: هوية آلة توثيق الرسالة، وزمن إعادة تشغيل الرسالة الموثقة، وزمن آلة الرسالة الموثقة، على فرض أن هذه القيم صحيحة.

9.3 اختيار الآلات الموثقة

إن أحد محطات التشغيل Entities (مرسل أو مستقبل) لأي رسالة مرسلة ينبغي اختيارها Designate لتعمل آلة سنمب– ف3 مفوضة (موثقة)، طبقاً للقواعد التالية:

أ – عندما تحتوي رسالة سنمب–ف3 على حمولة Payload تتوقع استجابة، على سبيل المثال، مثل رسائل(Get, GetNext, GetBulk, Set, or Informed) فإن المستقبل في هذه الحالة يتم تعيينه ليكون مفوضا Authoritative.

ب – عندما تحتوي رسالة سنمب–ف3 على حمولة لا تتوقع استجابة، على سبيل المثال، مثل رسائل (snmpv2-Trap, response, ReportPDU)، لذلك فإن مرسل هذه الرسائل يختار ليكون مفوضاً.

ومن ثم، فإن الرسائل المرسلة نيابة عن مولد الأمر، ورسائل المعلومات المرسلة من منشئ الإشعار، نجد أن المستقبل يعمل مفوضا. كما أن الرسائل المرسلة نيابة عن

مستجيب الأمر، أو رسائل المصيدة من منشئ الإشعار فإن الراسل يعين مفوضا. **وهذا التعيين يخدم غرضين هما:**

أ- أن زمن تأخير الرسالة يتم تحديده بالرجوع إلى الساعة clock الموجودة في الآلة المفوضة. عندما ترسل آلة مفوضة رسالة (مصيدة ، استجابة، أو تقرير) فإنها تحتوي على القيمة الحالية لهذه الساعة لذلك يستطيع الاستقبال غير المفوض ضبط تزامنه مع هذه الساعة. عندما ترسل الآلة غير المفوضة رسالة (Get, GetNext, GetBulk, Set, or Inform) فإنها تحتوي على القيمة التقديرية الحالية للزمن عند الهدف، وبذلك تسمح للهدف بتقدير assess زمن تأخير الرسالة.

ب- إن معالجة المفتاح المحلي (التي تم شرحها في الفقرات السابقة) ، تمكن مستخدم رئيسي واحد من أن يمتلك مفاتيح تخزن في آلات عديدة، وأن هذه المفاتيح تكون محلية في الآلات المفوضة بطريقة بحيث يكون المستخدم الرئيسي مسئولا عن مفتاح واحد، ولكن يتجنب مخاطر الأمن المتعلقة بتخزين نسخ عديدة من نفس المفتاح في الشبكة الموزعة.

إنه من المعقول أن يعين مستقبل مولد الأمر، ووحدات البيانات البروتوكولية PDUs كآلات مفوضة، وبذلك تكون مسئولة عن فحص زمن تأخير الرسالة. عندما يتم تأخير أو إعادة بث رسالة استجابة أو مصيدة، فإن القليل من الأذى ينبغي وقوعه. لكن فإن مولد الأمر- إلى حد ما- يعلم وحدات PDUs الناجمة عن العمليات الإدارية، مثل قراءة أو ضبط عناصر قاعدة المعلومات الإدارية MIB. وبذلك يكون من المهم أن نضمن ألا يتم تأخير أو إعادة بث وحدات PDUs التي قد تسبب تأثيرات غير مرغوب فيها.

أسئلة تقويم ذاتي

اذكر معاملات توثيق الرسالة المستخدمة في نموذج USM ، ووظيفة كل منها.

اشرح، مع الاستعانة بالرسم، كيف يتم توليد المفاتيح المحلية في بروتوكولSNMPv3 .

ما مميزات توليد المفاتيح المحلية.

اشرح كيف يتم التحقق من عدم ؟.

هناك شروط محددة إذا تحقق أحد هذه الشروط تعتبر الرسالة القادمة Incoming Message خارجة عن زمن النافذة، وتعتبر غير موثقة وبالتالي يتم إهمالها، ما هي هذه الشروط.

4. نموذج تحكم الوصول لرؤية المعلومات VACM

يستخدم نموذج "فاكم VACM" للتحكم في الدخول لإدارة العناصر في قاعدة المعلومات الإدارية MIB . يوجد هذا النموذج داخل النظام الفرعي لتحكم الدخول Access Control Subsystem. يكون مسئولاً في آلة "سنمب–ف3" عن فحص و سماحية نوع محدد من العناصر لإجراء عملية (كتابة، قراءة أو إعلام). ويعمل نظام "فاكم" عندما يقوم "سنمب–ف3" بإجراء عملية استرجاع أو تعديل طلب رسائل من محطة التشغيل Entity . على سبيل المثال، يقوم تطبيق مستجيب الأمر بتطبيق تحكم الدخول عندما يعالج الطلبات Requests التي يستقبلها من تطبيق مولد الأمر. تشمل هذه الطلبات أنواع العمليات التالية(GetRequest, GetNextRequest, GetBulkRequest, SetRequest

يعمل نظام تحكم الدخول للمعلومات أيضا داخل محطة تشغيل "سنمب–ف3" ، عندما يتم توليد رسالة إشعار بواسطة تطبيق منشئ الإشعار. وتشتمل هذه الرسائل على أنواع العمليات التالية (InformRequest, SNMPv2-Trap).

يحدد نموذج "فاكم" مجموعة من الخدمات التي يستطيع التطبيق (مثل مستجيب الأمر، أو منشئ الإشعار) استخدامها لفحص حقوق الدخول access rights . يكون من مسئولية التطبيق أن يقدم خدمةً مناسبةً للنداءات calls التي ترد إليه لفحص سماحية الدخول لتصفح المعلومات.

1.4 مخزن البيانات المهيأ محليا

Local Configuration Data-store (LCD)

تحتاج محطة تشغيل "سنمب–ف3" أن تحتفظ بمعلومات عن نظم policies وحقوق الدخول التي يتطلبها نموذج "فاكم" ويعمل على تنفيذها. وتكون هذه المعلومات جزءاً من مخزن بيانات مهيأ محليا LCD لآلة "سنمب–ف3". ولكي يسمح بتهيئة وحدة LCD عن بعد، فإن جزءاً منها يحتاج أن يكون الدخول إليه ممكناً إذ أنها عناصر إدارية. تشمل هذه العناصر الإدارية: قاعدة المعلومات الإدارية المهيئة لنموذج فاكم، و نموذج قاعدة المعلومات الإدارية MIB Module. والتي سيتم شرحهما تباعاً في الفقرات التالية.

2.4 العناصر المكونة لنموذج "فاكم" VACM

يختص نموذج "فاكم" بخاصتين هامتين هما:

أ– أنه يحدد سماحية دخول "مستخدم رئيسي بعيد" لعنصر إداري لقاعدة المعلومات المحلية.

ب– أنه يحدد نظام Policy تحكم الدخول لوكيل، لإمكانية إجراء التهيئة عن بعد.

وذلك باستخدام قاعدة المعلومات الإدارية MIB.

لقد تم تعريف خمسة عناصر لتكوين نموذج "فاكم" هي:

- المجموعات Groups – مستوى الأمن Security Level
- السياق Context – مرئيات قاعدة المعلومات الإدارية MIB Views
- نظام الدخول Access Policy .

- **أولا: المجموعات Groups**

تعرف المجموعة على أنها فئة set من المستخدمين تتكون من صفرٍ مستخدم أو أكثر، والتي نيابة عنها تستطيع عناصر إدارة "سنمب–ف3" الدخول. يتم تحديد المجموعة باستخدام اسم أمني securityName، ونموذج أمني securityModel.

يشير الاسم الأمني إلى مستخدم رئيسي a Principal ، والى حقوق الدخول Access Rights لكل الرؤساء وذلك لتحديد مجموعة معينة لتكون مطابقة identical. يتم تخصيص اسم مميز لكل مجموعة groupName . تفيد هذه الطريقة في أنها تستخدم كأداة لتصنيف المديرين طبقا لأحقية الدخول. على سبيل المثال، يمكن إعطاء جميع المديرين في مستوى القمة top-level فئة أحقية دخول واحدة، بينما يمكن إعطاء المديرين في المستوى المتوسط intermediate-level فئة أحقية دخول مختلفة.

تستطيع مجموعة معينة لها (اسم أمني، ونموذج أمني) أن تنتمي إلى مجموعة واحدة على الأكثر. بمعنى أنه، يعين هذا الوكيل رئيسا principal تكون اتصالاته محمية بواسطة نموذج الأمن. تستطيع مجموعة واحدة فقط استخدامه.

- **ثانيا: مستوى الأمن Security Level**

قد تختلف حقوق الدخول لمجموعة، ويعتمد ذلك على المستوى الأمني للرسالة التي يشملها الطلب request. على سبيل المثال، يمكن السماح لوكيل بإجراء عملية الدخول للقراءة فقط read-only وذلك لطلب اتصال قادم من رسالة غير موثقة، لكن قد يحتاج هذا الطلب توثيقا لإجراء عملية الدخول للكتابة write-access . بالإضافة لعناصر حساسة معينة؛ قد يحتاج الوكيل أن تتم عملية اتصال للطلب واستجابته باستعمال خدمة الخصوصية Privacy Service.

- **ثالثا: – السياق Context**

إن سياق قاعدة المعلومات الإدارية هو اسم لفئة تابعة لمثيلات العناصر Object Instances داخل قاعدة المعلومات الإدارية المحلية. وهو يتيح وسيلة مفيدة لتصنيف العناصر إلى مجموعات يكون لها أنظمة Policies دخول مختلفة. حيث إن السياق هو مفهوم Concept له علاقة بالتحكم في الدخول. مثلاً، عندما يتم الاتصال بين محطة إدارية مع وكيل من أجل الوصول إلى المعلومات الإدارية عند الوكيل، فإنه يحدث اتصال بين الرئيس Principal الإداري وآلة وكيل "سنمب–ف3"، ويتم تخصيص منح امتيازات Privileges تحكم الدخول إلى مرئيات MIB المختص بها الرئيس الإداري لهذا السياق.

- **خصائص السياق**

يختص السياق بعدة خصائص هي:

– يتم تخصيص هوية آلة سياق contextEngineID a مميزة لمحطة تشغيل "سنمب–ف3" والتي تحتوي على أكثر من سياق.

– قد يظهر العنصر أو مثيله في أكثر من سياق .

– لكي يتم تحديد مثيل عنصر منفرد ضمن سياقات متعددة ؛ فإنه ينبغي أن يتـــم تحديد اسم السياق contextName، وهوية آلة السياق contextEngineID، بالإضافة إلى: نوع العنصر مثيل العنصر.

رابعا: مرئيات قاعدة المعلومات الإدارية MIB Views

هي تمثل الحالة التي نرغب في وضع القيود على الوصول إليها، بواسطة مجموعة معينة لفئة من العناصر الإدارية عند الوكيل. لتحقيق هذا الهدف، فإن دخول السياق يتم بواسطة مرئية MIB، والتي تحدد فئةً محددةً من العناصر الإدارية (ومثيلاتها الاختيارية). يستخدم "فاكم" تقنية قوية ومرنة لتعريف مرئيات MIB المبنية باستخدام الشجرات الفرعية sub trees وعائلاتها.

يتم تحديد مرئية MIB بدلالة المجموعة Collection، أو العائلة Family، أو الشجرات الفرعية.

يتم تنظيم العناصر الإدارية في قاعدة البيانات المحلية على شكل هرمي hierarchical، أو شجرة، بناء على محددات العنصر Object Identifier. تحتوي قاعدة المعلومات المحلية على فئة فرعية من كل أنواع العناصر المعرفة طبقاً لهيكل المعلومات الإدارية SMI القياسي للإنترنيت.

يستخدم بروتوكول "سنمب– ف3" تنظيمة الشجرة الفرعية، وهي عبارة عن مركز اتصال (قطب Node) في المسمى الهرمي لقاعدة المعلومات الإدارية، بالإضافة إلى جميع العناصر التابعة Subordinate لها. ويمكن تعريف الشجرة الفرعية بطريقة نظاميةعلى أنها فئة من كل العناصر، ومثيلات العناصر التي لها "محدد عنصر أسن–1–شائع" common ASN.1 object identifier يشير إلى بادئة prefix أسمائهم. يكون أكبر بادئة شائع في كل مثيلات الشجرة الفرعية هو محدد عنصر القطب الأب Parent Node لهذه الشجرة الفرعية.

يصاحب كل مدخل في جدول دخول "فاكم" ثلاثة مرئيات MIB ، هي: مداخل الدخول للقراءة read، والكتابة write ، والإعلام (أو التبليغ) notify.

يتم تخصيص كل شجرة فرعية للمرئية في قاعدة المعلومات الإدارية لتكون إما مشمولة Included، أو مستبعدة Excluded. بمعنى أن، مرئية MIB إما أن تشمل وإما أن تستبعد كل مثيلات العنصر التي تحتويها تلك الشجرة الفرعية. بالإضافة إلى ذلك، فإنه يتم تحديد قناع للمرئية View Mask لكي يتم تقليل كمية معلومات التهيئة المطلوبة عندما يتم طلب تحكم دخول دقيق Fine-Grained (تحكم دخول إلى مستوى مثيل العنصر).

خامسا: نظام الدخول Access Policy

يمكن لنموذج "فاكم" تمكين محطة "سنمب–ف3" وتهيئتها لكي تجبر Enforce فئة حقوق دخول محددة. يعتمد هذا الدخول على عدة عوامل هي ما يلي:

- **الرئيس The Principal**

الرئيس The Principal هو الذي يطلب الدخول. من الممكن أن يتيح "فاكم" الإمكانية لوكيلٍ كي يسمح بامتيازات دخول مختلفة لمستخدمين مختلفين. على سبيل المثال، يمكن أن يكون مدير النظام مسئولاً عن تهيئة شبكة إقليمية، والسماح له بتفويضٍ أكثر لتغيير بنودٍ في قاعدة المعلومات الإدارية المحلية. بينما يسمح لمدير آخر بمستوىً متوسطٍ لمسئولية الرصد Monitoring، وذلك لإجراء الدخول للقراءة فقط، والدخول المحدود فقط لفئةٍ فرعيةٍ من قاعدة المعلومات الإدارية المحلية. وكما تم شرحه سابقاً، فإن الرؤساء Principals يتم تخصيصها إلى المجموعات، وأن نظام الدخول يتم تحديده طبقا للمجموعات.

- **مستوى الأمن Security Level**

يكون مستوى الأمن هو الذي يتم بواسطة اتصال طلب من رسالة "سنمب–ف3" . ثم يطلب الوكيل استخدام التوثيق للرسائل التي تحتوي على طلب إعداد set request (مثلا: عملية كتابة).

- **نموذج الأمن Security Model**

يستخدم نموذج الأمن لمعالجة طلب الرسالة. عندما يتم تنفيذ نماذج أمن عديدة عند الوكيل، ربما يتم تهيئته لكي يتيح مستويات دخول مختلفة لطلبات الاتصال، وذلك بواسطة معالجة الرسائل باستخدام نماذج أمن مختلفة. على سبيل المثال، يمكن السماح بدخول بنود معينة ، إذا كان طلب الرسالة قادما من خلال نموذج الأمن USM، وغير مسموح الدخول عندما يكون نموذج الأمن قادما من بروتوكول "سنمب–ف1".

- **سياق قاعدة المعلومات الإدارية MIB context للطلب.**

- **مثيل العنصر Object Instance**

هو مثيل لعنصر محدد يتم طلب الدخول إليه. إن بعض العناصر تحتوي معلومات حرجة أو حساسة أكثر من غيرها، لذلك فإن نظام الدخول ينبغي أن يعتمد على أنه يتم طلب هذا المثيل بذاته.

- **نوع الدخول Access Type**

تنقسم أنواع طلبات الدخول إلى ثلاثة هي: قراءة، كتابة ، إشعار. وهي عمليات إدارية متميزة Distinct ، وربما تُطبق نظمَ تحكُّمِ دخولٍ مختلفةٍ لكل عملية من هذه العمليات.

5. معالجة تحكم الدخول

Access Control Processing

يقوم تطبيق "سنمب–ف3" ببدء تشغيل invoke نموذج "فاكم" من خلال الدالة isAccessAllowed ، ومعاملات الإدخال التالية:

أ– اسم السياق contextName .

ب– نموذج الأمن securityModel .

ج– اسم الأمن securityName .

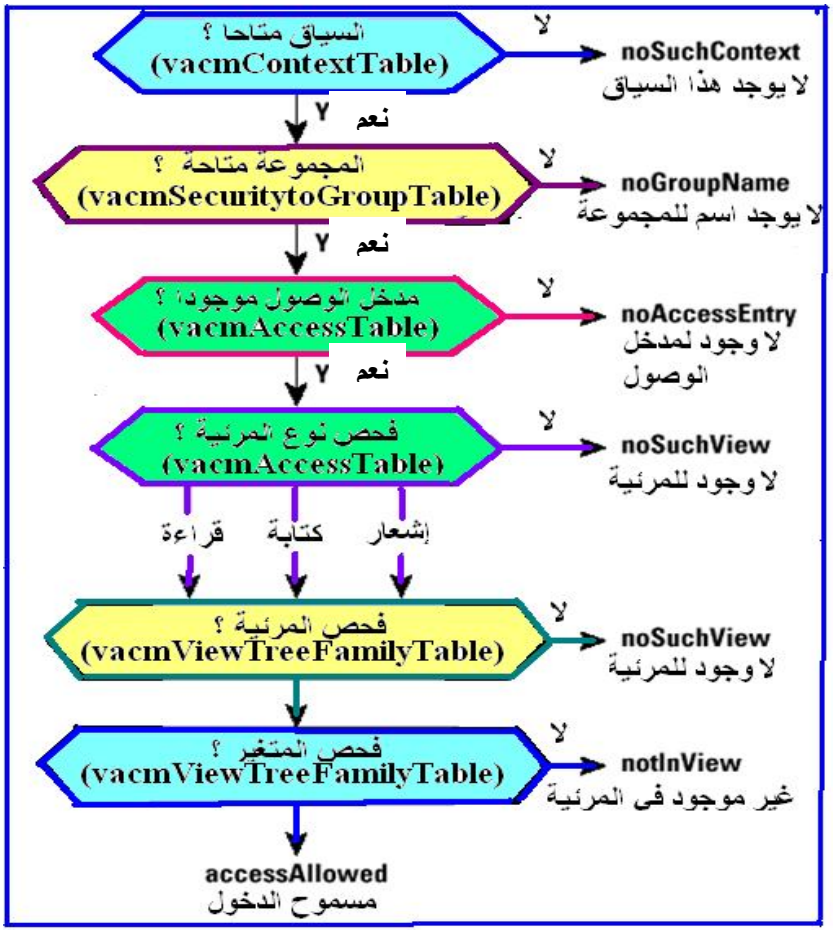
د– مستوى الأمن securityLevel .

هـ– نوع المرئية viewType .

و– اسم المتغير variableName .

1.5 العمليات المنطقية في نموذج "فاكم"

إن جميع المعاملات السابقة يتم الاحتياج إليها من أجل اتخاذ قرار تحكم الدخول. يوضح الشكل2.11 خريطة سير العمليات المنطقية التي يعمل بها نموذج "فاكم" ، ويمكن تلخيصها فيما يلي:



الشكل2.11 العمليات المنطقية التي يعمل بها نموذج "فاكم".

أ- يشير **اسم السياق** إلى مسمى فئة فرعية في عناصر قاعدة المعلومات الإدارية عند الوكيل. يفحص "فاكم" إن كان يوجد مدخل Entry في "جدول سياق فاكم" لاسم السياق المطلوب. إذا وجد المدخل، فإنه يكون قد تم معرفة السياق لآلة سنمب-ف3. إذا لم يوجد المدخل، فإنه يتم إرجاع رسالة بيان خطأ errorIndication إلى الراسل لتبين أنه لا يوجد هذا السياق noSuchContext.

ب- كل عملية يقوم بها الرئيس تتم **لنموذج أمني** معلوم، لمجموعة واحدة على الأكثر، وتحدد التهيئة امتيازات الدخول على أساس المجموعة. يفحص "فاكم" "جدول مجموعة أمن فاكم" لتحديد ما إذا كان تم طلب تخصيص مجموعة. إذا تم ذلك، فإن هذا الرئيس

يقوم بالعمل تحت نموذج الأمن المعطى، ويكون عضواً في المجموعة المهيأة عند آلة سنمب–ف3 هذه. إذا لم يتم، فإنه يتم إرجاع إشارة بيان خطأ تبين أنه لا يوجد اسم للمجموعة.

ج– يستفسر نموذج "فاكم" بعد ذلك من "جدول دخول فاكم" باسم المجموعة، واسم السياق، ونموذج الأمن، **ومستوى الأمن** (الذي يبين التوثيق، والتوثيق مع الخصوصية، أو ليس أي منهما) وتستخدم هذه المتغيرات ككشافات indices معينة في البحث. عندما يوجد مدخل، فإن نظام تحكم الدخول يكون قد تم تحديده بواسطة اسم المجموعة التي تعمل عند نموذج الأمن المعطى في هذا المستوى الأمني. إذا لم يتم إيجاد مدخل، فإنه يتم إرسال إشارة بيان خطأ، تبين عدم وجود مدخل للدخول noAccessEntry.

د– إن مرئية قاعدة المعلومات الإدارية هي عبارة عن هيكل لفئة فرعية من السياق. يحدد "فاكم" ما إذا كان "مدخل جدول دخول فاكم" يشتمل على مرجعية إلى **مرئية MIB** ونوع مرئية (قراءة – كتابة – إبلاغ notify). إذا كان الأمر كذلك، يكون هذا المدخل محتوياً على اسم المرئية viewName لهذا الاتحاد المتكون من:

اسم المجموعة groupName، اسم السياق contextName، نموذج الأمن securityModel ، مستوى الأمن securityLevel ، نوع المرئية viewType.

إذا لم يكن الأمر كذلك، يتم إرجاع بيان خطأ ليوضح عدم إيجاد هذه المرئية noSuchView.

هـ– يستخدم اسم المرئية (من الخطوة السابقة) كشافا index في "جدول عائلة شجرة المرئية" . إذا وجدت مرئية MIB ، يكون قد تم تهيئتها لاسم المرئية المعطى. إذا لم توجد المرئية، يتم إرجاع بيان خطأ يوضح عدم وجود هذه المرئية noSuchView.

و– يفحص "فاكم" **اسم المتغير** variableName مقابل مرئية MIB التي تم اختيارها. إذا شملت المرئية على هذا المتغير، يتم إرجاع بيان حالة statusInformation ليوضح سماحية الدخولaccessAllowed . إذا لم تحتوي المرئية على هذا المتغير، يتم إرجاع بيان خطأ ليوضح عدم وجود هذا المتغير في المرئية notInView.

2.5 تحقيق العمليات المنطقية داخل نظام "فاكم"

يمكن شرح تحقيق العمليات المنطقية داخل نظام "فاكم"، بطريقة سهلة، يتم تحديدها بواسطة النظام الفرعي subsystem للتحكم في الدخول. ويتم ذلك بتوفير أداة مرنة جدا لتهيئة تحكم الدخول عند الوكيل، وذلك بتقسيم مكونات قرار تحكم الدخول إلى ستة متغيرات منفصلة. يوضح الشكل2.12 هذه الطريقة، حيث يتم إدخال متغيرات الدخول منفصلة إلى جداول مختلفة في قاعدة المعلومات الإدارية لنموذج "فاكم" تعين في اتخاذ قرار الدخول. وتشمل هذه المتغيرات ما يلي:

من who: (تحديد المجموعة)

يتم تحديد العملية "من" باتحاد كل من اسم الأمن، ونموذج الأمن . يتم تحديد رئيس معطى تكون اتصالاته محمية بواسطة نموذج الأمن المعطى. وهذا الاتحاد combination ينتمي على الأغلب إلى مجموعة واحدة عند آلة سنمب–ف3.

أين where: (تحديد المكان)

يحدد اسم السياق أين نجد العنصر الإداري المرغوب. يحتوي "جدول سياق فاكم" على قائمة بأسماء السياقات التي يمكن التعرف عليها.

كيف how :(مدى السرية/الحماية)

بواسطة اتحاد كل من مستوى الأمن، ونموذج الأمن يتم تحديد كيفية حماية الطلب القادم، أو رسالة إعلام وحدة PDU قادمة، وأن الاتحاد الثلاثي بين "من" ، "أين" ، و "كيف" يحدد المدخل صفراً، وهو مدخل واحد إلى "جدول دخول فاكم".

لماذا why: (تحديد هدف الدخول)

يحدد "نوع المرئية" لماذا تم طلب الدخول: لأجل عملية قراءة، كتابة، أم تبليغ notify. يحتوي المدخل الذي تم اختياره في "جدول دخول فاكم" اسم مرئية قاعدة معلومات إدارية واحدة لكل ثلاثة أنواع من هذه العمليات، ويستخدم نوع المرئية لاختيار اسم

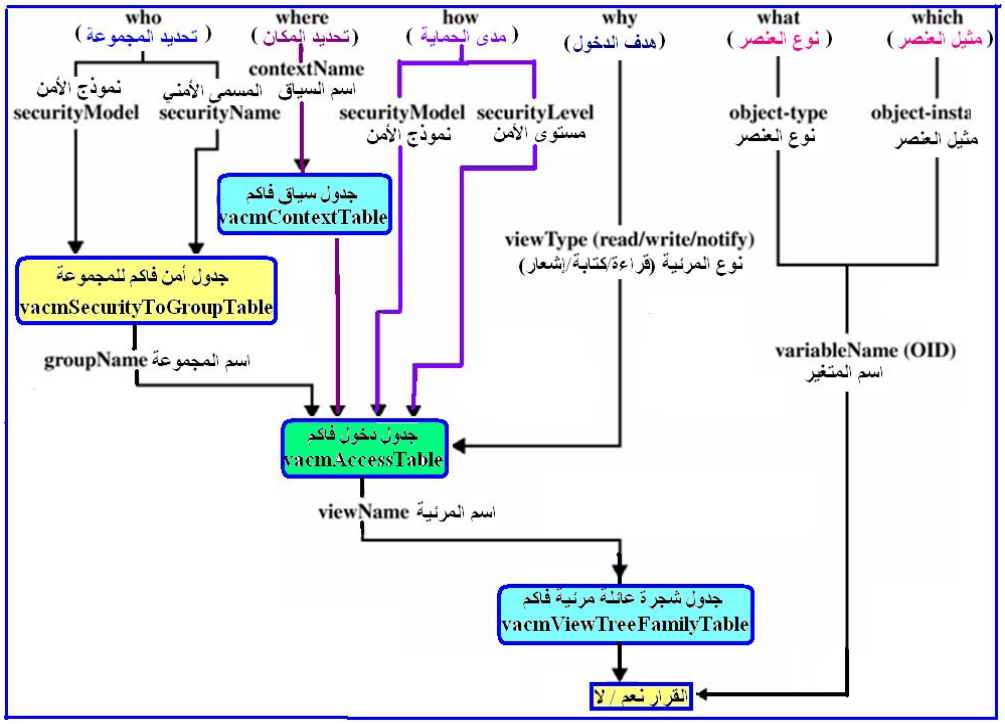
مرئية محدد. يحدد "اسم المرئية" مرئية قاعدة المعلومات الإدارية المناسبة من "جدول عائلة شجرة مرئية فاكم".

ما what :(تحديد نوع العنصر)

يحدد اسم المتغير variableName عنصراً محدداً، الذي تحدد بادئتُهُ prefix نوعَ العنصر، وتحدد لاحقتُه suffix مثيل العنصر. يبين نوع العنصر ما هية نوع المعلومات الإدارية المطلوبة.

أي which: (تحديد مثيل العنصر)

يبين مثيل العنصر object instance أية بند محدد من المعلومات تم طلبه. أخيرا يتم مقارنة اسم المتغيرvaraibleName ، ومرئية قاعدة المعلومات الإدارية MIB view التي تم استرجاعها. عندما يحدث توافق بين اسم المتغير والعنصر الموجود في المرئية، بعد ذلك يتم منح الدخول.



شكل2.12 العمليات المنطقية لتحكم الدخول في نموذج فاكم.

3.5 مقارنة مع سنمب– ف1 و سنمب– ف2

إن المفاهيم concepts التي تم شرحها سابقاً، يمكن أن تجعل نموذج "فاكم" يبدو من نتيجته أنه صعب إلى حد ما في تحديد تحكم الدخول. إن الغرض من استخدام نموذج "فاكم" كما تم توضيحه بالعلاقات السابقة المتعلقة بالوصول للمعلومات الإدارية هو تقليل الذاكرة، ومتطلبات عملية المعالجة التي تحدث داخل محطة الوكيل.

لفهم هذه الدوافع، ينبغي أن نراعي العوامل التالية:

في بروتوكول "سنمب–ف1" ، "سنمب–ف2" استخدم مفهوم المشاركة community concept للتعبير عن العمليات الأمنية المتعلقة بالمعلومات وهي:

أ– هوية المحطة الإدارية الطالبة.

ب– هوية المحطة المنفذة (الوكيل أو المحطة المعاونة Proxy Entity).

ج– هوية مكان إدارة المعلومات المطلوب الدخول إليه (الوكيل / المحطة المعاونة).

د– معلومات التوثيق.

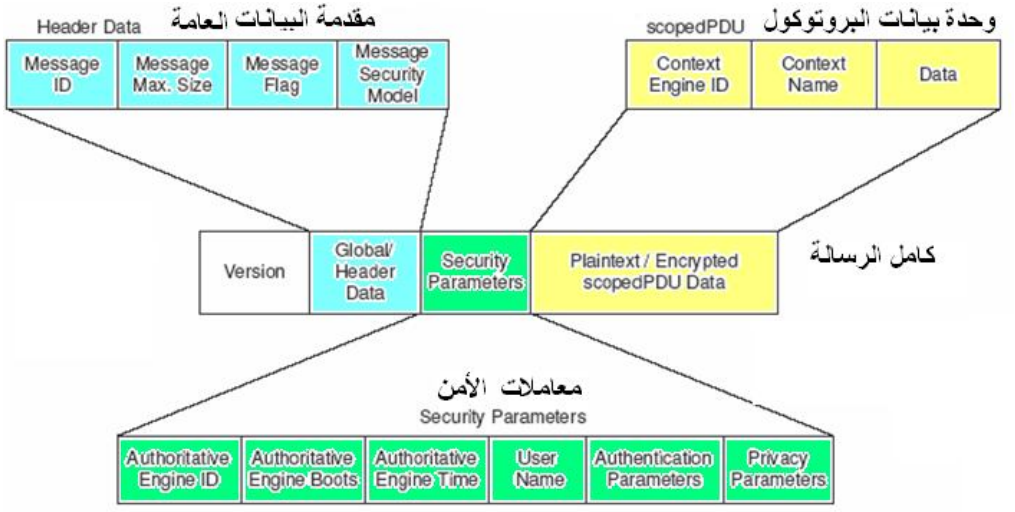
هـ– معلومات تحكم الدخول (التوثيق المطلوب لإجراء العملية).

و– معلومات التصفح MIB View .

إن تجميع كل هذه المفاهيم السابقة إلى متغير وحيد، يجعلها تفقد المرونة والأداء. إن "فاكم" يوفر نفس مجموعة المعلومات المتعلقة بالأمن بواسطة استخدام متغيرات لكل بند. وهذا يعتبر تحسن أساسي ملموس يفوق بروتوكول "سنمب–ف1". لأنه يفصل المفاهيم المختلفة لكي يتم إعطاء قيمة لكل واحدٍ منها على حدة.

6. مكونات شكل رسالة "سنمب-- ف3"

يوضح الشكل2.13 مكونات شكل رسالة بروتوكول "سنمب- ف3"، وهي تتكون من أربعة أجزاء رئيسية هي كما يلي:



شكل2.13 مكونات شكل رسالة بروتوكول "سنمب-ف3".

أ- **البيانات العامة** Common Data، وتكون موجودة في كل رسائل "سنمب- ف3". وتتكون من خمسة عناصر هي: نوع الإصدار msgVersion، ورقم الرسالة msgID ، وأقصي حجم للرسالة msgMaxSize، وأعلام الرسالة msgFlags، وأمن الرسالة msgSecurity .

ب- **بيانات نموذج الأمن** Security Model Data، وتشمل ثلاثة أجزاء، هي: جزء عام، وجزء خاص بالتوثيق، وجزء يحدد البيانات الخصوصية Privacy Data .

يتكون الجزء العام من أربعة مكونات هي:

هوية الآلة EngineID، تشغيلات الآلة EngineBoots، زمن الآلة EngineTime ، اسم المستخدم UserName .

يتكون الجزء الخاص بالتوثيق من: رسالة الاستيعاب MD5، وخوارزم الأمن SHA . ويعتمد جزء البيانات الخاص بالخصوصية على مفتاح التشفير DES Key.

ج- السياق (أو الحوار) Context

يستخدم لتوفير السياق الصحيح الذي ينبغي أن تقوم بمعالجته وحدة البيانات البروتوكولية Protocol Data Unit (PDU). ويتكون من: اسم السياق contextName، وهوية السياق contextEngineID.

د- وحدة بيانات البروتوكول PDU

وهي تحتوي على وحدة بيانات البروتوكول الخاصة بالبروتوكول "سنمب-ف3" . وتتكون من أعلام الرسالة msgFlags.

ويبين الجدول 2.2، والجدول 2.3 المعلومات التفصيلية لنوع ومسمي الحقول fields ووظيفتها في الأشكال المكونة لرسالة بروتوكول "سنمب-ف3" .

جدول2.2 عناصر الشكل المكونة لرسالة بروتوكول "سنمب-ف3 .

الترتيب	نوع ومسمى الحقل	الوظيفة
1	msgVersion إصدار الرسالة	تحديد نوع إصدار رسالة بروتوكول "سنمب-ف3" لكل من المدير/الوكيل. القيمة 0 تحدد رسائل سنمب-ف1 القيمة 1 تحدد رسائل سنمب-ف2c القيمة 2 تحدد رسائل سنمب-ف2 القيمة 3 تحدد رسائل سنمب-ف3
2	msgID هوية الرسالة	تحديد هوية الرسالة.
3	msgMaxSize أقصى حجم للرسالة	أقصى حجم للرسالة يستطيع الوكيل قبوله.
4	msgFlags أعلام الرسالة	تحديد أمن الرسالة. الخانة bit 0 تبين أن الرسالة موثقة authenticated

		الخانة الأولى تبين أن الرسالة خصوصية Privacy الخانة الثانية تبين أن تقرير PDU متوقعا من الرسالة(في حالة سقوط الرسالة ، أو عدم توليد استجابة).
5	msgSecurityModel نموذج أمن الرسالة	يبين نموذج الأمن المستخدم في توليد الرسالة. تشير القيمة 3 إلى استخدام النموذج USM.
6	msgSecurityParameters معاملات أمن الرسالة	يبين معاملات الأمن (التوثيق والخصوصية) التي يعتمد عليها نموذج الأمن.

جدول2.3 تابع عناصر الأشكال المكونة لرسالة بروتوكول "سنمب–ف3

الترتيب	نوع ومسمى الحقل	الوظيفة
7	msgEngineID هوية آلة الرسالة	يبين هوية آلة سنمب–ف3 للوكيل المشترك في العملية.
8	msgEngineBoots تشغيلات آلة الرسالة	يبين عدد المرات التي يتم فيها تحضير تشغيل Booting الوكيل المفوض لسنمب–ف3.
9	msgEngineTime زمن آلة الرسالة	يبين الوقت منذ لحظة إجراء عملية تحضير تشغيل الوكيل المفوض لسنمب–ف3.
10	msgUserName اسم مستخدم الرسالة	يحدد طالب الرجاء الرئيسي request principal . ويستخدم مع الحقل msgEngineID لتحديد مكان بيانات الأمن المصاحبة للرسالة من قاعدة بيانات USM. وتستخدم بيانات الأمن هذه في توثيق ومعالجة الرسالة.

11	contextEngineID هوية آلة السياق	تحديد وكيل سنمب–ف3 الذي يحقق مثيلاً instance للسياق مع اسم السياق المخصص.
12	contextName اسم السياق	يستخدم لتسمية السياق، ويجب أن يكون اسماً مميزاً unique من خلال وكيل سنمب–ف3.
13	PDU وحدة بيانات البروتوكول	يستخدم لإجراء عمليات الاتصال بين وكلاء سنمب–ف3. تحتوي بداخلها على: هوية الطلب requestID، حالة الخطأ errorStatus، متغيرات bindings، وغيرها. يوجد أنواع مختلفة من وحدات PDU تسمى بمسميات رسائل سنمب–ف3 (مثلا: Get-Request-PDU, GetNextRequset-PDU, etc) وأن الشكل الفعلي لوحدة PDU يعتمد على نوع وحدة PDU المستخدمة.

أسئلة تقويم ذاتي

يستخدم نموذج تحكم الوصول لرؤية المعلومات VACM، في بروتوكول إدارة الشبكة البسيط سنمب–ف3، اذكر وظائف هذا النموذج.

يختص نموذج "فاكم" بخاصتين هامتين اذكرهما ؟.

عدد العناصر المكونة لنموذج "فاكم".

اذكر ما تعرفه عن :

أ) السياق وخصائصه. ب) نظم حقوق الدخول Access Policy

يوضح الشكل التالي، مكونات فورمات رسالة بروتوكول سنمب–ف3.

اذكر وظيفة كل مكون منها باختصار.

Msg Vrsion
msgID
msgMaxSize
msgFlags
msgSecurityModel
msgAuthoritativeEngineID
msgAuthoritativEngineBoots
msgAuthoritativEngineTime
msgUserName
msgAuthoritativParameters
msgPrivacyParameters
context EngineID
contextName
PDU

الخلاصة

عزيزي الدارس،

تناولت الوحدة خصائص بروتوكول "سنمب--ف3" إن "سنمب-ف3". اشتمل على خصائص أمنية تسمح بإتمام تهيئتها باستقلالية Independent ، وهي:

- يدعم "سنمب-ف3" عملية توثيق الرسائل - تحقيق الخصوصية Privacy - تحقيق عملية التفويض Authorization ، والتحكم في الوصول لتصفح المعلومات - يسمح "سنمب-ف3" بإجراء عمليات التهيئة عن بعد .

وتناولت البناء الهيكلي لبروتوكول "سنمب--ف3". وهو يتكون من مكونين أساسيين هما: آلة سنمب-ف3، و مجموعة التطبيقات، و نطلق عليهما اسم محطة التشغيل، أو "كينونة سنمب-ف3 SNMP Entity". و تتكون آلة "سنمب-ف3" من أربعة مكونات هي: المنجز Dispatcher، ونظام الرسائل، ونظام الأمن، ونظام تحكم الدخول، أما مجموعة التطبيقات SNMP Applications فيوجد خمسة أنواع من التطبيقات للبروتوكول "سنمب-ف3" ، وهي: مولد الأوامر - مستجيب الأوامر - منشئ الإشعار - مستقبل الإشعار - الوكيل المعاون.

كما تناولت العمليات التفاعلية بين آلة "سنمب--ف3" ومجموعة التطبيقات، وذكرنا أنه يتم إجراء الخدمات Services بين وحدات برامج التشغيل Modules في محطة التشغيل Entity في بروتوكول "سنمب-ف3" بواسطة معاملات Parameters، ودوال Primitives . تستخدم المعاملات لتمرير بيانات ومعلومات التحكم، بينما تستخدم الدوال لتحديد الوظائف المطلوب تحقيقها. تناولت نموذج أمن المستخدم USM، ويوفر نموذج أمن المستخدم USM للبروتوكول "سنمب-ف3" خدمات التوثيق، وخدمات الخصوصية. وأوضحت أن نموذج USM تم تصميمه للحماية من التهديدات Threats الرئيسية وهي: تعديل المعلومات - التنكرMasquerade - تعديل فيض الرسالة Message Stream- كشف السر Disclosure، وللحماية من التهديدات السابقة فإن

نموذج أمن المستخدم USM في بروتوكول "سنمب–ف3" يستخدم بروتوكولين مختلفين للتوثيق، هما: بروتوكول HMAC-MD5-96، وبروتوكول HMAC-SHA-96. ويستخدم نموذج USM مفتاحين، أحدهما خاص لتحقيق الخصوصية هو privKey، والمفتاح الآخر لتحقيق التوثيق وهو authKey. ويستخدم هذان المفتاحان للمستخدمين المحليين Local Users، والمستخدمين عن بعد Remote Users. وأن هذين المفتاحين لا يتم تخزينهما في قاعدة المعلومات الإدارية MIB في الشبكة. ولذلك من غير الممكن الوصول إليهما مباشرة من خلال رسائل "سنمب–ف3 get, set "، وتناولت الوحدة تحقيق التوثيق وصحة الرسائل Authentication and Integrity، والتي تستخدم تقنية شفرة توثيق الرسالة Message Authentication Code (MAC) لتحقيق عملية توثيق الرسالة، كما تناولت استخدام نموذج USM للخوارزم القياسي لتشفير البيانات Data Encryption Standard (DES) في تشفير الرسائل، وذلك لضمان تحقيق الخصوصية Privacy. وتناولت معالجة الرسالة في نموذج USM في مرحلتي الإرسال والاستقبال، وذكرنا أنه عندما تمر رسالة خرج outgoing إلى نموذج USM بواسطة معالج الرسالة، فإن USM يضع بها معاملات الأمن ذات العلاقة في مقدمة الرسالة Message Header. وعندما تمر رسالة دخل incoming إلى نموذج USM بواسطة معالج الرسالة، فإن نموذج USM يقوم بمعالجة القيم الموجودة في هذه الحقول البيانية للرسالة، وتشمل معامِلات الأمن ذات العلاقة. تكون قيمة معامل الخصوصية هي القيمة المبدئية IV (متجه مبدئي Initial Vector)في خوارزم DES CBC، وتناولت الوحدة أيضاً توليد المفاتيح السرية، والمشاكل التي تحدث عندما تستخدم محطات الإدارة مفاتيح سرية مختلفة، وتعرفنا كيف يتم حل هذه المشكلة في نموذج USM بواسطة توليد مفتاح محلي Localized Key . حيث عرفت المفتاح المحلي بأنه مفتاح سري يتم مشاركته بين المستخدم U وآلة سنمب–ف3 المفوضة E. وأوضحت مميزات توليد المفاتيح المحلية وهي: تتميز بأنها تبطئ بقيمة كبيرة جدا هجوم المعجم الشرس Brute-Force Dictionary، الميزة الأخرى هي أنها

تفك ارتباط Decouple مفاتيح المستخدم من أي نظام إدارة شبكة NMS. حيث لا حاجة لتخزين قيم مفاتيح المستخدم في داخل نظام إدارة شبكة NMS. فبدلا من ذلك، فإنه عند الحاجة يتم توليد مفتاح المستخدم من كلمات سر المستخدم، ولإيجاد حل آخر لتخزين المفتاح السري بدلا من توليده من كلمة السر تناول القسم إدارة المفاتيح السرية من خلال الاحتفاظ بمستودع مركزي Centralized Repository للمفاتيح السرية. والتي ينبغي أن يتم الاحتفاظ بها في أماكن آمنة. كما حددت الوحدة أهدافاً لإدارة المفاتيح وأوضحت الوحدة أنه لأخذ هذه الأهداف بعين الاعتبار، فإنه يتم استخدام مفتاحٍ واحد للمستخدم، يتم تحويله إلى مفاتيح محلية مختلفة لآلات (وكلاء) مفوضين مختلفين باستخدام "دالة الطريق الواحد غير العكسي" nonreversible-one way function ، بينت الوحدة أن نموذج USM يستخدم طريقة للتحقق من عدم تأخر الرسائل، حيث تتطلب هذه الطريقة أن يقوم بروتوكول "سنمب–ف3" باستلام الرسائل خلال نافذة زمنية Time Window مناسبة. وذلك لتجنب التأخير، ومهاجمات إعادة بث الرسائل replay attacks. كما تناول القسم التوقيت المتزامنTime Synchronization ، حيث تحتاج آلة سنمب–ف3 غير المفوضة إجراء تزامن للتوقيت لكي تستمر في اتصالاتها المفوضة وتناول القسم أيضاً اختيار الآلات الموثقة، وبيَّن القسم أن أحد محطات التشغيل Entities (مرسل أو مستقبل) لأي رسالة مرسلة، ينبغي اختيارها Designate لتعمل آلة سنمب–ف3 مفوضة (موثقة)، طبقا للقواعد التالية:

– عندما تحتوي رسالة سنمب–ف3 على حمولة Payload تتوقع استجابة، فإن المستقبل في هذه الحالة يتم تعيينه ليكون مفوضا Authoritative.

– عندما تحتوي رسالة سنمب–ف3 على حمولة لا تتوقع استجابة، فإن مرسل هذه الرسائل يختار ليكون مفوضا. ومن ثم، فإن الرسائل المرسلة نيابة عن مولد الأمر، ورسائل المعلومات من منشئ الإشعار، فإن المستقبل يعمل مفوضا. وأن الرسائل المرسلة نيابة عن مستجيب الأمر، أو رسائل المصيدة من منشئ الإشعار فإن الراسل يعين مفوضا. وهذا التعيين يخدم غرضين هما:

– إن زمن تأخير الرسالة يتم تحديده بالرجوع إلى الساعة clock الموجودة في الآلة المفوضة.

– إن معالجة المفتاح المحلي، تمكّن مستخدماً رئيسياً واحداً من أن يمتلك مفاتيح تخزن في آلات عديدة، وأن هذه المفاتيح تكون محلية في الآلات المفوضة بطريقة بحيث يكون المستخدم الرئيسي مسئولا عن مفتاح واحد.

تناولت الوحدة نموذج تحكم الوصول لرؤية المعلومات VACMويستخدم للتحكم في الدخول لإدارة العناصر في قاعدة المعلومات الإدارية MIB.

وذكرت الوحدة أن نموذج "فاكم" يختص بخاصتين هامتين هما:

– أنه يحدد سماحية دخول "مستخدم رئيسي بعيد" لعنصر إداري لقاعدة المعلومات المحلية.

– أنه يحدد نظام Policy تحكم الدخول لوكيل، لإمكانية إجراء التهيئة عن بعد. وذلك باستخدام قاعدة المعلومات الإدارية MIB. كما تم تعريف خمسة عناصر لتكوين نموذج "فاكم" هي: المجموعات Groups – مستوى الأمن Security Level– السياق Context – مرئيات قاعدة المعلومات الإدارية MIB Views – نظام الدخول Access Policy .تناولت الوحدة معالجة تحكم الدخول Access Control Processing ، حيث أوضح القسم أن تطبيق "سنمب–ف3" يقوم ببدء تشغيل invoke نموذج "فاكم" من خلال الدالة isAccessAllowed ، ومعاملات الإدخال التالية:

اسم السياق contextName. – نموذج الأمن securityModel .

اسم الأمن securityName . – مستوى الأمن securityLevel .

نوع المرئية viewType . – اسم المتغير variableName .

كما تناولت الوحدة تحقيق العمليات المنطقية داخل نظام "فاكم"، حيث بينت أنه يمكن شرح تحقيق العمليات المنطقية داخل نظام "فاكم"، بطريقة سهلة، يتم تحديدها بواسطة النظام الفرعي subsystem للتحكم في الدخول. تناولت الوحدة مكونات شكل رسالة

بروتوكول "سنمب–ف3"، وهي تتكون من أربعة أجزاء رئيسية هي كما يلي: البيانات المعتادة – بيانات نموذج الأمن – السياق (أو الحوار) – ووحدة بيانات البروتوكول .

لمحة مسبقة عن الوحدة التالية

الوحدة التالية تأتي بعنوان بروتوكول إدارة الخدمات المعلوماتية الشائعة MIS/CMIP، حيث تناقش هذه الوحدة الدراسية: خصائص بروتوكول معلومات الإدارة الشائعة CMIP، وخدمات معلومات الإدارة الشائعةCMIS، ومميزات وعيوب هذا البروتوكول، وكذلك البروتوكولات الأخرى التي تستخدم من أجل حل بعض المشاكل المتعلقة ببروتوكول CMIP. كما تجد في هذه الوحدة شرحاً لأنواع الرسائل المستخدمة ووظيفة كل منها بالتفصيل مع إعطاء بعض الأمثلة لفحص بعض العناصر الخاصة بإدارة الشبكة، وتشمل: عمليات الإعداد، والأداء والمراقبة. كما تقدم الوحدة مقارنة بين بروتوكول إدارة الشبكة البسيط SNMP، وبروتوكول CMIP.

مسرد المصطلحات

بروتوكول إدارة الشبكة البسيط Simple Network Management Protocol (SNMPv3).

لقد تم اشتقاق وتطوير الإصدار الثالث لبروتوكول إدارة الشبكات البسيط "سنمب–ف3" من كلا الإصدارين الأول والثاني، والتعديلات الأساسية التي حدثت في بروتوكول "سنمب–ف3"، شملت الأمن Security، وعمليات الإدارة Administration. وذلك بهدف بناء تصميم عام يتميز بنظام أمني مرن يجعل من الممكن إجراء عمليات التفاعل بين المدير وأجهزة الإدارة تحقق عمليات الأمن التي تطلبها المؤسسة. الهدف الأخر هو أن يتم تصميم نظام عمليات إدارة الأمن بسهولة ولتحقيق هذه الأهداف، فإن "سنمب–ف3" اشتمل على خصائص أمنية تسمح بإتمام تهيئتها باستقلالية Independent .

المنجز Dispatcher

هو الذي يختص بعمليات إرسال واستقبال الرسائل. وتحديد نوع إصدار الرسالة التي يستقبلها سنمب–ف1، سنمب–ف2،سنمب–ف3. عندما تتم عملية تحديد الإصدار ومعالجته، يقوم المنجز بتسليم الرسالة إلى نظام معالجة الرسالة، وكذلك إلى الكيانات الأخرى (الوكلاء والمديرين في محطة التشغيل).

نظام الرسائل Message Subsystem

ويختص بمعالجة الرسائل الصادرة من الإصدارات الثلاثة لبروتوكول "سنمب–ف3"، وأي نماذج رسائل لبروتوكولات أخرى.

نظام الأمن Security Subsystem

يختص بمعالجة الأمن مستخدما نموذج أمن المستخدم User Based Security Mode (USM)، الخاص بالبروتوكول "سنمب–ف3" . كما يستخدم نموذج أمن المشاركة Community Based Security Model، الذي يتعامل مع الإصدارين الأول والثاني للبروتوكول "سنمب–ف3". وأي نماذج أمنية إضافية جديدة يتم تحديدها.

نظام تحكم الدخول Access Control System

وهو يختص بمنح أو منع عمليات الدخول إلى عناصر إدارية محددة في قاعدة المعلومات الإدارية MIB.

مُوَلّدُ الأوامر Command Generator

أحد أنواع تطبيقات بروتوكول "سنمب–ف3"، وظيفته إنشاء الأنواع المختلفة لرسائل بروتوكول "سنمب–ف3".

مستجيب الأوامر Command Responder

أحد أنواع تطبيقات بروتوكول "سنمب–ف3"، ووظيفته الـــرد على رسائل بروتوكـــــول "سنمب–ف3".

منشئ الإشعار Notification Originator

أحد أنواع تطبيقات بروتوكول "سنمب–ف3" ، ووظيفته إرسال رسالة مصيدة Trap أو إرسال رسالة إشعار (إعلام) Inform.

مستقبل الإشعار Notification Receiver

أحد أنواع تطبيقات بروتوكول "سنمب–ف3" ، ووظيفته استقبال ومعالجة رسائل المصيدة Trap ، أو الإشعار Inform .

الوكيل المعاون Proxy Forwarder

أحد أنواع تطبيقات بروتوكول "سنمب–ف3" ، ووظيفته توصيل الرسائل بين مكونات محطة "سنمب–ف3" (Entity).

إنكار الخدمة Denial of Service

أحد أنواع التهديدات، والمقصود بهذا التهديد هو أن يقوم المهاجم بمحاولة منع المستخدم الشرعي من استخدام الشبكة. حيث يقوم المهاجم هنا بمحاولة منع المبادلات التي تتم بين المدير والوكيل. ويحتاج هذا النوع من التهديدات وجود وسائل أمنية أخرى، خلاف الموجودة في بروتوكول إدارة الشبكة.

تحقيق التوثيق وصحة الرسائل Authentication and Integrity

تحقق طريقة توثيق الرسائل إجراء عمليات الاتصال بين طرفي الاتصال من استقبال رسائل موثقة. وذلك لضمان أن محتويات الرسالة لم يتم تعديلها وأن مصدر الرسالة موثق. وتستخدم تقنية شفرة توثيق الرسالة Message Authentication Code (MAC) لتحقيق عملية توثيق الرسالة.

المفاتيح المحلية Localized Key

المفتاح المحلي هو مفتاح سري يتم مشاركته بين المستخدم U وآلة سنمب–ف3 المفوضة E. حتى عندما يكون للمستخدم كلمة سر واحدة فقط ومفتاح واحد لكل الشبكة. فإن الأسرار الفعلية المشتركة بين المستخدم وآلة سنمب–ف3 المفوضة سوف تكون مختلفة. يتم تحقيق ذلك بواسطة المفتاح المحلي.

نموذج تحكم الوصول لرؤية المعلومات View Access Control (VACM) Model

يستخدم نموذج "فاكم VACM" للتحكم في الدخول لإدارة العناصر في قاعدة المعلومات الإدارية MIB .

المصطلح بالإنجليزية	معناه بالعربية
Access Control Processing	**معالجة تحكم الدخول**
Access Policy	سياسات **الدخول**
Access Rights	**حقوق الدخول**
Adversary	**العدو**
Administration	**عمليات الإدارة**
Assess	**تقدير**" تقييم"
Attacker	**المقتحم**
Brute-Force Dictionary	**معجم القوة الشرس**
Centralized Repository	**مستودع مركزي**
Concatenating	**سلسلة**
Connectionless	**عديم الاتصال**
Compromise	**شبهة**
Community Based Security Mode	**نموذج أمن المشاركة**
Concepts	**المفاهيم**
Context	**السياق**
Common Data	**البيانات المعتادة**
Decouple	**فك ارتباط**
Decryption	**فك التشفير**
Disordered	**غير منظمة**
Disclosure	**كشف السر**
Encryption	**تشفير**
Hash	**دالة الأمن**
Hierarchical	**هرمي**

Independent	**باستقلالية**
Initial Vector (IV)	**متجه مبدئي**
Impersonate	**تمثيل شخصية**
Local Users	**المستخدمون المحليون**
Local Configuration Data Data-store(LCD)	**بيانات التهيئة المحلية**
Loosely	**بحرية**
Matching	**التوافق**
Masquerade	**التنكر**
Message Authentication	**توثيق الرسائل**
Message Stream	**فيض الرسالة**
Message Authentication Code(MAC)	**شفرة توثيق الرسالة**
Message Timeliness Verification	**التحقق من توقيت الرسائل**
Message Header	**مقدمة الرسالة**
Nonreversible-one way function	**دالة الطريق الواحد غير العكسي**
Object instances	**مثيلات العناصر**
Out of Order	**غير نظامية**
Parameters	**معامِلات**
Privacy	**الخصوصية**
Protocol Data Unit (PDU)	**وحدة بيانات بروتوكول**
Plaintext	**الرسالة الأصلية**
Privileges	**امتيازات**
Principal	**مستخدم رئيسي**

Primitives	**دوال**
Reordered	**إعادة ترتيبها**
Remote Users	**المستخدمون عن بعد**
Replayed	**إعادة تشغيل**
Reboot	**إعادة تشغيل**
Reliability	**الاعتمادية**
Remote Configuration	**التهيئة عن بعد**
Report indicator	**مبيِّن تقرير**
Round-trip Communication Delay	**التأخير الناتج عن رحلة الاتصال**
Threats	**التهديدات**
Traffic Analysis	**تحليل الحركة**
Time Window	**نافذة زمنية**
Troubleshooting	**تشخيص الأعطال**
Time Synchronization	**تزامن التوقت**
Security Level	**مستوى الأمن**
SNMP Entity	**كينونة سنمب(محطة التشغيل)**
User Based Security Mode(USM)	**نموذج أمن المستخدم**
Vulnerability to malicious	**مهاجمات سهلة ماكرة**

قائمة المراجع

1- Network Management: Concepts and Practice, a Hands-on Approach, by Richard Burke - Computers – 2003.

2- A Practical Guide to SNMPv3 and Network Management, by David Zeltserman, Published by Prentice Hall Professional Technical Reference, Publication date: 1999.

2- SNMP, SNMPv2c, SNMPv3, and RMON 1 and 2, 3rd Edition, by William Stallings, Published by Addison-Wesley Pub Co., Publication date: December 1998, ISBN: 0201485346

3- "Basking in Glory-SNMPv3", An article from Network Computing, Aug. 15, 1998.

4- SNMP: An Object-Oriented Approach to Developing Network Management Applications, (Hewlett-Packard Professional Books) - Bk&Cd-Rom Edition, by Peter Erik Mellquist, Published by Prentice Hall Publication date: July 1, 1997, ISBN: 0132646072

5- SNMP at the Edge: Building Effective Service Management Systems, **by Jonathan Saperia Published by McGraw-Hill Professional Publication date: June 28, 2002, ISBN: 0071396896**

6- SNMP Network Management, **(McGraw-Hill Computer Communications Series) Book & CD-ROM Edition by Paul Simoneau Published by McGraw-Hill Companies**
Publication date: May 20, 1999, ISBN: 0079130755

7- SNMP, SNMPv2c, SNMPv3, and RMON 1 and 2, **3rd Edition, by William Stallings**
Published by Addison-Wesley Pub Co Publication date: December 1998, ISBN: 0201485346

8- Total SNMP: Exploring the Simple Network Management Protocol
2nd Edition, by Sean J. Harnedy Published by Prentice Hall Publication date: July 1, 1997, ISBN: 0136469949

9- Troubleshooting with SNMP and Analyzing MIBs, by Louis A. Steinberg Published by McGraw-Hill Companies Publication date: August 21, 2000, ISBN: 0072124857

10- Policy-based Network Management: Solutions for the Next Generation (The Morgan Kaufmann Series in Networking), by John Strassner Published by Morgan Kaufmann Publication date: August 25, 2003, ISBN: 1558608591

11- Managing Internetworks With Snmp, by Mark A. Miller - Computers - 1999

12- SNMPv3 RFCs, at http://www.ietf.org/RFC/.

- RFC 3412. Message Processing and Dispatching (December 2002)

- RFC 3413. SNMP Applications (December 2002)

- RFC 3414. User-based Security Model (December 2002)

- RFC 3415. View-based Access Control Model (December 2002)

- RFC 3417. Transport Mappings (December 2002)

- RFC 3584. Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework

- RFC 3826. The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model.


الوحدة الثالثة
بروتوكول إدارة الخدمات المعلوماتية
الشائعة CMIS/CMIP

محتويات الوحدة

المقدمة

تمهيد

عزيزي الدارس،

مرحباً بك عزيزي الدارس في الوحدة الثالثة من مقرر " استخدام وإدارة الشبكات2" نناقش في هذه الوحدة الدراسية: خصائص بروتوكول معلومات الإدارة الشائعة CMIP، وخدمات معلومات الإدارة الشائعة CMIS، ومميزات وعيوب هذا البروتوكول، وكذلك البروتوكولات الأخرى التي تستخدم من أجل حل بعض المشاكل المتعلقة ببروتوكول CMIP. كما نتناول بالتفصيل أنواع الرسائل المستخدمة ووظيفة كل منها بالتفصيل مع إعطاء بعض الأمثلة لفحص بعض العناصر الخاصة بإدارة الشبكة، وتشمل عمليات الإعداد والأداء والمراقبة. ثم نقارن بين بروتوكول إدارة الشبكة البسيط SNMP، وبروتوكول CMIP. وتشتمل هذه الوحدة على سبعة أقسام: القسم الأول منها يتناول خصائص بروتوكول CMIP، حيث يتميز بروتوكول معلومات الإدارة الشائعة "ثميب CMIP "، وخدمات معلومات الإدارة الشائعة "ثميس CMIS " بالعديد من الخصائص التي تجعله مفيدا لأداء وظائف إدارة الشبكات. القسم الثاني يتناول نموذج إدارة الشبكة باستخدام بروتوكول CMIP ويتناول القسم الثالث خدمات المعلومات الإدارية الشائعة CMIS، وتوفر خدمات المعلومات الإدارية الشائعة CMIS قوالب Bocks البناء الأساسي، والأداء الجوهري Intrinsic للنظام الذي يتم إدارته. القسم الرابع يتناول المرافقات الإدارية والمرافق الإداري Management Association هو اتصال Connection بين النظم المفتوحة ونظائرها لإدارة النظم في الشبكة كذلك يتناول القسم قوائم الدخول أما القسم الخامس فيتناول بروتوكول CMIP، كما نجد في هذا القسم أيضاً مشاكل بروتوكول CMIS/CMIP. القسم السادس يتناول بروتوكول "CMOT" و بروتوكول "LMMP" .

أهداف الوحدة

عزيزي الدارس، بعد فراغك من دراسة هذه الوحدة ينبغي أن تكون قادراً على أن:

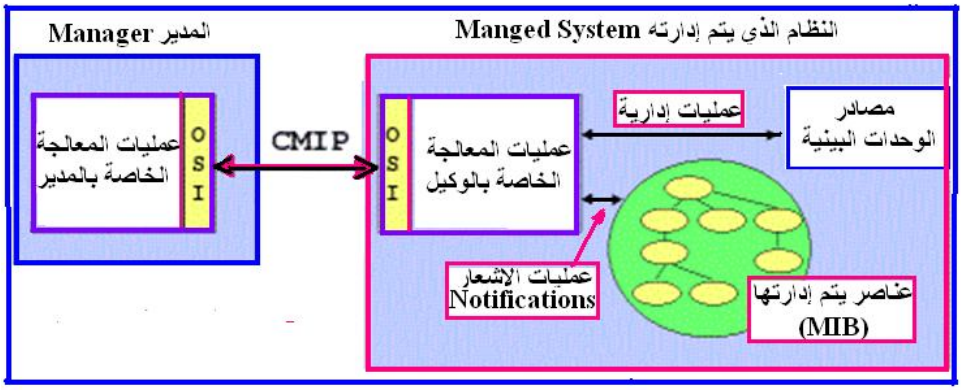
- **تعدد** وظائف وخصائص بروتوكول ثميب CMIP.
- **تشرح** نموذج المدير/ الوكيل باستخدام بروتوكول "ثميب" لإدارة الشبكات.
- **تعدد** خدمات المعلومات الإدارية الشائعة CMIS .
- **تبين** أنواع الخدمات الإدارية المرافقة،و إدارة الإشعار،و إدارة العملية.
- **تحدد** أنواع الرسائل المتعددة المستخدمة في بروتوكول "ثميب".
- **تصف** مشاكل بروتوكول CMIS/CMIP .
- **تبين** وظائف بروتوكول CMOT، و بروتوكول LMMP .
- **تشرح** المصطلحات العملية الخاصة ببروتوكول CMIP، CMIS.
- **تشرح** كيفية إدارة الشبكات باستخدام بروتوكول CMIP/CMIS.
- **تشرح** بعض الأمثلة العملية لتطبيق بروتوكول

1. خصائص بروتوكول CMIP

يتميز بروتوكول معلومات الإدارة الشائعة "ثميب CMIP "، وخدمات معلومات الإدارة الشائعة "ثميس CMIS " بالعديد من الخصائص التي تجعله مفيدا لأداء وظائف إدارة الشبكات. تحدد "CMIS " الخدمات العامة المتوفرة لكل مكونات الشبكة من أجل إدارة الشبكة. ويقوم بروتوكول "ثميب CMIP " بتنفيذ هذه الخدمات. إن بناء وأداء "ثميس/ثميب" يختلف بشكل واضح عن بروتوكول "سنمب". أحد هذه الاختلافات الأساسية هو أن بروتوكول "ثميس/ثميب" يسأل الجهاز الذي يتم إدارته لإجراء وظائف متعددة كثيرة. كما أنه يستخدم في الشبكات المبنية على أساس النظام المرجعي OSI (ذو المستويات السبع)، و تعرف هذه النظم بالنظم المفتوحة Open Systems. على أساس أنه يمكن إضافة (أو إلغاء) مستويات بروتوكولية معينة في أجهزة الشبكة طبقاً للوظائف المحددة المطلوبة من أجهزة الشبكة، وحسب الإمكانات المتاحة للمؤسسة.

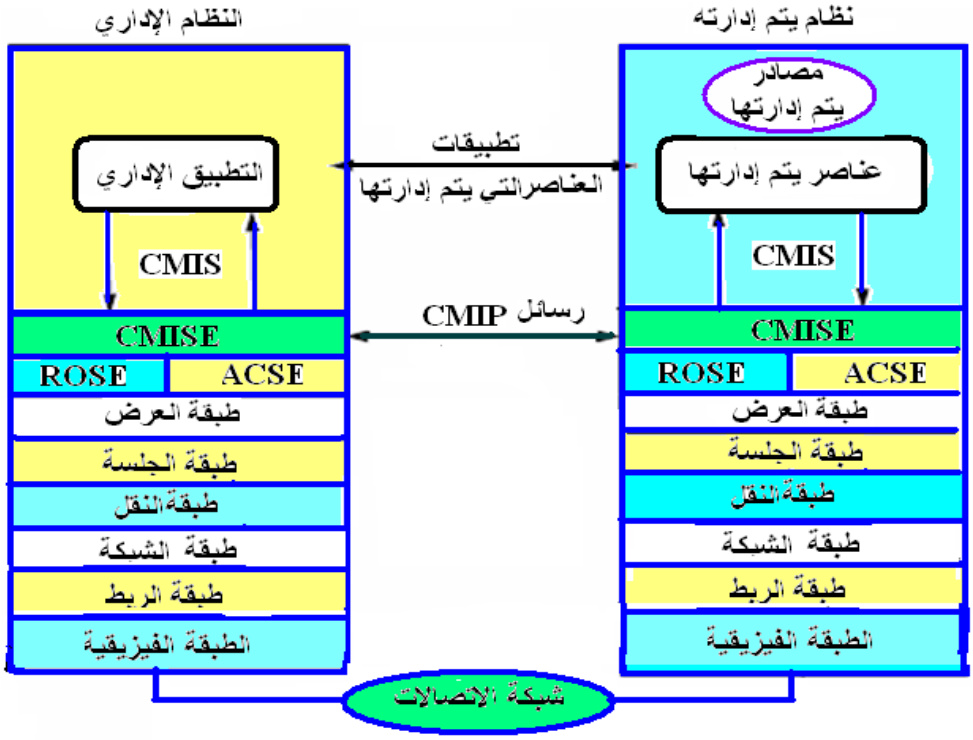
2. نموذج إدارة الشبكة باستخدام بروتوكول CMIP

يوضح الشكل 3.1 استخدام نموذج "المدير/الوكيل" في إدارة الشبكة باستخدام بروتوكول CMIP.



الشكل3.1 نموذج "المدير/الوكيل" في إدارة الشبكة باستخدام بروتوكول CMIP.

تستخدم عمليات تطبيق إدارة الشبكات، المستوى التطبيقي Application Layer في النموذج المرجعي OSI، الذي يستخدم في بناء الشبكات للنظم المفتوحة Open System. يوجد في هذا المستوى التطبيقي أيضا، بروتوكول عنصر المعلومات الإدارية الشائعة CMISE، لتوفير الوسائل التطبيقية اللازمة لاستخدام بروتوكول CMIP. وأن العنصر الخدمي CMISE بدوره يستخدم مستويين إضافيين على المستوى التطبيقي في النموذج المرجعي OSI، كما هو موضح في الشكل3.2 . وهذين المستويان هما: عنصر خدمة التحكم المرافق "أكسي ACSE "، وعنصر خدمة العمليات البعيدة "روزي ROSE" .



الشكل3.2 طبقة البروتوكول "CMIP" في النموذج المرجعي OSI

يقوم بروتوكول ACSE بتشغيل أو إعلام العمليات المرافقة Associations بين التطبيقات. بينما بروتوكول ROSE يقوم بمعالجة التفاعلات الخاصة بالطلب والرد request/response بين التطبيقات. وطبقا للنموذج المرجعي OSI، فإن كلا من

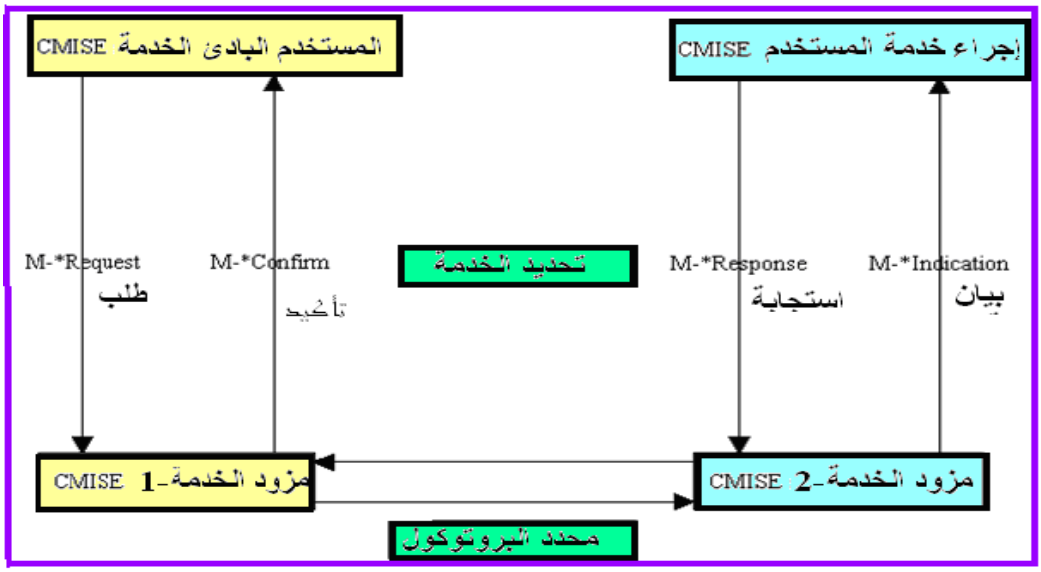
البروتوكولين ROSE, ACSE يفترض أن يستعملا خدمة طبقة العرض Presentation Layer في النموذج المرجعي OSI، وكذلك باقي النموذج.

أسئلة تقويم ذاتي

ما الاختلافات الأساسية بين بروتوكول "ثميس/ثميب" و بروتوكول "سنمب" ؟

3. خدمات المعلومات الإدارية الشائعة CMIS

توفر خدمات المعلومات الإدارية الشائعة CMIS قوالب Blocks البناء الأساسي، والأداء الجوهري Intrinsic للنظام الذي يتم إدارته، وأن كل خدمة تمثل عملية منفردة يستطيع تطبيق إدارة الشبكة إجراؤها. وأن أي تطبيق يتم إجراؤه بواسطة نظام الإدارة يكون مستخدماً خدمة CMISE. يوضح الشكل 3.3 الرسائل المتبادلة بين اثنين من المستخدمين بواسطة البروتوكول CMISE.



الشكل 3.3 الرسائل المتبادلة بين اثنين من المستخدمين بواسطة البروتوكولCMISE.

تحدد خدمات المعلومات الإدارية الشائعة CMIS ثلاثة أصناف Classes للخدمات التي يستخدمها المستخدمين وهي:

أ- الخدمات الإدارية المرافقة Services Management Association.

ب- خدمات إدارة التبليغ (الإشعار) Management Notification Services .

ج- خدمات إدارة العملية Management Operation Services .

وأن النظام المفتوح المناظر Peer Open System عليه أن يحدد تنفيذ واحد من هذه الخدمات أو تنفيذ كل هذه الخدمات.

1.3 الخدمات الإدارية المرافقة

تكون وظيفة الخدمات الإدارية المرافقة، هي التحكم في الاتصال بين النظم المفتوحة النظيرة. حيث إنها تؤدي وظائف أساسية لتحقيق أو إنهاء الاتصالات بين النظم، وكذلك التحكم في بدء التشغيل، أو إنهاؤه، أو توقيف اتصال غير طبيعي Abnormal. ويلخص الجدول3.1 الخدمات الإدارية المرافقة، ووظيفة كل منها.

الجدول3.1 الخدمات الإدارية المرافقة ، ووظيفة كل منها.

المرافق (نوع الخدمة) Association	**الوظيفة التي يؤديها**
M-INITIALIZE	**إنشاء** مرافقة مع مستخدم-خدمة-عنصر CMISE نظير لإدارة النظام.
M-TERMINATE	**إنهاء** الاتصال بين مستخدمين خدمة CMISE النظراء.
M-ABORT	**إيقاف** الاتصال بين مستخدمين خدمة CMISE النظراء لحالة غير عادية.

إن هذه الخدمات الإدارية المرافقة يفترض أن تستخدم خدمات بروتوكول "أكسي ACSE" لأجل التشغيل. حيث إن بروتوكول ACSE يستخدم لإجراء بدء الاتصال أو

إغلاقه بين التطبيقات. وأن خدمات CMIS الأخرى التي تستخدم اتصالا موجودا لإدارة المعلومات تعمل باستخدام بروتوكول ROSE.

2.3 خدمات إدارة التبليغ (الإشعار)

مثلما يحدث في برتوكول "سنمب" أنه يوفر معلومات عن تبليغ الأحداث events في الشبكة بواسطة رسائل المصيدة traps ؛ فإن خدمات التبليغ الإدارية CMIS توفر أداء مشابها. حيث تستخدم خدمة تدوين الحدث M-EVENT-REPORT لإبلاغ مستخدم–خدمة عنصر CMISE نظير عن الحدث الذي يقع عند مستخدم–خدمة–عنصر CMISE نظير آخر.

عندما يلاحظ مستخدم–خدمة–عنصر CMISE تغيرا لقيمة في النظام (مثلا: تغير وحدة بينية Interface)، فإنه يستطيع تبليغ Notify نظام الإدارة باستخدام خدمة تدوين الحدث M-EVENT-REPORT. على خلاف رسائل مصايد بروتوكول "سنمب" القياسية، فإن هذه الأحداث تكون قاصرة على هذا التحديد. إضافة، فهي محددة للنظام الذي ينشئ التبليغ، مثل مصايد "سنمب" المحددة للمؤسسة Enterprise.

إن الأجهزة التي ربما تختار فقط تنفيذ خدمات التبليغ الإدارية، هي الأجهزة التي لها قدرة معالجة محدودة ، أو هي ببساطة الأجهزة التي تحتاج إرسال تقرير تدوين خطأ إلى نظام مفتوح نظير Peer Open System. على سبيل المثال، يمكن لمستخدم–خدمة–عنصر CMISE الذي ربما يطلب فقط أن تكون خدمات التبليغ لعميل نظام إدارة شبكة هرمية، أن يقوم بإرسال تقرير أخطاء Faults إلى النظام المركزي Central System.

أسئلة تقويم ذاتي

تحدد خدمات المعلومات الإدارية الشائعة CMIS ثلاثة مصنفات Classes للخدمات التي يستخدمها المستخدمين، اذكر هذه المصنفات.

أكمل الجدول التالي والذي يلخص الخدمات الإدارية المرافقة ، ووظيفة كل منها :

المرافق(نوعالخدمة) Association	**الوظيفة التي يؤديها**
M-INITIALIZE	....
.....	**إنهاء** الاتصال بين مستخدمين خدمة CMISE النظراء.
M-ABORT	....

توفر خدمات إدارة التبليغ معلومات عن أجهزة الشبكة، بواسطة:

أ) خدمة تدوين الحدث لإعلام مستخدم خدمة نظير عن الحدث الذي يقع عند مستخدم نظير آخر.

ب) إرسال تقرير الخطأ إلى النظام المركزي بالشبكة.

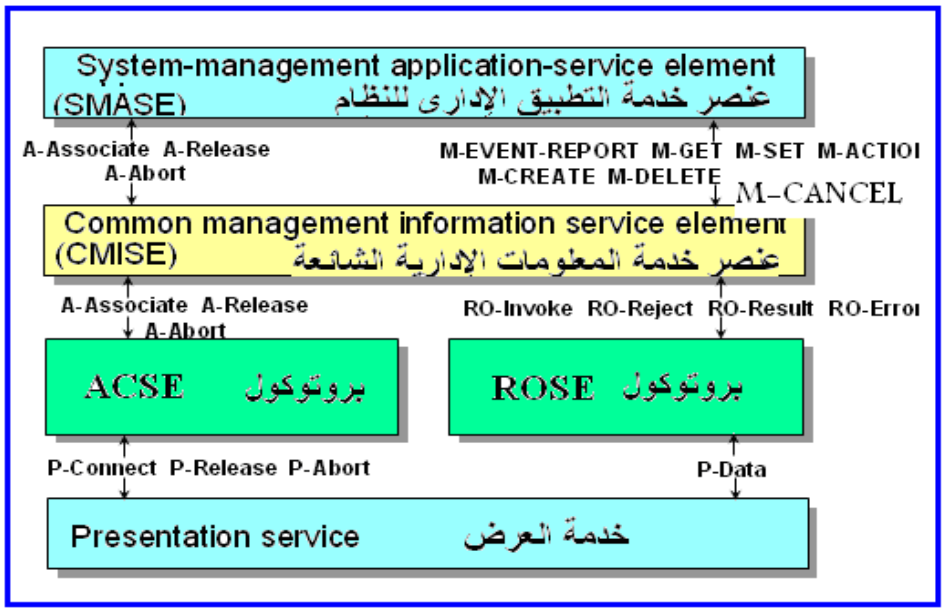
ج) يستخدم رسائل Traps في تبليغ الأحداث التي تقع في أجهزة الشبكة.

د) أ ، ب.

هـ) لا شيء مما سبق.

3.3 خدمات إدارة العملية

تحتوي خدمات إدارة العملية وهي خدمات المجموعة الثالثة من خدمات CMIS على ستة عمليات خدمية، كما هو موضح في الشكل3.4، و تشمل ما يلي:



الشكل3.4 الخدمات المستخدمة والمتاحة بواسطة CMISE.

أ- خدمة الحصول M-GET.

ب- خدمة إلغاء الحصول M-CANCEL-GET.

ج- خدمة الإعداد M-SET.

د- خدمة الأداء M-ACTION.

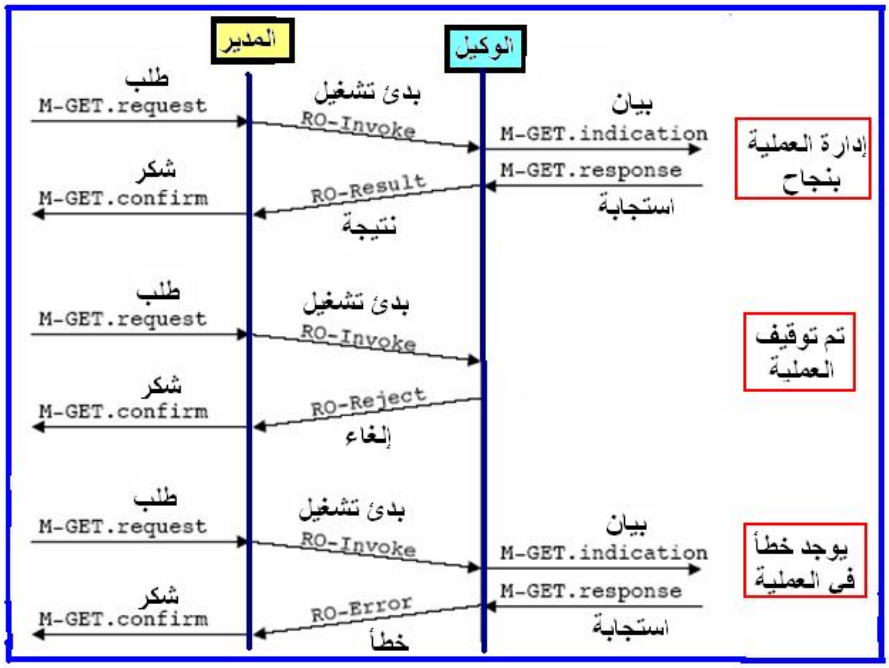
هـ- خدمة إنشاء M-CREATE.

و- خدمة حذف M-DELETE.

وفيما يلي نشرح بالتفصيل وظائف واستخدامات هذه الخدمات مع إعطاء بعض الأمثلة التوضيحية.

أولا: خدمات الحصول *M-GET* ،وإلغاء الحصول *M-CANCEL-GET*

تستخدم خدمة الحصول ***M-GET*** بواسطة مستخدم-خدمة-عنصر CMISE لاسترجاع المعلومات الإدارية من مستخدم-خدمة-عنصر CMISE نظير، وهي تماثل رسالة رجاء-حصول Get-Request في بروتوكول "سنمب". تستخدم رسالة إلغاء الحصول ***M-CANCEL-GET*** لإلغاء طلب حصول قد تم إرساله ولكن ما زال واقفا Outstanding . لذلك عندما يرسل مستخدم-خدمة-عنصر CMISE طلب الحصول M-GET ويقرر قبل عملية إرسال استجابة، أن هذا الطلب لم يعد يحتاج لهذه المعلومات، فإنه يستطيع إلغاء هذا الطلب بواسطة إرسال رسالة M-CANCEL-GET. يوضح الشكل3.5 إجراء خدمة الحصول M-GET بين المدير والوكيل.



الشكل3.5 إجراء خدمة الحصول M-GET بين المدير والوكيل.

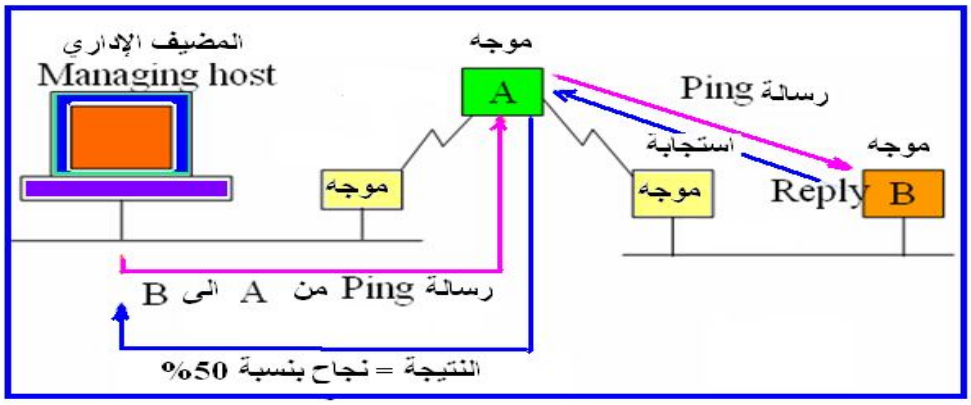
على سبيل المثال، نفترض أننا نريد كتابة تطبيق إدارة الأداء لمتابعة معدل الاستخدام Utilization لشبكة حلقية من نوع Token Ring. فإن مستخدم-خدمة-عنصر CMISE سوف يحاول إنشاء اتصال إدارة مرافقة مع جهازي الحاسب المتصلين بالشبكة مستخدما خدمة ابدأ M-INITIALIZE . بعد ذلك، للحصول على المعلومات الإدارية الضرورية؛ فإن التطبيق سوف يستعمل طلب الحصول على خدمة إدارة عملية بواسطة إرسال رسالة M-GET. بعد استقبال المعلومات، يمكن للتطبيق – بعد ذلك- أن يرسم منحنياً بيانياً Data Graph ، موضحا معدل الاستخدام في الشبكة الحلقية.

ثانيا:خدمة الإعداد *M-SET*

تسمح خدمة الإعداد ***M-SET*** لمستخدم-خدمة-عنصر CMISE ، أن يعدل المعلومات الإدارية لمستخدم-خدمة-عنصر CMISE نظير. وأن هذه الخدمة تشبه خدمة رسالة طلب إعداد Set-Request في بروتوكول "سنمب"، والتي تسمح بتعديل المعلومات لجهاز متصل بالشبكة.

ثالثا: خدمة الأداء *M-ACTION*

يتم بدء تشغيل **خدمة الأداء *M-ACTION*** بواسطة مستخدم-خدمة-عنصر CMISE لإرشاد instruct مستخدم-خدمة-عنصر CMISE نظير لتنفيذ الأداء المطلوب. ويتم أداء هذه الأعمال حسب طبيعة عمل كل جهاز يتم إدارته. على سبيل المثال، يمكن للنظام المفتوح أن يطلب من مستخدم نظير أن يرسل رسائل صدى pings بواسطة ICMP Echoes إلى أماكن مختلفة لاختبار توصيلة شبكة IP، كما هو موضح في الشكل3.6. وهذا المفهوم يكون مشابهاً لرسالة طلب الإعداد Set-Request في بروتوكول "سنمب-ف1"، الذي يبدأ تشغيل جهاز في الشبكة. يستطيع النظام المفتوح أن يطلب إجراء أعمال عديدة بواسطة نظام مفتوح آخر.



الشكل3.6 أحد استخدامات خدمة الأداء M-ACTION.

<u>على سبيل المثال،</u> يستطيع نظام إدارة الشبكة اتخاذ إجراء بعزل بعض الأخطاء Faults آليا بواسطة إرسال طلب الأداء M-ACTION إلى نظام مفتوح نظير، مثلاً نظام إدارة شبكة أخرى.

عند تنصيب إدارة شبكة هرمية، ويكتشف خادم نظام الإدارة مشكلة في منطقة معينة في الشبكة؛ فإنه بعد ذلك يمكن أن يفوض وظيفة أداء الخطأ لنظام عميل آخر، هو الذي يكون مسئولاً عن المنطقة المتأثرة (والذي يقع فيها الخطأ).

<u>رابعا: خدمة إنشاء *M-CREATE*</u>

تستخدم خدمة إنشاء M-CREATE بواسطة مستخدم – خدمة – عنصر CMISE، لإرشاد (أو أمر) مستخدم – خدمة – عنصر CMISE نظير، لكي ينشئ مثيلاً آخر لعنصر الإدارة، ليمثل هذا العنصر الإداري. في نظام الخدمة المتاحة CMIS، فإن كل عنصر يتم إدارته يمكن أن يوجد له مثيلٌ مرافقا له Associate Instance . تسمح خدمة CMIS لمثيلات عديدة لنفس العنصر، لكن واحدا فقط يتم تحديده من العنصر Object. وهذا المفهوم يشابه المستخدم في البرمجة الشيئية Object Oriented Programming، حيث كل عنصر يتم تعريفه كصنف Class، يمكن منه أن يتم تعريف مثيل instance.

أحد طرق استخدام خدمة إنشاء M-CREATE، هو أن يسمح للعناصر الإدارية بإرشاد أحدهما عن وجود عناصر جديدة أخرى. على سبيل المثال، يمكن في أحد النظم الإدارية أن يتم تعريف قنطرة ايثرنيت موجودة بالشبكة. وعند كل مرة يتم فيها إضافة قنطرة جديدة، فإن نظام الإدارة سوف ينشئ ويستخدم مثيلاً Instance لهذا التعريف. يستطيع النظام الإداري بعد ذلك إعلام النظم الإدارية الأخرى (في التركيب الهرمي أو التركيب الموزع للوسط المحيط بالشبكة) عن وجود القنطرة الجديدة. ويتم إجراء ذلك بواسطة المرافق الإداري، وباستخدام خدمة M-CREATE لإنشاء مثيلات للقنطرة الجديدة في النظم الأخرى.

خامسا: خدمة الحذف *M-DELETE*

تستخدم خدمة الحذف M-DELETE لتؤدي وظائف عكس التي تؤديها خدمة إنشاء M-CREATE. فهي تستخدم بواسطة مستخدم – خدمة – عنصر CMISE كي يطلب من مستخدم نظير أن يقوم بحذف مثيل للعنصر الإداري.

أسئلة تقويم ذاتي

تحتوي خدمات إدارة العملية على ستة عمليات خدمية، ما هي ؟

خدمة الحصول ***M-GET*** تماثل رسالة ..... في بروتوكول "سنمب".

تسمح خدمة الإعداد ***M-SET*** لمستخدم–خدمة–عنصر CMISE، أن يعدل المعلومات الإدارية لمستخدم–خدمة–عنصر CMISE نظير. حدد شبيه هذه الخدمة في بروتوكول "سنمب" .

يستطيع نظام إدارة الشبكة اتخاذ إجراء لاختبار توصيلة شبكة IP آليا، بواسطة إرسال طلب الأداء M-ACTION إلى نظام مفتوح نظير. اشرح مع الاستعانة بالرسم، كيف يتم أداء هذه العملية باستخدام خدمة CMIS، وبروتوكول CMIP.

4. المرافقات الإدارية و قوائم الدخول

1.4 المرافقات الإدارية Management Associations

المرافق الإداري هو اتصال Connection بين النظم المفتوحة ونظائرها لإدارة النظم في الشبكة. تعتمد عملية الاتصال على العنصر البروتوكولي CMISE لمواجهته مع البروتوكولات الأخرى في مركم Stack بروتوكول OSI . ويوجد أربعة أنواع ممكنة من المرافقات الإدارية عند تحقيق الاتصال بين النظم المفتوحة وهي كما يلي:

أ- الحدث Event.

ب- رصد/الحدث Event/Monitor.

ج- تحكم/الرصد Monitor/control.

د- الوكيل/المدير الرسمي Full Manager/Agent.

وفيما يلي شرحٌ تفصيلي لهذه المرافقات الإدارية، وبعض الأمثلة التوضيحية التي تبين استخدام كل مرافق منها بالتفصيل.

أولا: الحدث Event

يسمح المرافق الحدث لاثنين من النظم المفتوحة أن ترسل رسائل تدوين-حدث E-EVENT-REPORT . إذ ربما يوجد لنظامين مفتوحين حدثٌ مرافقٌ، عندما يحتاجون لإرسال إدارة أحداث إلي بعضهما فقط. كما يمكن لنظامين مفتوحين نظيرين أن يستخدما خدمات المرافقات الإدارية، وخدمات التبليغ الإدارية، من أجل حدث مرافق.

ثانيا: رصد/ الحدث Event/Monitor

تكون وظيفة مرافق رصد/ الحدث مثل وظيفة مرافق الحدث، فيما عدا أن كل نظام مفتوح نظير يمكن أن يستقبل ويرسل رسائل M-GET . يسمح مرافق رصد/ الحدث لنظم مفتوحة نظيرة أن تستفسر عن معلومات إدارية، وأن تستقبل أحداث الشبكة.

يكون هذا المرافق مفيداً من أجل مستخدمين لخدمات بروتوكول CMISE مهتمين لمعرفة حالة نظم مفتوحة نظيرة معينة، ولكن لا يسمح بتغييرها. كما يمكن أن يستخدم مستخدمين نظيرين من النظم المفتوحة خدمات المرافق الإدارية، و خدمات التبليغ الإدارية، وكذلك فئة فرعية لخدمات الأعمال الإدارية لمرافق رصد/ الحدث.

مثال: من الحالات الشائعة في إدارة النظم، أنه يمكن لمستخدم–خدمة–عنصر CMISE أن يتمكن من رصد ورؤية نظامٍ مفتوحٍ نظير ليس تحت سيطرته المباشرة (مثلا: نظام تمتلكه مؤسسة أخرى). فعلى الرغم من أن هذا النظام المفتوح النظير لا يتم إدارته بواسطة النظام الإداري الرسمي، فهو يمكن أن يتيح عملا هاما مطلوبا لعملية الرصد Monitoring. مثلا: إن الموجه Router الذي يقوم بربط المؤسسة بشبكة الإنترنيت، ربما يكون مملوكا لمزود خدمة الإنترنيت، لكن حالة هذا الموجه وعمله الحالي يكونان مهمين للمؤسسة. لذلك فإن نظام إدارة الشبكة، يقوم بإجراء مرافق "رصد/الحدث" مع موجه الإنترنيت.

ثالثا: تحكم/الرصد Monitor/Control

يسمح مرافق "تحكم/الرصد" بإجراء طلبات الاتصال مستخدما خدمات:

M-GET, M-CANCEL-GET, M-SET, M-CRAETE, M-ACTION, M-DELETE)

على الرغم من عدم وجود سماحية بتدوين الحدث Event Reporting. ربما يستخدم مستخدم–خدمة–عنصر CMISE، مرافق "تحكم/الرصد" لتغيير تهيئة نظام مفتوح نظير. في هذه الحالة، تكون خدمات التبليغ المستقبلة غير مهمة عادة، بسبب أن المهمة المطلوبة هي فقط تهيئة النظام المفتوح النظير. يمكن لنظامين مفتوحين نظيرين أن يستخدمان الخدمات الإدارية المرافقة ، وكذلك خدمات إدارة العملية من أجل مرافق "تحكم/الرصد".

مثال: نفترض مستخدم–خدمة–عنصر CMISE الذي يغير التهيئة في مجموعة من النظم المفتوحة النظيرة. يحتاج كل نظامٍ مفتوحٍ نظير أن يحصل على مراجعة جديدة New Revision لنظام التشغيل الذي تم تحميله على القرص الصلب Hard Disk . يقوم مستخدم–خدمة–عنصر CMISE بإجراء مرافق "تحكم/الرصد" للاستفسار عن حالة كل نظام مفتوح نظير هدف (مستخدما خدمة M-GET)، ويحدد المساحة الخالية للقرص الصلب الهدف. عندما يكون النظام المفتوح يؤدي عمله وبه مساحة قرص كافية لاستقبال نظام تشغيل جديد، فإنه يتم تحميله (ربما باستخدام اتحاد من خدمات كل من M-SET, M-ACTION). أثناء هذه العملية، فإن استقبال خدمات التبليغ تكون غير ضرورية. بسبب أن مستخدم–خدمة–عنصر CMISE المحدد، ليست لديه وسيلة لمعالجة هذه الخدمة، أو لتبليغ مهندس الشبكة. في الحالة المثالية، فإنه أثناء هذه العملية، فإن مستخدم–خدمة–عنصر CMISE آخر في نظام إدارة الشبكة، يكون له المقدرة على معالجة خدمات التبليغ الإدارية، ويقوم بتبليغ مهندس الشبكة بطريقة مناسبة عندما يقع الحدث.

رابعا: الوكيل/المدير الرسمي Full Manager/Agent

يدعم هذا المرافق جميع خدمات CMIS.عندما يقوم نظام إدارة الشبكة بإدارة نظام مفتوح نظير، ويحتاج أن يكون قادرا على إجراء أي وظيفة إدارية به، فإن النظام يستطيع استخدام وكيل/مدير رسمي.

أسئلة تقويم ذاتي

يعرف المرافق الإداري بأنه اتصال بين النظم المفتوحة، ونظائرها لإدارة نظام الشبكة، ويوجد له أربعة أنواع هي:

أ)..... ب).....

ج)..... د) .....

2.4 قوائم الدخول Access Lists

بنفس الطريقة التي يستخدم فيها بروتوكول "سنمب–ف1" حروف المشاركة Community Strings، ويستخدم فيها بروتوكول "سنمب–ف2" أطراف الاتصال Parties، والسياقات Contexts، لتحقيق أن النظام يستطيع دخول قاعدة المعلومات الإدارية؛ فإن خدمات CMIS تستخدم قوائم الدخول.

لكل نظام مفتوح، يوجد قوائم دخول تحدد بوضوح طرق الدخول للنظم المفتوحة الأخرى. ينبغي لمستخدم–خدمة–عنصر CMISE، فحص تحكم قوائم الدخول قبل توسل Invocation خدمات CMIS.

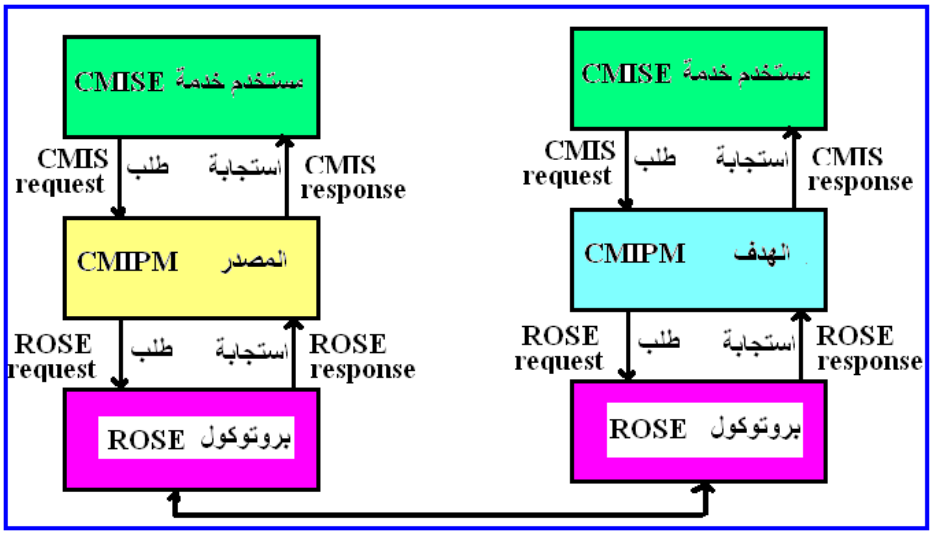
5. بروتوكول CMIP

يقوم بروتوكول CMIP بتنفيذ خدمات CMIS. يحتاج بروتوكول CMIP لآلة كي يؤدي وظائفه، أو مديرٍ CMIPM ليعمل حسب المواصفات المحددة. إن المدير CMIPM هو البرنامج الذي يؤدي الأعمال التالية:

أولا: يسمح باستقبال العمليات المرسلة إليه بواسطة مستخدم– خدمة– عنصر CMISE، ويبدأ تشغيل دالة مناسبة لتحقيق عملية المرافقة.

ثانيا: يستخدم بروتوكول ROSE لإرسال رسائل عبر الشبكة.

يوضح الشكل3.7 تدفق طلب خدمة CMIS بين مستخدمي–خدمة–عنصر CMISE .



الشكل3.7 تحقيق طلب خدمة CMIS بين اثنين من مستخدمي خدمة CMISE.

يستخدم المدير CMIPM مجموعة وحدات بيانات Data Units معرفة جيدا لتنفيذ خدمات CMIS، تستخدم كل خدمة CMIS سلسلة من وحدات هذه البيانات. على سبيل المثال، تستخدم الدالة m-GET للحصول على جزء محدد من بيانات قاعدة المعلومات الإدارية MIB من مستخدم–خدمة–عنصرCMISE. بينما تستخدم الدالة m-Linked-Reply للاستجابة على الدالة m-GET، وتحدد طريقا لمستخدم –خدمة–عنصر CMISE، لربط رسالة استجابة، التي ربما تحتاج حزم بيانات متعددة. بذلك عندما يرسل مستخدم –خدمة–عنصر CMISE خدمة M-GET ، تكون النتيجة إرسال وحدة بيانات m-GET، وإعادة إرسال وحدات بيانات أو أكثر لرسالة m-Linked-Reply.

يوضح الجدول3.2 قوائم الخدمات CMIS ، وما يقابلها من وحدات بيانات CMIP.

الجدول3.2 قوائم الخدمات CMIS وما يقابلها من وحدات بيانات CMIP.

خدمة CMIS	وحدات بيانات CMIP
تدوين–حدث M-EVENT-REPORT	تدوين–حدث m-EventReport تأكيد تدوين–حدث m-EventReport-Confirmed
حصول M-GET	حصول m-Get استجابة ربط m-Linked-Reply
إلغاء حصول M-CANCEL-GET	تأكيد إلغاء حصول m-Cancel-Get-Confirmed
إعداد M-SET	تأكيد الإعداد m-Set-Confirmed استجابة ربط m-Linked-Reply
أداء M-ACTION	أداء m-Action تأكيد الأداء m-Action- Confirmed استجابة ربط m-Linked-Reply
إنشاء M-CREATE	إنشاء m-Create
حذف M-DELETE	حذف m-Delete

1.5 مشاكل بروتوكول CMIS/CMIP

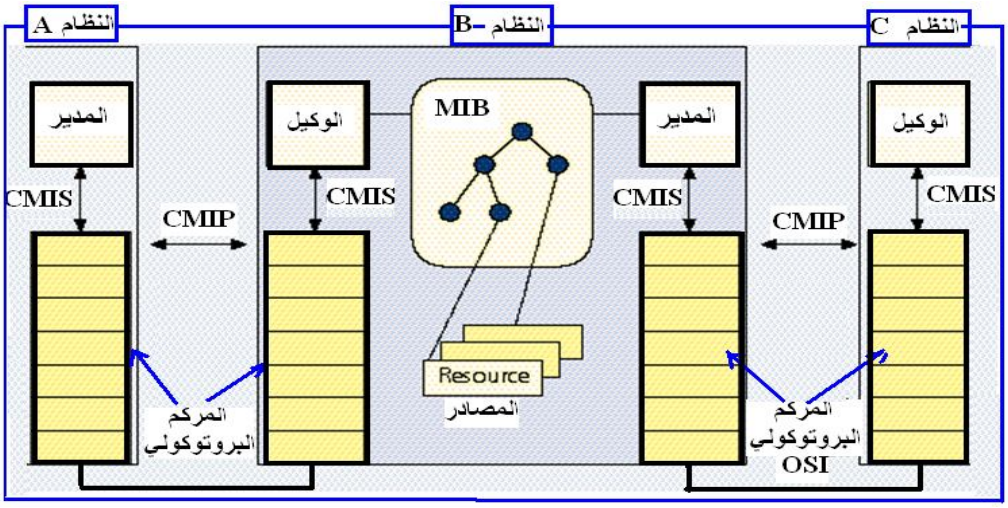
<u>توجد مشكلتان هما:</u>

أ – يحتاج بروتوكول CMIS/CMIP كمية ضخمة من عبء الاتصال Overhead.

ب– صعب تنفيذه.

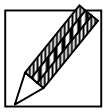
تنتج هذه المشاكل من حقيقة أن بروتوكول CMIS/CMIP تم تصميمه ليعمل مع مركم Stack بروتوكول OSI الرسمي، كما هو موضح في الشكل3.8. وبسبب الخواص

الطبيعية الرسمية للبروتوكولات OSI . فهي تتيح أداءً مرناً وتتطلب كمية ضخمة من العبء. ربما لا تمتلك بعض أجهزة الشبكة الذاكرة الكافية، أو قدرة المعالجة اللازمة لتدعيم مركم بروتوكول OSI الرسمي. لهذه الأسباب فإن بعض الموردين لأجهزة الشبكات يجدون صعوبة في تنفيذ مركم بروتوكول OSI بسبب قيود العتاد والبرمجة. ويوجد العديد من أدوات تنفيذ مركم بروتوكول OSI، لكنها ليست واسعة الانتشار.



الشكل3.8 المركم البروتوكولي OSI اللازم لتشغيل بروتوكول CMIS/CMIP.

تدريب (1)



وضح بالرسم مقارنة بعض الرسائل المستخدمة في بروتوكول CMIP، SNMP.

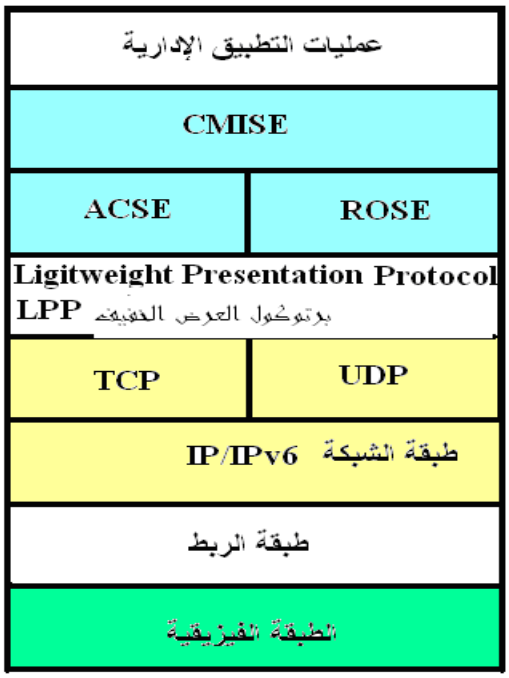
أسئلة تقويم ذاتي

اذكر وظائف برنامج المدير CMIPM في بروتوكول CMIP.
ما مشاكل بروتوكول CMIS/CMIP ؟

6. بروتوكول "CMOT" و بروتوكول "LMMP"

1.6 بروتوكول CMOT

هو مقترح عبارة تحميل خدمات المعلومات الإدارية الشائعة CMIS فوق قمة طبقة بروتوكول النقل TCP/IP ، وذلك لبناء خدمات CMIS كحل مرحلي Interim مؤقت. ويوضح الشكل3.9 بروتوكول CMOT في النموذج المرجعي OSI ذي المستويات السبع. وأن بروتوكولات التطبيق المستخدمة بواسطة CMIS، لا تتغير مع تنفيذ أداء CMOT.



الشكل3.9 بروتوكولات CMOT في النموذج المرجعي OSI.

حيث يعتمد بروتوكول CMOT على البروتوكولات (CMISE, ACSE, ROSE). على الرغم من ذلك، بدلا من الانتظار لبناء طبقة بروتوكول العرض Presentation OSI-، فإن بروتوكول CMOT يحتاج استخدام بروتوكول آخر على نفس الطبقة للنموذج المرجعي OSI. ويسمى هذا البروتوكول "بروتوكول العرض الخفيف

"Lightweight Presentation Protocol (LPP). وهذا البروتوكول LPP يعمل كوحدة بينية لكل من بروتوكولات طبقة النقل الشائعة وهما TCP, UDP الذان يستخدمان بروتوكول الشبكة IP في عملية الإرسال.

إن النظام الذي يلتزم بمواصفات البروتوكول CMOT ينبغي أن يحقق الأداء الذي يميز المرافقات Associations (التي تم شرحها سابقاً في بروتوكول CMIP) وذلك مع النظم المفتوحة. وينبغي على هذا النظام أيضا أن يدعم فقط نوع المرافق المناسب للنظام.

وتشمل هذه المرافقات ما يلي:

- الحدث event .
- مراقب/الحدث event/monitor .
- تحكم/المراقب monitor/control .
- الوكيل/المدير الكامل full manager/agent .

إن أحد المشاكل المجهدة لاستخدام بروتوكول CMOT، هو أن العديد من موردي أجهزة إدارة الشبكات، لا يرغبون في بذل الوقت والجهد لبناء حل مؤقت آخر. و بدلا من ذلك، فإن العديد من موردي أجهزة إدارة الشبكات، قاموا بجهود لدعم بروتوكول "سنمب" .

2.6 بروتوكول LMMP

هو بروتوكول لإدارة شبكات LAN MAN ، كمحاولة لتوفير حلاً لإدارة الشبكات في الوسط المحيط للشبكات المحلية LAN. ويعرف بروتوكول LMMP رسميا بأنه اتحاد بين خدمات المعلومات الإدارية الشائعة CMIS، مع بروتوكول تحكم الربط المنطقي IEEE 802 وهو CMOL.

من أمثلة أجهزة الشبكة في الوسط المحيط للشبكات المحلية LAN هي: قناطر محدد المصدر Source Route Bridges، والمجمع السلكي Wiring Hub، ومكرر التكبير Repeater.

لقد تم تطوير البروتوكول LMMP من قبل شركة 3Com Corp ، وشركة IBM ،وتم الاستغناء عن الاحتياج لبروتوكول OSI في تنفيذ خدمات CMIS. لأن بروتوكول LMMP يركب مباشرة فوق قمة طبقة الربط المنطقي IEEE 802، التي لا تعتمد على بروتوكول شبكة محدد، مثل IP لإجراء عملية الإرسال.

بسبب أن بروتوكول LMMP لا يحتاج لأي بروتوكول مستوى شبكي، فإنه أسهل في تنفيذه من بروتوكول CMOT، وبروتوكولCMIS/CMIP. لكن بدون بروتوكول المستوى الشبكي Network Layer، الذي هو ضروري لتوفير معلومات تحديد المسارات Routing في الشبكة؛ فإن رسائل بروتوكول LMMP لا تستطيع أن تجتاز عائق الموجهات Routers. على الرغم من ذلك، فإن بناء الوكلاء المعاونين Proxy Agents، يقوم بنقل معلومات بروتوكول LMMP خارج حدود الشبكات المحلية متغلبة بذلك على هذه المشكلة.

أسئلة تقويم ذاتي

علل لماذا بروتوكول LMMP أسهل في تنفيذه من بروتوكول CMOT، وبروتوكولCMIS/CMIP.

اذكر استخدامات البروتوكولات التالية:

أ) LMMP ب) LPP

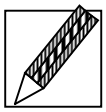
ج) CMOL د)CMOT

قارن بين بروتوكول CMIP، وبروتوكول SNMP من حيث الآتي:

أ) النموذج البنائي. ب) تنفيذ العمليات. ج) الأمن ووسائل الحماية.

د) تكلفة البرنامج. هـ) سعة الانتشار والتسويق.

تدريب (2)



أكمل الجدول التالي وهو مقارنة بين بروتوكول CMIP، SNMP :

عنصر المقارنة	**CMIP**	**SNMP**
النموذج	.....	.....
وسيلة المعلومات	.....	.....
تركيب الوكيل	.....	.....
حالة المعلومات	.....	.....
التنفيذ	.....	.....
استرجاع المعلومات	.....	.....
العمليات Actions	.....	.....
الأمن	.....	.....
الوظائف الإدارية	.....	.....
السعر	.....	.....
التسويق	.....	.....

الخلاصة

ناقشت الوحدة الدراسية خصائص بروتوكول CMIP و CMIS ، حيث أوضحت الوحدة إن بناء وأداء "ثميس/ثميب" تختلف بشكل واضح عن بروتوكول "سنمب". أحد هذه الاختلافات الأساسية هو أن بروتوكول "ثميس/ثميب" يسأل الجهاز الذي يتم إدارته لإجراء وظائف متعددة كثيرة. كما أنه يستخدم في الشبكات المبنية على أساس النظام المرجعي OSI (ذو المستويات السبع). وتناول القسم الأول استخدام نموذج "المدير/الوكيل" في إدارة الشبكة باستخدام بروتوكول CMIP، حيث تستخدم عمليات تطبيق إدارة الشبكات، المستوى التطبيقي Application Layer في النموذج المرجعي OSI، ويوجد في هذا المستوى التطبيقي أيضا، بروتوكول CMISE، لتوفير الوسائل التطبيقية اللازمة لاستخدام بروتوكول CMIP. وأن العنصر الخدمي CMISE بدوره يستخدم مستويين إضافيين على المستوى التطبيقي في النموذج المرجعي OSI وهذان المستويان هما: عنصر خدمة التحكم المرافق "أكسي ACSE "، وعنصر خدمة العمليات البعيدة "روزي ROSE". القسم الثاني تناول خدمات المعلومات الإدارية الشائعة CMIS وتحدد خدمات المعلومات الإدارية الشائعة CMIS ثلاثة مصنفات Classes للخدمات التي يستخدمها المستخدمين وهي:

- الخدمات الإدارية المرافقة Services Management Association.
- خدمات إدارة التبليغ (الإشعار) Management Notification Services .
- خدمات إدارة العملية Management Operation Services

القسم الثالث تناول المرافقات الإدارية Management Associations ، وذكرنا أن المرافق الإداري هو اتصال Connection بين النظم المفتوحة ونظائرها لإدارة النظم في الشبكة. كما أوضح القسم أنه يوجد أربعة أنواع ممكنة من المرافقات الإدارية عند تحقيق الاتصال بين النظم المفتوحة وهي كما يلي:

- الحدث Event.
- رصد/الحدث Event/Monitor .
- تحكم/الرصد Monitor/control.
- الوكيل/المدير الرسمي Full Manager/Agent.

القسم الرابع تناول بروتوكول CMIP الذي يقوم بتنفيذ خدمات CMIS . وأوضح القسم أن بروتوكول CMIP يحتاج لآلة كي يؤدي وظائفه، أو مديرٍ CMIPM ، والمدير CMIPM هو البرنامج الذي يؤدي الأعمال التالية:

- يسمح باستقبال العمليات المرسلة إليه بواسطة مستخدم-خدمة-عنصر CMISE، ويبدأ تشغيل دالة مناسبة لتحقيق عملية المرافقة.
- يستخدم بروتوكول ROSE لإرسال رسائل عبر الشبكة .

القسم الخامس تناول مشاكل بروتوكول CMIS/CMIP، وذكرنا أنه يوجد مشكلتان هما:

- يحتاج بروتوكول CMIS/CMIP كمية ضخمة من عبء الاتصال Overhead.
- صعب تنفيذه .

القسم السادس تناول بروتوكول CMOT، وتم تعريفه بأنه مقترح عبارة تحميل خدمات المعلومات الإدارية الشائعة CMIS فوق قمة طبقة بروتوكول النقل TCP/IP ، وذلك لبناء خدمات CMIS كحلاً مرحلياً Interim مؤقتاً ، كما تناول القسم أيضاً بروتوكول LMMP وهو بروتوكول لإدارة شبكات LAN MAN ، محاولة لتوفير حلّ لإدارة الشبكات في الوسط المحيط للشبكات المحلية LAN. ويعرف بروتوكول LMMP رسميا بأنه اتحاد بين خدمات المعلومات الإدارية الشائعة CMIS مع بروتوكول تحكم الربط المنطقي IEEE 802 وهو CMOL.

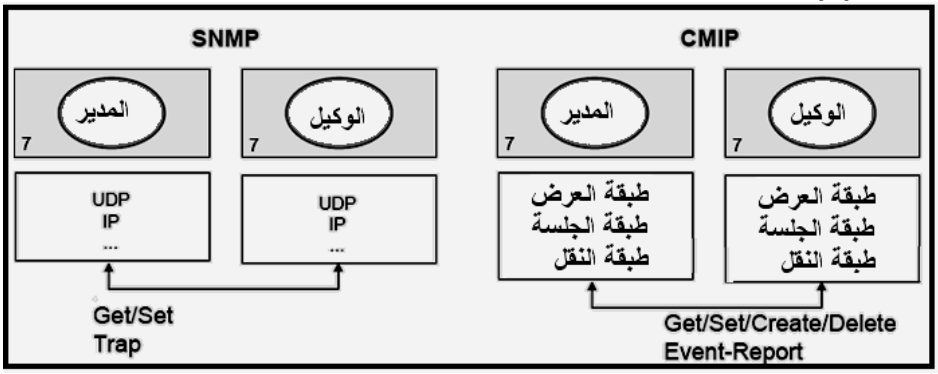
لمحة مسبقة عن الوحدة التالية

عزيزي الدارس،

الوحدة التالية تأتي بعنوان "قواعد معلومات إدارة الشبكات (الجزء الأول)" وتحتوي قواعد المعلومات الإدارية على المعلومات الحيوية الضرورية من أجل إجراء عمليات الإدارة، والتهيئة، والرصد بواسطة البروتوكول. فهي تعرِّف بدقة المعلومات المتاحة عن أجهزة الشبكة التي يمكن الوصول إليها Accessible بواسطة بروتوكول إدارة الشبكة. حيث تشرح الوحدة هيكل بناء قواعد المعلومات الإدارية. كذلك تجد في هذه الوحدة البنود الأساسية المستخدمة في قاعدة المعلومات الإدارية MIB-I، التي يستخدمها بروتوكول"سنمب–ف1". وأيضاً تتناول الوحدة قاعدة المعلومات الإدارية MIB-II، التي يستخدمها بروتوكول"سنمب–ف2".

إجابات التدريبات

تدريب (1)



رسم يوضح مقارنة بعض الرسائل المستخدمة في بروتوكول CMIP ، SNMP.

تدريب (2)

جدول مقارنة بين بروتوكول CMIP ، SNMP.

عنصر المقارنة	CMIP	SNMP
النموذج	مبني على الحدث event	يستخدم التصويت polling
وسيلة المعلومات	شيئي التوجه object oriented	يستخدم متغيرات variable
تركيب الوكيل	معقد	بسيط
حالة المعلومات	تحفظ بواسطة الوكيل	تحفظ بواسطة المدير
التنفيذ	معقد	بسيط
استرجاع المعلومات	شيئية objects	جداول scalars
العمليات Actions	مدعومة supported	تحتاج مهارة tricky
الأمن	من خلال الخدمات	بواسطة التوثيق والتشفير
الوظائف الإدارية	متعددة	أقل
السعر	مرتفع	منخفض
التسويق	محدود	واسع الانتشار.

مسرد المصطلحات

الخدمات الإدارية المرافقة Services Management Association

تكون وظيفة الخدمات الإدارية المرافقة، هو التحكم في الاتصال بين الـنظم المفتوحـة النظيرة. حيث إنها تؤدي وظائف أساسية لتحقيق أو إنهاء الاتصالات بين النظم، وكـذلك التحكم في بدء التشغيل، أو إنهائه ، أو توقيف اتصال غير طبيعي Abnormal.

المرافقات الإدارية Management Associations

المرافق الإداري هو اتصال Connection بين النظم المفتوحة ونظائرها لإدارة الـنظم في الشبكة.

تحكم/الرصد Monitor/Control

يسمح مرافق "تحكم/الرصد" بإجراء طلبات الاتصال مستخدما خدمات: (M-GET, M-CANCEL-GET, M-SET, M-CRAETE, M-ACTION, M-DELETE)

بروتوكول CMOT

هو مقترح عبارة تحميل خدمات المعلومات الإدارية الشائعة CMIS فوق قمـة طبقـة بروتوكول النقل TCP/IP، وذلك لبناء خدمات CMIS كحلاً مرحلياً Interim مؤقتاً.

بروتوكول LMMP

هو بروتوكول لإدارة شبكات LAN MAN، محاولة لتوفير حلّ لإدارة الشـبكات فـي الوسط المحيط للشبكات المحلية LAN. ويعرف بروتوكول LMMP رسميا بأنه اتحـاد بين خدمات المعلومات الإدارية الشائعة CMIS، مع بروتوكول تحكم الـربط المنطقـي IEEE 802 وهو CMOL.

المصطلح بالإنجليزية	معناه بالعربية
Access Lists	قوائم الدخول
Association	المرافقة
Association Control Service Element (ACSE)	عنصر خدمة التحكم المرافق
Associate Instance	مثيل مرافق
Class	صنف
Community Strings	حروف المشاركة
Contexts	السياقات
Common Management Information Protocol (CMIP)	بروتوكول معلومات الإدارة الشائع
Common Management Information Services (CMIS)	خدمات المعلومات الإدارية الشائعة
Common Management Information Services Element (CMISE)	بروتوكول عنصر المعلومات الإدارية الشائعة
Common Management Information Over IEEE802 Logic link control (CMOL), Known as LMMP	بروتوكول معلومـــــات الإدارة الشائع المحمل أعلى طبقة الربط المنطقية
Common Management Services Over Information TCP (CMOT)	بروتوكول خدمات المعلومات الإدارية الشائع المحمل فــوق طبقة النقل TCP
Data Graph	رسم بياني
Enterprise	مؤسسة

Event Reporting	تدوين الحدث
Invocation	توسل
Interim	مؤقت / مرحلي
LAN Man Management Protocol (LMMP), Previously called CMOL	بروتوكول إدارة شبكات LAN MAN
New revision	مراجعة جديدة
Management Notification Services	خدمات إدارة التبليغ أو الإشعار
Management Associations	المرافقات الإدارية
Management Operation Services	خدمات إدارة العملية
Management Association Services	الخدمات الإدارية المرافقة
Monitoring	عملية الرصد/ المراقبة
Open systems	النظم المفتوحة
Object Oriented Programming	البرمجة الشيئية
Overhead	عبء الاتصال
Parties	أطراف الاتصال
Peer Open System	النظام المفتوح المناظر
Proxy Agents	الوكلاء المعاونون
Routing	تحديد المسارات
Remote Operations Service Element (ROSE)	عنصر خدمة العمليات البعيدة
Source Route Bridges	قناطر محدد المصدر
Token Ring	شبكة حلقية
Utilization	معدل الاستخدام
Wiring Hub	المجمع السلكي

عزيزي
الدارس، بعد
فراغك من

المراجع

1- SNMP, SNMPv2, and CMIP: The Practical Guide to Network Management Standards by William Stallings: (Addison-Wesley Publishing Company Inc. Publication: 1994, ISSN:0163-5964 .

2- OSI Network Management: CMIS & CMIP, BY Charles Hayes.

3- Network Management: A Practical Perspective by Allan Leinwand and Karen Fang Conroy second edition, Addison-Wesley, ISBN# 0-201-60999-1 .

4- Network Management Standards: SNMP, CMIP, TMN, MIBs, and Object Libraries, 2nd Edition ,by Ulyses Black Published by McGraw Hill Text Publication, 1994, ISBN: 007005570X

5- Internet Web Sites and sample chapters:

www.linktionary.com/c/cmip.html

www.cellsoft.de/telecom/cmip.htm

www.networkdictionary.com/protocols/cmip.php

www.cs.luc.edu/~pld/courses/netmgmt/fall06/notes

www.informit.com/content/images/0672324083/samplechapter

www.personal.ee.surrey.ac.uk/Personal/G.Pavlou/Publications/Book-chapters/


الوحدة الرابعة
قواعد معلومات إدارة الشبكات (الجزء الأول)

محتويات الوحدة

المقدمة

تمهيد

عزيزي الدارس،

مرحباً بك في الوحدة الرابعة من مقرر "استخدام و إدارة الشبكات 2"والتي تحمل العنوان: "قواعد معلومات إدارة الشبكات (الجزء الأول)". تحتوي قواعد المعلومات الإدارية على المعلومات الحيوية الضرورية من أجل إجراء عمليات الإدارة، والتهيئة، والرصد بواسطة البروتوكول. فهي تعرف بدقة المعلومات المتاحة عن أجهزة الشبكة التي يمكن الوصول إليها Accessible بواسطة بروتوكول إدارة الشبكة.

نشرح في القسم الأول من هذه الوحدة الدراسية هيكل بناء قواعد المعلومات الإدارية. وفي القسم الثاني من الوحدة نقدم البنود الأساسية المستخدمة في قاعدة المعلومات الإدارية MIB-I، التي يستخدمها بروتوكول"سنمب–ف1". القسم الثالث من الوحدة يتناول قاعدة المعلومات الإدارية التي يستخدمها بروتوكول"سنمب–ف2". القسم الرابع يبحث في التوافق مع إصدارات بروتوكول سنمب. في القسم الخامس نتناول قاعدة المعلومات الإدارية MIB-II . القسم السادس يتناول مجموعة النظام واستخدامها لإدارة الأعطال وإدارة التهيئة مع الأمثلة . القسم السابع يقدم مجموعة البينية واستخدامها في إدارة التهيئة والأداء والحسابات مع الأمثلة . القسم الثامن والأخير من الوحدة يتناول مجموعة ترجمة العنوان وهيكلها البنائي وطرق الترجمة مع الأمثلة.

أهداف الوحدة

عزيزي الدارس، بعد فراغك من دراسة هذه الوحدة ينبغي أن تكون قادراً على أن:

- **تصف** الهيكل البنائي لقاعدة المعلومات الإدارية.
- **تشرح** محدد العنصر و الشجرة المستعرضة وتطبيقاتها.
- **تعدد** عناصر قاعدة المعلومات الإدارية **MIB-I** لبروتوكول سنمب–ف1.
- **تشرح** المعلومات المعرفة لنظام **SMI** مع أمثلة تطبيقية.
- **تعدد** أقسام قاعدة المعلومات الإدارية لبروتوكول سنمب–ف2 .
- **تصف** قاعدة المعلومات الإدارية الخاصة بالمديرين وأطراف الاتصال.
- **تستخدم** طرق التوافق **Coexistence** مع إصدارات بروتوكول سنمب.
- **تعرف** حساب معدل التغير للعنصر.
- **تصف** مع استخدام الأمثلة مجموعة النظام واستخدامها لإدارة الأعطال وإدارة التهيئة .
- **تصف** مع استخدام الأمثلة مجموعة البينية واستخدامها في إدارة التهيئة والأداء والحسابات .
- **تعدد** وظائف عناصر تحديد المستويات الفرعية و الدوائر الافتراضية والمعلومة والحرف.
- **تشرح** مع استخدام الأمثلة كيفية عمل مجموعة ترجمة العنوان و هيكلها البنائي و طرق الترجمة.

1. الهيكل البنائي لقاعدة المعلومات الإدارية

عزيزي الدارس،

يستخدم التركيب الهرمي Hierarchical و الشكل الهيكلي Structure Format في بناء قاعدة المعلومات الإدارية MIB. لكي يقوم بروتوكول إدارة الشبكة القياسي بتمثيل كل جهاز في الشبكة، فإنه ينبغي أن يستخدم الأشكال الخاصة بعرض المعلومات التي يتم تحديدها بواسطة قاعدة المعلومات الإدارية. يوجد مجموعة كبيرة من التوصيات RFC التي تصف نوع وقواعد المعلومات المتاحة في قاعدة المعلومات الإدارية، التي تستخدم لإدارة شبكات من النوع TCP/IP، و التي يطلق عليها "المعلومات الإدارية لتحديد الهيكلية SMI". وقد تم تطوير وتحديث هيكلية المعلومات الإدارية SMI بعدة توصيات قياسية حديثة.

تستخدم قواعد المعلومات الإدارية MIB، القواعد النحوية Syntax التي اقترحتها الهيئة الدولية للقياسات ISO وتعرف باسم "**الرموز النحوية المثالية الأولى**": Abstract Syntax Notation One "***ASN.1***" . وسوف نطلق عليها ؛هنا في هذا الكتاب؛ الاسم *"أسن.1"* وذلك بهدف تعريب المصطلحات المختصرة وكذلك للسهولة.

- **<u>محدد العنصر Object Identifier (OID):</u>**

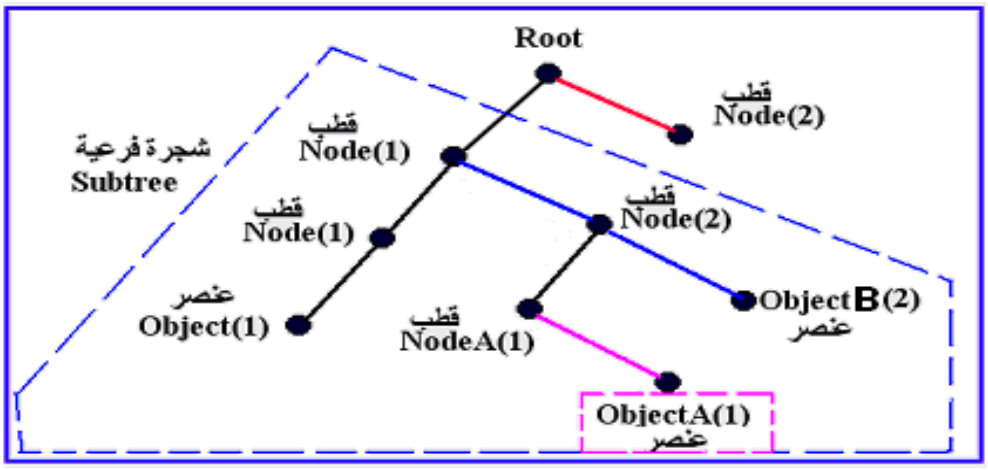
يستخدم البناء الشجري Tree Architecture لتنظيم جميع المعلومات المتاحة في قاعدة المعلومات الإدارية. يمثل كل جزء من المعلومات في الشجرة ***قطباً*** بعلامة ***Labeled Node***. يحتوي كل قطب بعلامة على ***محدد للعنصر*** ، ووصف نصي مختصر. يتكون محدد العنصر من سلسلة من الأعداد الصحيحة، يفصلها ***نقط periods***، وذلك لتسمية القطب node وترميز الجانب العرضي للشجرة "اسن.1" بدقة. يمكن أن يتفرع من القطب شجيرات فرعية أخرى لأقطاب ملصقات أخرى. يتم ترقيم كل قطب في الشجيرات الفرعية Sub Trees تصاعديا Ascending Order . ويستخدم هذا

المعجم Lexigraphical في ترقيم كل العناصر الموجودة في شجرة قواعد إدارة المعلومات.

عندما لا يوجد شجيرات فرعية لقطبٍ بعلامة، أو أقطاب ورقية Leaf Nodes ، في هذه الحالة يحتوي القطب على قيمة تعرف ***باسم العنصر object***. يوضح الشكل4.1 مثالاً لشجرة قاعدة معلومات إدارية، مع ما يقابلها من ترقيم رموز نحوية "اسن.1" .

يكون ترقيم ترتيب المعجم Lexigraphical لشجرة قاعدة المعلومات الإدارية هو:

1, 1.1, 1.1.1, 1.2, 1.2.1, 1.2.1.1, 1.2.2, 2.



الشكل4.1 مثال شجرة أسن.1 .

تدريب (1)

وضَّح الشكل4.1 السابق مثالاً لشجرة قاعدة معلومات إدارية، مع ما يقابلها من ترقيم رموز نحوية "اسن.1" :

ما محدد العنصر ObjectA ؟

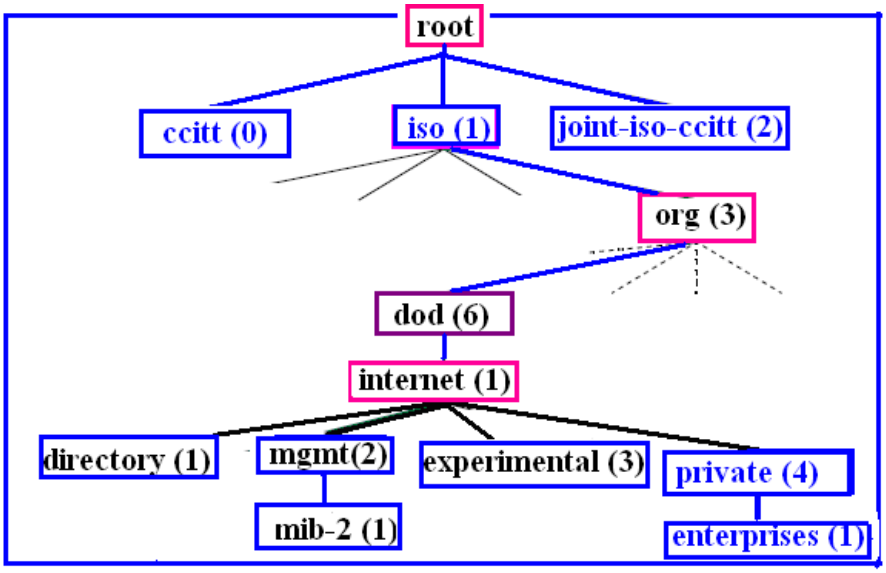
1.1 الشجرة المستعرضة Traversal وتطبيقاتها

يوضح الشكل4.2 البناء الهيكلي للشجرة المستعرضة لقاعدة المعلومات الإدارية من القمة. نلاحظ أن الجذر القطبي Root Node في الشجرة، لا يحتوي على اسم أو رقم ولكنه يحتوي على ثلاث شجيرات فرعية هي:

أ- ***ccitt (0)*** والتي يتم إدارتها بواسطة الهيئة الدولية CCITT.

ب- ***iso (1)*** والتي يتم إدارتها بواسطة الهيئة الدولية ISO.

ج- ***joint-iso-ccitt(2)*** والتي يتم إدارتها مشاركة بواسطة الهيئة الدولية CCITT والهيئة الدولية ISO.



الشكل4.2 البناء الهيكلي لشجرة قاعدة المعلومات الإدارية من القمة.

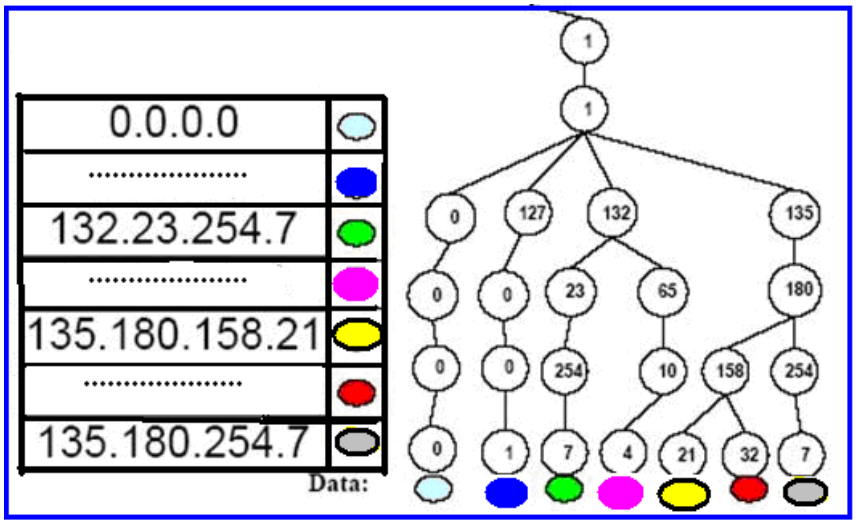
يستخدم الرمز ***ccitt (0)*** ليرمز إلى قطب ملصق يسمى ccitt، له رقم محدد عنصر هو (0) عند هذا المستوى من شجرة قاعدة المعلومات الإدارية. بالإضافة إلى ذلك، يوجد عديد من الشجيرات الفرعية الأخرى متفرعة تحت القطب ***iso (1)***، منها الشجرة الفرعية المحددة بواسطة هيئة ISO لمنظمات أخرى مثل ***org(3)***. يتفرع تحت الشجرة الفرعية ***org(3)*** قطب يستخدم من قبل وزارة الدفاع الأمريكية هو ***dod(6)***.

إن كل المعلومات المجمعة من أجهزة الاتصال بواسطة بروتوكول DOD مثل بروتوكول TCP/IP، تقيم في الشجرة الفرعية التي لها محدد عنصر مكتمل Complete Object Identifier هو 1.3.6.1، ويعرف محدد العنصر هذا باسم ***internet***. يكون الوصف النصي لهذا المحدد هو: ***iso org(3) dod(6)***، يوجد أربعة شجيرات فرعية – كما مبين في الشكل4.2– تحت محدد عنصر ***internet(1)*** هي: ***directory(1), mgmt(2), experimental(3), private(4)***.

يكون الوصف النصي لقطب الدليل directory node هو {internet 1}، والقطب mgmt, هو {internet 2} ، والقطب experimental هو {internet 3}، والقطب private هو {internet 4}.

تدريب (2)

الشكل الموضح أمامك، هو عبارة عن شجرة مستعرضة لعناصر قاعدة المعلومات لأحد الشبكات. أكمل باقي محددات العناصر في الجدول.



- **الشجرة الفرعية للدليل *directory(1)*:**

يتم الاحتفاظ بالشجرة الفرعية للدليل directory(1) للاستخدامات المستقبلية. وهي تحتوي على معلومات عن خدمات الدليل OSI التي تنظمها مجموعة التوصيات القياسية X.500 التي تحدد توزيع صيانة الملفات والأدلة.

- **الشجرة الفرعية*mgmt(2)* :**

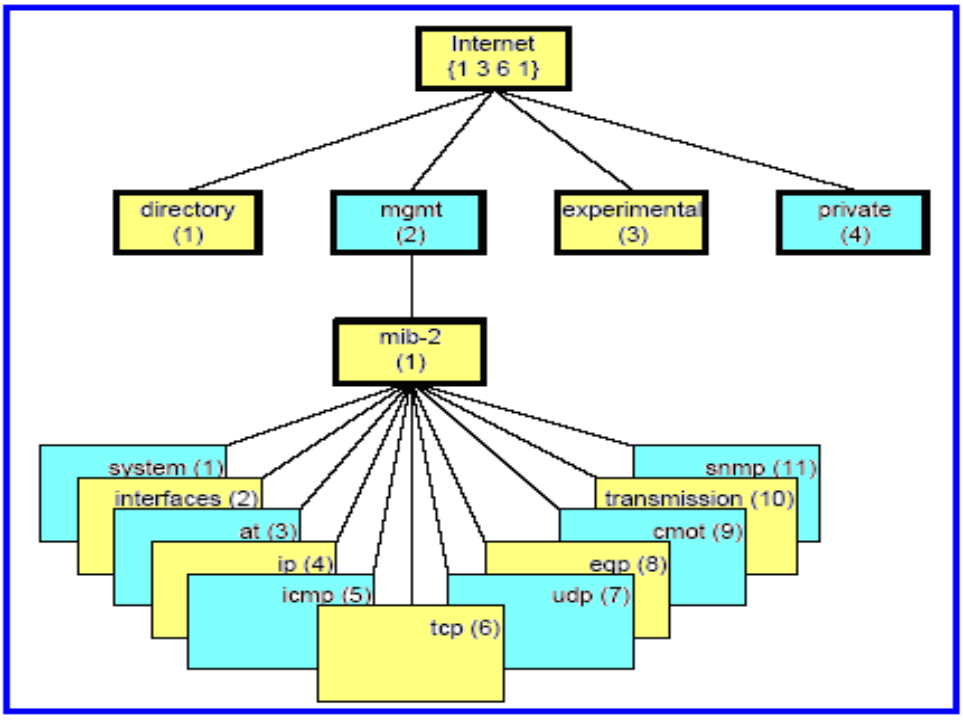
يبين الشكل4.3 البناء الهيكلي للشجرة الفرعية ***mgmt(2)*** ، وتشمل بعض العناصر من خلال كل مصنف category. وهي تستخدم لتخصيص المعلومات الإدارية للبروتوكول DOD. تعتبر العناصر المكونة لهذه الشجرة الفرعية أكثر العناصر واسعة التنفيذ. وقد تم تخصيص محدد العنصر 1.3.6.1.2.1 أو {mib(1)} لهذه الشجرة. تحتوي الشجرة الفرعية ***mgmt(2)*** على العناصر المستخدمة للحصول على معلومات محددة من أجهزة الشبكة. وتنقسم هذه العناصر إلى أحد عشر قسما، كما هو موضح في الجدول**4.1**.

الجدول4.1

فئة المعلومات في الشجرة الفرعية mgmt(2)

category الفئة	Information المعلومات
System(1)	نظام تشغيل جهاز الشبكة
Interfaces(2)	محدد وحدة بينية في الشبكة
Address translation(3)	ترجمة العناوين
Ip(4)	محدد بروتوكول IP
Icmp(5)	محدد بروتوكول icmp
Tcp(6)	محدد بروتوكول إرسال
Udp(7)	محدد برتوكول Datagram للمستخدم
Egp(8)	محدد بروتوكول بوابة سريعة gateway خارجي
Cmot(9)	محدد خدمات إدارة المعلومات الشائعة باستخدام البروتوكول TCP
Transmission(10)	محدد وسط إرسال
Snmp(11)	محدد بروتوكول "سنمب"

تقوم فئة ترجمة العنوان address translation (3) بتحويل عناوين IP إلى عناوين Ethernet. على الرغم من أن قواعد المعلومات الإدارية MIB كان القصد منها هو تخصيص معلومات إدارية للبروتوكولات خلاف IP (مثل بروتوكول الشبكة المعتمد على OSI)، فقد أوصت وثيقة RFC 1213 بحذف هذه الفئة، كي تحدث عملية ترجمة العناوين لكل البروتوكولات الموجودة في الشجرة الفرعية. يوضح الشكل4.3 البناء الهيكلي للشجرة الفرعية mgmt(2) .



الشكل4.3 البناء الهيكلي للشجرة الفرعية ***mgmt(2)*** .

- **<u>الشجرة الفرعية *Experimental(3):*</u>**

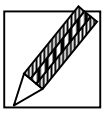
إن القصد من البروتوكولات التجريبية Experimental Protocols وتطوير قاعدة إدارة المعلومات هو الدخول إلى الجانب القياسي، لهذا الغرض تستخدم الشجرة الفرعية الثالثة وهي experimental(3).

إن جميع عناصر البروتوكول dod المتفرعة من هذه الشجرة الفرعية خصص لها الأرقام التي تحدد عناصرها، والتي تبدأ بالرقم الصحيح 1.3.6.1.3 . يمكن تخصيص قواعد معلومات إدارية MIB لتجارب جديدة ، يتم تحديد الرقم 10 لها، وهذا يقابل محدد عنصر هو {experimental 10}.

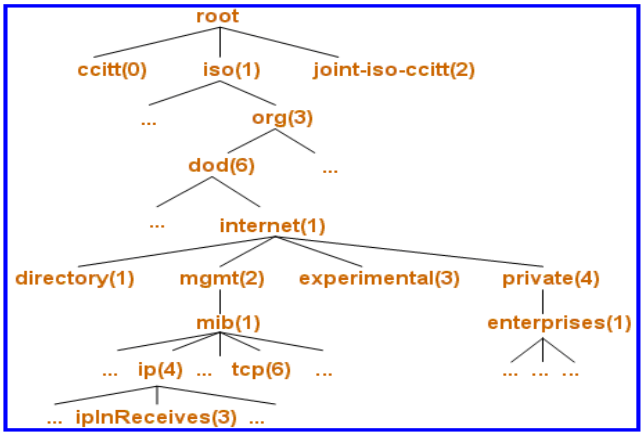
- **<u>الشجرة الفرعية الخاصة *private(4)* :</u>**

تستخدم الشجرة الفرعية الخاصة private(4) لتحديد العناصر الأحادية unilaterally في نظم إدارة الشبكات، حيث إن الجزء الذي يتم الدخول إليه غالباً لهذه الشجرة الفرعية هو أقطاب خاصة {private 1} أو أقطاب مؤسسة تجارية enterprises(1). يعرف قطب المؤسسة enterprise node بأنه هيئة لها سجلاتها الخاصة ذات امتداد محدد في قاعدة المعلومات الإدارية. كل فرع من هذه الشجرة الفرعية يتم تخصيصه لمؤسسة تجارية بمفردها. تستطيع المؤسسة التجارية بعد ذلك إنشاء خصائص attributes تتفرع من هذه الشجرة الفرعية لتحديد منتجاتها products. ويوجد قواعد المعلومات الإدارية المحددة للمورد في هذا المكان على شكل هرمي hierarchical.

تدريب (3)



مستعينا بالشكل الذي أمامك، اشرح وظيفة الشجرة الخاصة private(4) . مع إعطاء مثال توضيحي.



يوجد العديد من قواعد المعلومات الإدارية المخصصة للموردين متاحة في الأسواق. عندما يتم توصيل جهاز بالشبكة التي تعمل باستخدام بروتوكول "سنمب"، فإنها غالبا تدعم قاعدة المعلومات الإدارية المحددة للمورد، بالإضافة إلى قاعدة المعلومات الإدارية القياسية. تصمم قواعد المعلومات الإدارية الخاصة بالمورد لتتكامل مع قواعد المعلومات القياسية، وذلك لتوفير الوظائف الأساسية لإدارة الشبكات.

يوجد العديد من قواعد المعلومات الإدارية الخاصة بالموردين لمنتجات متعددة مختلفة من تقنيات النظم والشبكات، مثل: أجهزة المودم، مفاتيح ATM، مجمعات Hubs، جسور Bridges، موجهات Routers، خدم Servers، محطات عمل Workstations، وغيرها من الأجهزة. معظم العناصر الشائعة التي توجد في قواعد المعلومات الإدارية الخاصة بالموردين، تتعلق بمعلومات عن التهيئة الفيزيقية Physical Configuration مثل: رقم التسلسل، عدد منافذ التوسعة Slots، عدد المنافذ Ports، نوع الموائم Adapter، وغيرها. وأيضا تهيئة البرمجيات مثل : نوع الإصدار، خصائص التشغيل، معاملات التشغيل، وغيرها. توفر بعض الموردين أيضا، عناصر نستطيع استخدامها في كل مجالات إدارة الشبكة مثل: عدد الأخطاء لتقنيات محددة، معدل استخدام الذاكرة، تشغيل نظام الملفات، معالجة النظام الحالي.

<u>على سبيل المثال</u>: تستخدم بعض الدول آليات Robotics، لها قواعد معلومات إدارية تحتوي على معلومات عن أجهزة المودم الخاصة بها، مثل: تهيئة المودم، حروف الاتصال dialing Strings. بعض النظم لها قواعد إدارة معلومات للعناصر التي تحدد عدد الفتحات slots في المجمع hub. كما أن قاعدة المعلومات الإدارية لشبكات ATM لشركة IBM تحدد معلومات عن حجم الذاكرة Buffer، وأقصى عدد من الدوائر التصورية (الافتراضية) Virtual Circuits ، ونوع مركز البيانات Data Concentrators المستخدمة. كما أن نظم سيسكو CISCO يكون لها قواعد معلومات إدارية تحتوي على معلومات إحصائية عن بطاقات المواءمة Adapter Cards، وبروتوكول لكل وحدة بينية، وخصائص حسابات الشبكة. كما أن محطات يونيكس,

لشركة "هيلويت بيكارد" يوجد بها قواعد معلومات إدارية لفحص معلومات نظم الملفات، وعمليات المعالجة التي تعمل في الوقت الحالي، ومعلومات عن تجمعات Clusters لمحطات العمل.

ينبغي على مهندس إدارة الشبكة أن يكون متأكدا أن المنتجات التي يديرها على الشبكة، يكون لها قاعدة معلومات إدارية قياسية، وكذلك قواعد المعلومات الإدارية الخاصة بالموردين، التي قد يحتاجها من أجل إجراء كل الوظائف الخاصة بمناطق إدارة الشبكة.

أسئلة تقويم ذاتي

اختر الإجابة الصحيحة

1. ستخدم قواعد المعلومات الإدارية MIB قواعد نحوية لتنظيم المعلومات المتاحة بداخلها، وهذه القواعد تستخدم النظام:

أ) ISO ب) ASN.1 ج) TCP د) X.25 .

2. محدد العنصر (OID) في الشجرة الاستعراضية للمعلومات هو عبارة عن:

أ) سلسلة من الأعداد الصحيحة تحدد مكان العنصر للجهاز المستخدم في الشبكة.

ب) تسمية لأقطاب الشجرة الاستعراضية لمعلومات MIB.

ج) أعداد ترقم تصاعديا في الشجيرات الفرعية.

د) ترقيم لكل عنصر موجود في شجرة قواعد إدارة المعلومات لتسهيل الوصول إليه.

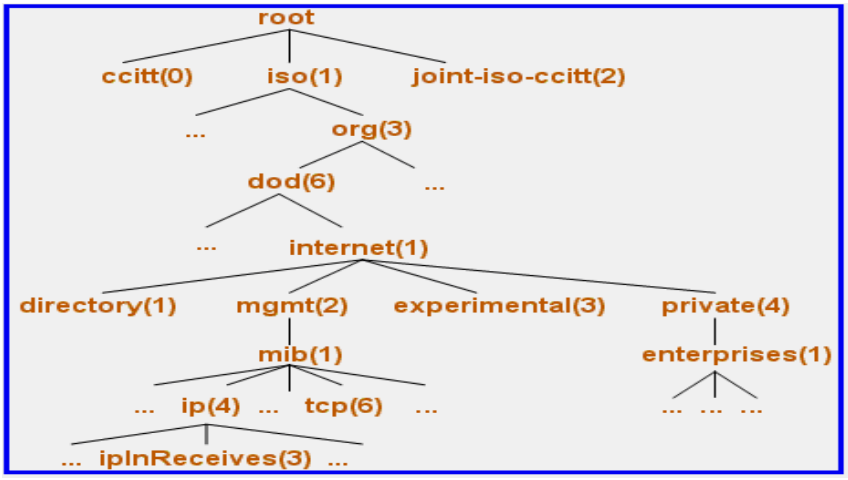
هـ) كل ما سبق.

3. اذكر وظيفة الشجرة الفرعية mgmt(2).

4. أكتب مسميات خمس فئات من العناصر المتفرعة من البناء الهيكلي لشجرة mgmt(2) ووظيفة كل منهما.

5. مستعيناً بالشكل الذي أمامك، اشرح وظائف ما يلي، مع إعطاء مثال توضيحي كلما أمكنك ذلك.

أ) الشجرة الفرعية experimental(3). ب) شجرة الدليل directory (1)



2. قاعدة المعلومات الإدارية MIB-I

عزيزي الدارس،

تستخدم قاعدة المعلومات الإدارية MIB-I في بروتوكول"سنمب–ف1". يبين الجدول4.2 نوع المعلومات الإدارية المستخدمة في البروتوكول"سنمب–ف1"، التي تحددها توصيات RFC. كما هو مبين في جدول4.2، فإن قاعدة معلومات "سنمب–ف1" تحتوي على ستة عناصر هي: عنوان الشبكة، وعنوان بروتوكول الربط IP، وعداد موجب يتزايد فقط من 1 إلى 2^32-1 وطوله 32 معلومة، وعداد آخر يسمى Gauge موجب يتزايد أو ينقص وقيمته العظمي 2^32-1، وعداد الزمن TimeTicks، وقواعد نحوية اختيارية يطلق عليها اسم Opaque تستخدم لوصف البيانات النصية. كما يوضح الجدول بعض أمثلة لاستخدامات هذه العناصر.

جدول (4.2) نوع المعلومات المعرفة لنظام SMI

نوع المعلومات المعرفة لنظام SMI

نوع المعلومات	الهدف منها	مثال
عنوان NetworkAddress	عنوان من أحد البروتوكولات العديدة الممكنة. حاليا لا يوجد فقط إلا البروتوكول IP	تحديد عنوان شبكة عامة. حاليا تكون الشبكة من نوع يستخدم البروتوكول IP
عنوان IPAddress	تحديد عنوان IP طوله 32 معلومة.	تحديد عنوان شبكة تستخدم البروتوكول IP
عداد Counter	عدد صحيح موجب يتزايد من 0 الى2^32– 1	إجمالي عدد الأخطاء المستقبلة في وحدة المواجهة interface.
عداد Gauge	عدد صحيح موجب يتزايد أو ينقص وله قيمة عظمى 2^32– 1	عدد حزم البيانات الحالية الموجودة في طابورqueue الخرج داخل interface.
عداد الوقت TimeTicks	عدد صحيح موجب لعد الوقت بالثانية	المدة الزمنية التي ظل يعمل فيها النظام.
قواعد اختيارية "Opaque"	قواعد نحوية Syntax اختيارية تستخدم للبيانات النصية	تعرف التوصيات RFC 1213 عنصرين هما: DisplayString لتحديد كيفية طباعة حروف أسكي ASCII. و PhysAddress لتحديد كيفية فرمتة العناوين الفيزيقية للشبكة، مثل عناوين MAC.

أسئلة تقويم ذاتي

؟ اذكر عناصر قاعدة معلومات "سنمب–ف1 ".

3. قاعدة المعلومات الإدارية لبروتوكول سنمب– ف2

تنقسم قاعدة المعلومات الإدارية لبروتوكول سنمب–ف2 إلى ثلاثة أقسام هي:

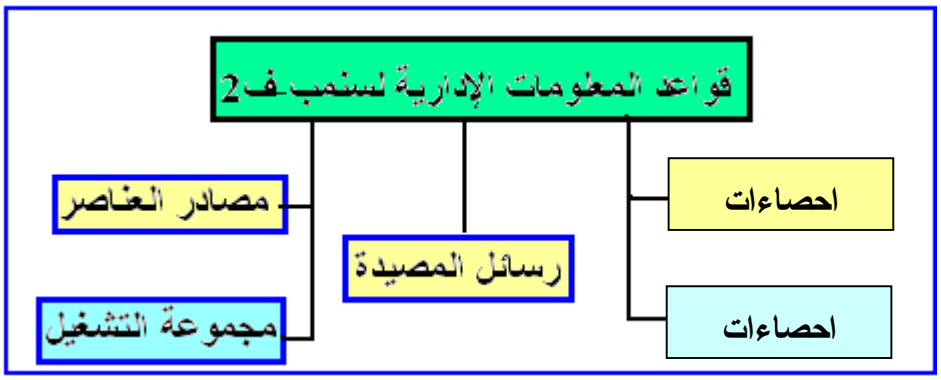
أ– قواعد المعلومات الإدارية التي يستخدمها البروتوكول "سنمب–ف2".

ب– قواعد معلومات إدارية من مدير لآخر، Manage-to-Manager MIB.

ج– قواعد معلومات إدارية لطرفي الاتصالParty MIB .

1.3 قواعد المعلومات الإدارية المستخدمة في "سنمب-ف2"

تنقسم قواعد المعلومات الإدارية التي يستخدمها البروتوكول "سنمب–ف2" ؛ كما موضح في الشكل4.4 ؛ إلى خمسة مجموعات هي:



الشكل4.4 قواعد المعلومات الإدارية لسنمب–ف2

أ- مجموعة إحصاءات الإصدار الثاني SNMPv2 Statistics Group.

ب- مجموعة إحصاءات الإصدار الأول SNMPv1 Statistics Group.

ج- مجموعة مصادر العناصر Object Resource Group.

د- مجموعة رسائل المصيدة Traps Group.

هـ - مجموعة التشغيل Set Group.

وقد تم تعريف وتوصيف هذه المعلومات الإدارية في التوصيات RFC. وفيما يلي شرحٌ لهذه الوظائف.

أولا: مجموعة إحصاءات الإصدار SNMPv2

وهى توضح العناصر التي تقوم بتوفير الإحصائيات عن المدير والوكيل للبروتوكول "سنمب-ف2". وهي توفر بالتحديد معلومات عن الرسائل التي لم يتم استطاعة معالجتها. وهي تماثل في وظائفها مجموعة قواعد المعلومات الإدارية MIB-II.

ثانيا: مجموعة إحصاءات الإصدار SNMPv1

وهي توفر العناصر التي تعطي إحصاءات عن المدير أو الوكيل SNMPv2 التي تتصل أيضا مع البروتوكول SNMPv1. على سبيل المثال، فإن العنصر الموجود في مجموعة هذه المعلومات MIB يقوم بعد count عدد الرسائل التي بها "حروف مشاركة Community Strings" خطأ.

ثالثا: مجموعة مصادر العناصر Object Resources

وهي توفر المعلومات التي تحدد عناصر وكيل البروتوكول "سنمب-ف2" المسموح لها أن تحدد ديناميكيا. كل مصدر عنصر يكون له محدد عنصر Object Identifier (OID)، ووصف Description. يستطيع المدير- بواسطة إجراء استفسار- تحديد المعاملات البروتوكولية المسموح لها أن تهيأ ديناميكيا داخل الوكيل. يمكن ؛على سبيل المثال أن يكون أحد هذه العناصر، هو قيام طرف الاتصال Party بإجراء عملية التوثيق Authentication، أو عملية التشفير Encryption.

رابعا: مجموعة رسائل المصيدة Traps Group

تحتوي هذه المجموعة على رسائل المصايد traps التي يمكن أن يرسلها الوكيل. يصاحب كل رسالة trap محدد العنصر OID، وعداد Counter لتحديد عدد المرات التي تم فيها إرسال رسالة trap. ربما يحتوي هذا الجدول – على سبيل المثال– على معلومات تبين أن الوكيل يستطيع إرسال رسالة trap تبين متى حدث اختناق congestion في منفذ مفتاح Switch Port لشبكة إقليمية WAN. وأن العداد counter المصاحب لرسالة trap سوف يخبرنا بعدد المرات التي قام بها الوكيل بإرسال رسالة trap إلى المدير.

خامسا: مجموعة التشغيل Set Group

توفر هذه المجموعة من المعلومات عنصرا منفردا Single Object يسمح لمديرين متعددين أن ترسل رسائل تشغيل SNMP Set إلى وكيل منفرد دون مشاكل أو معاناة. ويطلق على هذا العنصر "رقم تسلسل التشغيل Set Serial Number"، ليساعد على تجنب الشروط التي بها يمكن أن يعاود اثنين من المديرين تشغيل نفس عنصر قاعدة المعلومات الإدارية في نفس الوقت تقريبا، وذلك بواسطة زيادة العد لمرة incrementing once لكل طلب تشغيل Set Request يتم معالجته processed.

مثال: عندما يقوم وكيل باستقبال طلب تشغيل Set Request من بروتوكول "سنمب" من مدير يسمى "ألفا" ليقوم بإغلاق الوحدة البينية interface لشبكة ايثرنيت. يمكن قبل إتمام هذه العملية، أن تصل رسالة طلب تشغيل Set Request من البروتوكول "سنمب" من المدير الآخر "بيتا" لتخبر الوكيل أن يقوم بتشغيل نفس الوحدة البينية لشبكة ايثرنيت. عندما يقوم المدير "ألفا" بفحص حالة الوحدة البينية لشبكة ايثرنيت، فإنه يجدها في حالة تشغيل، وليست مغلقة. ويعتقد بذلك أن الوكيل ربما يكون به خطأ أو مشكلة. لتجنب هذه المشكلة، فإن المدير "ألفا" يحتاج الاستفسار عن رقم تسلسل التهيئة the set serial number قبل وبعد معالجة رسالة التشغيل Set Request. بسبب أن رقم تسلسل التشغيل (أو التهيئة) يزداد عند كل عملية معالجة يقوم بها الوكيل لكل رسالة Set

Request ، فيمكن للمدير "ألفا" أن يفهم أنه قد تم معالجة رسالة أخرى Set Request. وأنه ربما يكون السبب أن الوحدة البينية لشبكة ايثرنيت تكون حالياً في حالة تشغيل.

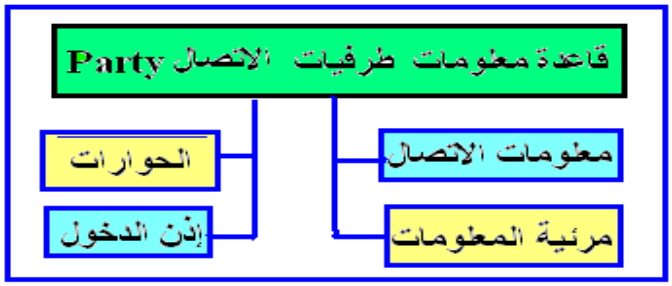
2.3 قاعدة المعلومات الإدارية الخاصة بالمديرين

توفر هذه العناصر معلومات عن كيفية تصرفات المدير في البروتوكول"سنمب–ف2". وتنقسم عناصر هذه المعلومات الإدارية إلى مجموعتين هما: مجموعة الإنذارات Alarm Group، ومجموعة الأحداث Event Group. وهاتان المجموعتان تشبهان مجموعة الإنذارات، ومجموعة الأحداث الأساسية لبروتوكول الرصد عن بعد RMON، والذي سوف يتم شرحه في الوحدة الدراسية السادسة من هذا الكتاب.

3.3 قاعدة المعلومات الإدارية لأطراف الاتصال Parity MIB

تحتوي قاعدة المعلومات الإدارية لأطراف الاتصال، على عناصر لوصف تهيئة أطراف الاتصال Parties المصاحبة لأحد كيانات Entity بروتوكول"سنمب–ف2" (الوكيل Agent).

و تنقسم، كما هو موضح في الشكل 4.5، إلى أربعة مجموعات هي:



الشكل4.5 مجموعات قاعدة المعلومات الإدارية لأطراف الاتصال.

أ– مجموعة قاعدة معلومات طرفي الاتصال Party.

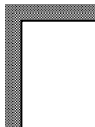
ب– مجموعة قاعدة معلومات الحوارات البروتوكولية (السياق contexts).

ج– مجموعة قاعدة المعلومات المميزة لإذن الدخول.

د- مجموعة قاعدة المعلومات الخاصة برؤية المعلومات الإدارية MIB View.

تحتوي قاعدة معلومات طرفي الاتصال Party على المعلومات التي تخزن في الجهاز عن كل أطراف الاتصال المحلية والبعيدة. تحدد بعض هذه المعلومات العمر الزمني لطرف الاتصال، وكيفية تخزين معلومات عن طرف الاتصال في ذاكرة القراءة فقط ROM، وذاكرة القراءة والكتابة RAM. أما المجموعات الثلاثة الأخرى من قواعد المعلومات، فإنها تتعامل مع امتيازات Privileges بين المدير والوكيل. وتسمح هذه المجموعات بالتحكم في السياقات الحوارية المحلية والبعيدة لمحطة بروتوكول "سنمب-ف2". وكذلك التحكم في طريقة الوصول إلى الوكيل أو المدير التنفيذيين وتحديد رؤية المعلومات الإدارية الحالية، وأطراف الاتصال التي تمكن الوصول إليهم.

أسئلة تقويم ذاتي



عدد أقسام قاعدة المعلومات الإدارية لبروتوكول سنمب-ف2.

اشرح وظائف مايلي :

مجموعة إحصاءات الإصدار SNMPv2.

مجموعة مصادر العناصر Object Resources.

4. التوافق Coexistence مع إصدارات بروتوكول سنمب

إن الهدف من إنشاء الإصدار الثاني لبروتوكول "سنمب" هو أن يتم استخدامه ليحل مكان الإصدار الأول "سنمب-ف1". لتحقيق هذا الانتقال، فإن مديرين ووكلاء بروتوكول الإصدار الأول لسنمب، ينبغي أن تواجه مشكلة التعامل مع هياكل المعلومات الإدارية SMI، وكذلك المشكلة المتعلقة بتغيير رسائل البروتوكول.

إن التغيرات في هياكل المعلومات الإدارية SMI لبروتوكول "سنمب-ف2" تجعل من الضروري لكل من الوكلاء والمديرين أن يتم تحديثهم كي تتعامل مع أنواع المعلومات

الجديدة الموجودة في بروتوكول "سنمب–ف2". لكن بما أن هياكل المعلومات الإدارية SMI لبروتوكول "سنمب–ف2"، تعتبر مجموعة متقدمة Super Set من هياكل المعلومات الإدارية للإصدار الأول لسنمب؛ فإن جميع قواعد إدارة المعلومات الإدارية، المعروفة للإصدار الأول لسنمب، تكون متوافقة مع مديرين ووكلاء الإصدار الثاني. وأنه من المهم أن تتواءم التعريفات المحددة في هيكل المعلومات الإدارية لسنمب–ف1، مع هيكل إدارة المعلومات SMI لسنمب–ف2 لأسباب قياسية، وليس فقط لأسباب التشغيل.

إن رسائل البروتوكول سنمب–ف2، تكون أيضا مشابهة جدا لرسائل سنمب–ف1. كلا من البروتوكولين لهما نفس رسائل:

.Get-Request, Get-Next-Request, Set-Request, Get-Response, Traps

بالإضافة إلى أن البروتوكول "سنمب–ف2" به رسالة GetBulkRequest التي يمكن اعتبارها سلسلة من رسائل Get-Next-Request الموجودة في الإصدار الأول "سنمب–ف1". إن عملية التحويل السلسة بين أنواع الرسائل لكلا البروتوكولين سنمب–ف1، سنمب–ف2 ، يعني أنه يوجد طريقتان للاتصال بين محطتي الاتصال التي تستخدم الإصدارين. الطريقة الأولى هي أن يتم استخدام وكيل مساعد Proxy Agent لتحويل الرسائل Message Translation . والطريقة الثانية هي أن يتم استخدام مدير يتعامل مع البروتوكولين سنمب–ف1، سنمب–ف2.

<u>طريقة :استخدام مدير يتعامل مع البروتوكولين سنمب–ف1، سنمب–ف2:</u>

إن استخدام مدير يتعامل مع البروتوكولين سنمب–ف1، سنمب–ف2، هو الذي يتم استخدامه بسهولة هذه الأيام، لأن المدير يستطيع اتخاذ قرار ديناميكي Dynamic Decision عن البروتوكول الذي يحتاج إليه لكي يخاطب كل وكيل. يحتاج المدير أن يستفسر عن الوكيل الجديد مرة باستخدام رسالة GetRequest للإصدار الثاني لسنمب، للحصول على شيء ما موجود في الجهاز(مثل اسم الجهاز)، ليعرف إن كان الجهاز يستجيب أم لا. عندما لا يستجيب الجهاز، فإن المدير يستطيع إرسال رسالة Get-

Request من الإصدار الأول لسنمب إلى الجهاز للاستفسار عن نفس المعلومات. عندما يستجيب الجهاز، فإن المدير يستطيع تحديد أن هذا الجهاز يستخدم بروتوكول الإصدار الأول لسنمب. إذا لم يستجب الجهاز، ولا يوجد تعليقات يمكن أخذها منه بعد، ربما يكون الجهاز مطفأ. أيضا باستخدام مدير يعمل باللغتين Bilingual، هما الإصدار الأول والثاني لسنمب، فإن ذلك يقلل من الاحتياج إلى تخصيص وكلاء مساعدين Proxy Agents في الشبكة لإتمام عملية التحويل من الإصدار الأول إلى الإصدار الثاني للبروتوكول "سنمب".

كذلك تستخدم طرق مماثلة لتحقيق التوافق مع بروتوكول الإصدار الثالث "سنمب–ف3".

5. قاعدة المعلومات الإدارية MIB-II

يتم بصفة دورية تحديث وتنقيح قواعد المعلومات الإدارية، بهدف تصحيح أي نواقص تظهر فيها نتيجة الخبرات العملية، وكذلك إضافة عناصر جديدة إليها. تحتوي قاعدة المعلومات الإدارية MIB-II على أحد عشر مجموعة تم تبيانها سابقا في الجدول 4.2، وسوف نتناول في هذا الجزء من الوحدة الدراسية، دراسة كل عنصر منها ودلالاته وتأثيره في إدارة الشبكة. وخلال هذه الدراسة سوف نقوم بفحص معدل التغير في عنصر MIB-II .

- **معدل التغير للعنصر:**

يعرف معدل التغير Rate of Object بأنه كمية التغيرات لعنصر محدد بين الزمن t والزمن t+1 ، مقسوما على الفرق الزمني بين t، t+1، كما في المعادلة التالية:

$$Rate\ of\ Object = \frac{Value\ of\ Object\ (at\ t+1) - Value\ of\ Object\ (at\ t)}{(t+1) - t}$$

يوجد وسائل عديدة يمكن بواسطتها حساب هذا المعدل آليا. حيث تستخدم بعض نظم إدارة الشبكات خصائص الرسم لحساب معدل عنصر MIB-II. أخرى تسمح بأن تكتب

برامج بسيطة لحساب هذا المعدل. أيضا يمكن أن نجد تطبيق إدارة الشبكة يخزن قيم العناصر في قاعدة بيانات علاقية، ونستخدم أوامر SQL لإجراء حسابات المعدل.

إن كل الوظائف التي يتم وصفها في هذه الوحدة الدراسية يمكن تنفيذها بواسطة مهندس الشبكة يدويا، لكن يفضل أن يتم ذلك بواسطة استخدام تطبيق إدارة شبكة مناسب، كما سوف يتم شرحه تباعا.

1.5 مجموعة النظام System Group

تحتوي مجموعة النظام معلومات عن النظام الذي يوجد به محطة التشغيل entity . يفيد الكثير من هذه العناصر في إدارة الأداء وإدارة التهيئة.

أولا: مجموعة عناصر النظام الخاصة بإدارة الأعطال:

تشتمل عناصر مجموعة النظام التي تستخدم في إدارة الأعطال في الشبكة على ما يلي:

أ- عنصر "الهوية" sysObjectID: يستخدم لبيان هوية عنصر النظام، ويفيد لتصنيف الموردين لأجهزة الشبكة، وكذلك البيانات المعاونة لمعرفة مصنعي الأجهزة.

ب- عنصر "الخدمات" sysServices: يحدد طبقة خدمات الجهاز في النموذج المرجعي OSI ذو الطبقات السبعة. تستخدم المعادلة ***2^(L-1)*** ، حيث ***L*** هو رقم المستوى المحدد لطبقة البروتوكول. وأن القيمة العائدة returned تساوي مجموع القيم لكل طبقة بروتوكول.

مثال: إن الموجه Router الذي يعمل أساسا عند المستوى الثالث، سوف يرجع القيمة ***2^(3-1)*** وهي تساوي ***4*** . بينما الحاسب المضيف Host الذي يعمل عند خدمات طبقة

النقلTransport Layer (المستوى الرابع)، وخدمات طبقة التطبيقات Application Layer (المستوى السابع) سوف يرجع قيمة تساوي ***72*** تم حسابها بواسطة جمع القيمة العائدة من كل طبقة، كما يلي:

$$2^{(7-1)} + 2^{(4-1)} = 64 + 8 = 72$$

تفيد هذه المعلومات في حل مشاكل فحص الأعطال Debugging عندما توجد مشكلة غير معروفة عند تشغيل الجهاز.

ج- عنصر "التشغيل" sysUpTime : يبين طول المدة التي اشتغل فيها النظام. يمكن باستخدام تطبيق إدارة الأعطال إجراء عملية التصويت Polling على هذا العنصر، وأن نعرف ما إذا كانت محطة التشغيل entity قد تم إعادة تشغيلها restarted . إذا وجد التطبيق زيادة في قيمة العنصر sysUpTime، فإننا نعرف أن محطة التشغيل تكون قد بدأت العمل. إذا كانت القيمة الزمنية للعنصر sysUpTime أقل من قيمتها السابقة، فإننا ندرك أن محطة التشغيل قد بدأت إعادة العمل منذ التصويت الأخير Last Poll.

عندما تقل قيمة الزمن sysUpTime منذ التصويت الأخير للعنصر، يمكن لتطبيق الإدارة أن يفترض إما أن تكون محطة تشغيل الوكيل agent قد بدأت إعادة التشغيل، أو أن قيمة الزمن sysUpTime قد وصلت إلى القيمة العظمى لها وهي2^32 -1 .

أحد الوسائل الممكنة لتحديد أي من هذه الوقائع قد حدثت، هو النظر في المدة الزمنية منذ فترة التصويت الأخير، والقيمة الأخيرة المعروفة للزمن sysUpTime . من ذلك يتم تحديد إذا كان شرط حدوث wrap قد تحقق. **عندما يتحقق شرط وجود** wrap ، فإن تطبيق الإدارة لا يستطيع تحديد أي من الحدثين قد وقع. كما سوف نشرح في الوحدة الدراسية الخامسة، أن قاعدة المعلومات الإدارية لرصد جهاز الشبكة عن بعد RMON-MIB يوصي بإجراء عملية تصويت متعددة للعناصر حتى يستطيع تحديد أي من الحدثين قد تم وقوعه.

د- عنصر"جدول الفحص" ifTestTable : يحدد جدول عناصر يتكون من صف واحد لكل وحدة بينية Interface في محطة التشغيل. يحدد هذا الجدول العناصر التي تسمح

لتطبيق إدارة الشبكة بأن يختبر أنواعاً متعددةً من الأعطال في الوحدة البينية. يتم تحديد الاختبارات الفعلية لوحدة بينية محددة في قاعدة المعلومات الإدارية الخاصة بالوسط Media لهذه الوحدة. على سبيل المثال، يتم تحديد اختبارات وحجة بينية لشبكة حلقة Token بواسطة نوع قاعدة المعلومات التي تسمى IEEE802.5 Token Ring Interface.

ثانيا: مجموعة عناصر النظام الخاصة بإدارة التهيئة

يبين الجدول4.3 ، مجموعة عناصر النظام التي تستخدم في إدارة التهيئة، واستخداماتها.

الجدول4.3

عناصر النظام الخاصة بإدارة التهيئة واستخداماتها.

مسمى العنصر	استخدامه
"وصف النظام" sysDescr	هو عبارة عن نظام التشغيل المتاح أو البرمجيات المرجعية الخاصة بمحطة التشغيل. تفيد هذه البيانات في كل من إدارة تشغيل الجهاز، وفحص الأعطال.
"مكان النظام" sysLocation	يحدد مكان التواجد الفعلي للنظام.
"مسئول النظام" sysContact	يحدد الشخص الذي يتم الاتصال به عند وقوع مشاكل.
"اسم النظام" sysName	يحدد اسم جهاز الشبكة.

2.5 مجموعة البينية Interface Group

توفر مجموعة البينية بيانات عن الوحدات البينية لأجهزة الشبكة. وتفيد في العمليات الإدارية الخاصة بالأعطال، والتهيئة، والأداء، والحسابات. وتحتوي هذه المجموعة على جدول العناصر، كل صف فيه يمثل بينية واحدة في محطة التشغيل. يلخص الجدول4.4 مجموعة البينية ووظائفها. تتيح مجموعة البينية في قاعدة المعلومات الإدارية MIB-II المطورة ما يلي:

أ- جدول جديد للعناصر لكل وحدة بينية في محطة التشغيل.

ب- طريقة مرجعية لترقيم الوحدة البينية.

ج- قيم أضخم لعناصر وحدة بينية معينة.

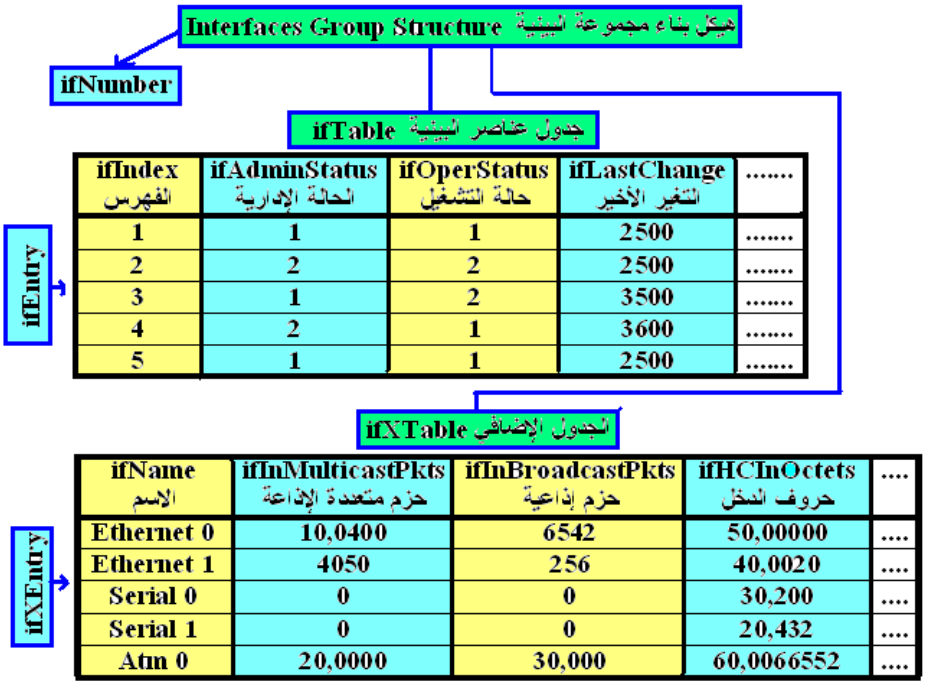
د- طريقة لمعالجة المستويات الفرعية sublayers للوحدة البينية.

جدول4.4

عناصر مجموعة البينية ووظائفها

اسم العنصر	وظيفته
ifTable	يحتوي معلومات عن الوحدات البينية في محطة التشغيل
ifEntry	صف من المعلومات عن بينية محددة
ifXTable	جدول إضافات للعناصر الموجودة في الجدول ifTable
ifNumber	يحتوي على سجلات records لعناصر ifEntry
ifIndex	عدد صحيح يبين فهرس مصفوفة مجموعات ifEntry

يوضح الشكل4.6 مثالا لهيكل Structure مجموعة الوحدات البينية. وهو لجهاز به خمس وحدات بينية. يمكن الاستفسار عن عدد السجلات في ifNumber ، سوف نجده يحدد القيمة 5. كما نلاحظ – في هذا المثال- أنه لم يتم إظهار كل العناصر المتاحة في كل من الصف ifEntry ، والجدول الإضافي ifXTable.



الشكل4.6 مثال لهيكل مبسط لمجموعة البينية.

- **أولا: عناصر مجموعة البينية المستخدمة في إدارة الأعطال:**

تشتمل عناصر مجموعة البينية التي يمكن تطبيقها في إدارة الأعطال على أربعة عناصر هي: عنصر الحالة الإدارية"ifAdminStatus"، عنصر حالة التشغيل "ifOperStatus"، عنصر التغير الأخير "ifLastChange"، وعنصر فحص العطل "ifTestTable". إن اتحاد العنصران ifAdminStatus, ifOpenStatus يجعل تطبيق إدارة الأعطال قادراً على تحديد الحالة الحالية Current Status للوحدة البينية. كلاً من العنصران يقومان بإرجاع أعداد صحيحة توضح حالة الوحدة البينية، كما هو مبين في الجدول4.5.

جدول4.5

بيان الحالة الحالية للوحدة البينية، المناظرة للرقم العائد من العنصر.

الرقم العائد	بيان الحالة الحالية للوحدة البينية
1	Up تشغيل
2	Down توقف
3	Testing تحت الاختبار
4	Unknown غير معروفة
5	Dormant انتظار وقوع حدث محدد قبل الانتقال لحالة التشغيل
6	Not present مكونات مفقودة
7	Lower layer Down المستوى السفلي للبروتوكول متوقف

يبين الجدول4.5 –على سبيل المثال – ما يلي:

– تكون الوحدة البينية تعمل، عندما يقوم العنصران ifOpenStatus, ifAdminStatus بإرجاع حالة تشغيل up (أي العدد 1).

– تكون الوحدة البينية متوقفة، عندما يقوم العنصران ifOpenStatus, ifAdminStatus بإرجاع حالة توقف down (أي العدد 2).

عندما يقوم العنصران ifOpenStatus, ifAdminStatus بعدم إرجاع أية قيمة من نتيجة عملية الاستفسار query ، فإن محطة التشغيل أو برامج الجهاز، ربما تعمل بطريقة غير سليمة. وأن العنصر ifLastChange سوف يحتوي على القيمة الزمنية sysUpTime للحالة المتعلقة بحالة التشغيل الحالية للوحدة البينية.

–عندما يجد تطبيق إدارة الشبكة، وحدة بينية يكون فيها العنصر ifOpenStatus=5 أي يظهر حالة السكون dormant ، فإن هذه الوحدة البينية تكون في حالة انتظار وقوع

حدث محدد قبل أن تنتقل إلى حالة التشغيل. من أمثلة ذلك ، عندما يقوم الجهاز بإجراء عمليات مثل:

- Dial-backup طلب خدمة النسخ الاحتياطي.
- Bandwidth-on-demand طلب سعة نطاق إضافية .
- Dial-on-demand features طلب خدمة خصائص إضافية.

فإن خاصية " طلب خدمة النسخ الاحتياطي" Dial-backup تشير إلى وحدة بينية لجهاز تم تهيئته ليكون نشيطًا فقط عندما تتعطل الوحدة البينية الأساسية، وتستخدم غالباً في حالات العلاج عند الكوارث disaster-recovery.

يتم ضبط الوحدة البينية لتكون نشيطة فقط؛ عندما تتخطى الوحدة البينية الأساسية Primary القيمة الحدية لمعدل الاستخدام المحدد للمستخدم، وطلب خاصية الاحتياج إلى سعة نطاق إضافية Bandwidth-on-demand. تستخدم هذه الخاصية غالبا، لإتاحة سعة نطاق إضافية إلى مواقع sites ، نادرا ما يتم طلبها. مثلا: المكتب الذي يطلب سعة نطاق إضافية أثناء فترة الذروة في العمل Peak Business Period.

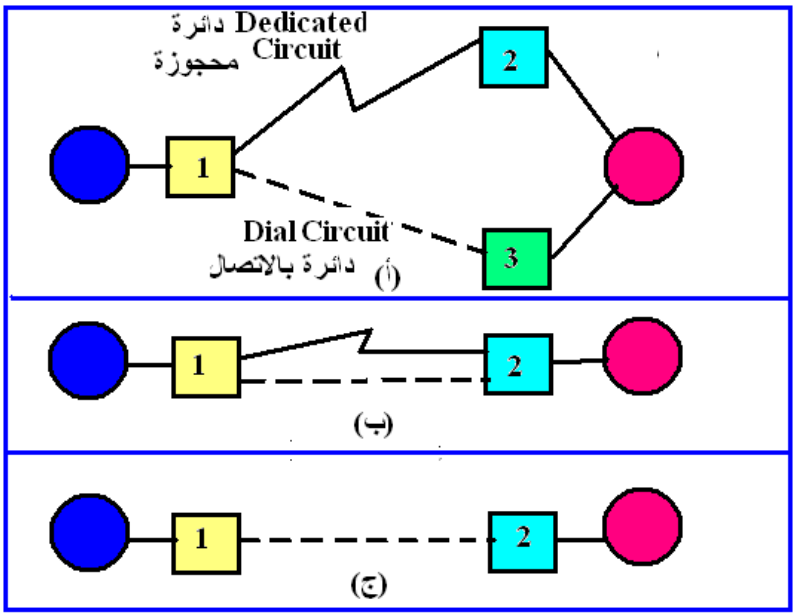
إن خدمة الاتصال عند الحاجة Dial-on-demand يستخدمها الجهاز الذي ليس له اتصال بالشبكة، لكن يصبح نشطًا ويجري اتصالات مؤقتة (ربما عن طريق جهاز مودم)، عندما تصله بعض الحزم البرمجية المهمة. وهذه الخاصية تستعمل غالبا للأجهزة التي ترسل كميات صغيرة من البيانات، ولا تحتاج وجود توصيلة دائمة.

يوضح الشكل4.7 خصائص اتصال باستخدام هذه الطرق السابقة.

في الشكل–أ، يقوم الجهاز رقم1 بطلب الاتصال بالجهاز رقم3 فقط عندما تتعطل الوصلة الأساسية التي تربطه بالجهاز رقم2.

الشكل–ب، يوضح حالة طلب سعة نطاق، يقوم الجهاز رقم1 بإجراء اتصال بالجهاز رقم2 فقط عندما تزيد سعة الوصلة الأساسية عن حد معدل الاستخدام المخصص لهذا المستخدم.

الشكل–ج، يوضح حالة طلب الاتصال عند الحاجة Dial-on-demand، حيث يقوم الجهاز بطلب الاتصال بالجهاز رقم2 فقط عندما تصله البيانات التي تجيز له إجراء الاتصال.



الشكل4.7 خصائص اتصال لطلب خدمة باستخدام بعض عناصر البينية.

- **<u>جدول عنوان المستقبل ifRcvAddressTable</u>**

يحتوي "جدول عنوان المستقبل" على مدخل لكل عنوان في محطة التشغيل، لاستقبال حزم بيانية packets لوحدة بينية محددة. وهذه المعلومات ربما تبلغ لمهندس الشبكة لكي يجري تهيئة محطة التشغيل، خاصة عندما تكون مصغية listening إلى عدد من العناوين أكثر من اللازم أو أقل من اللازم.

يمكن أن تستقبل الوحدة البينية حزم بيانات كلها إذاعية broadcasts ، أو مجموعة منها فقط مذاعة multicast، أو مذاعة لفرد واحد فقط unicasts (مرسلة مباشرة إلى محطة التشغيل). ربما تقوم الوحدة البينية بالإصغاء إلى العناوين الخاصة بمجموعة مذاعة multicast ،لكن يعتمد ذلك على بروتوكولات الشبكة التي تعمل في هذه الوحدة البينية.

على سبيل المثال، يمكن للوحدة البينية أن تصغي إلى عنوان مجموعة مذاعة مخصصة لشبكة ديكنت Dec_Net للفيز الرابع (رسائل الترحيب Hello Messages) عندما تكون الوحدة البينية تعمل بهذا البروتوكول.

يوجد العديد من البروتوكولات تستخدم عناوين مجموعة إذاعية خاصة لإرسال رسائل إلى مجموعة مختارة من الأجهزة خلال وسط الإرسال Medium. يستطيع تطبيق إدارة شبكة الدخول إلى جدول عناوين المجموعة الإذاعية، مستخدما بروتوكولات طبقة الشبكة ذات العلاقة، ويستطيع البروتوكول الاستدلال على بروتوكولات طبقة الشبكة التي تتخاطب معها محطة التشغيل.

ثانيا: عناصر مجموعة البينية المستخدمة في إدارة التهيئة

يبين الجدول4.6 عناصر مجموعة الوحدات البينية التي تستخدم في تطبيقات إدارة التهيئة. على سبيل المثال، عندما يقوم العنصر ifDescr بإرجاع الحروف "Ethernet0" ، فإن العنصر ifType ربما يقوم بإرجاع الرقم 6 . وأن معاني الأرقام التي يتم إرجاعها بواسطة العنصر ifType يتم تحديدها في قاعدة المعلومات الإدارية MIB. لكي تكون تطبيقات إدارة الشبكة أكثر تعاونا لنا، ينبغي أن تحول الرقم 6 إلى الحروف التي تعطينا معلومات أكثر عن نوع الوحدة البينية (مثلا: "Ethernet-CSMA/CD").

جدول4.6

عناصر مجموعة الوحدات البينية المستخدمة في إدارة التهيئة

تسلسل	العنصر object	المعلومات
1	ifDescr	وصف الوحدة البينية
2	ifName	اسم الوحدة البينية
3	ifType	نوع الوحدة البينية
4	ifMTU	أقصى طول رسالة داتاجرام خلال الوحدة البينية
5	ifSpeed	سرعة معلومة / ثانية للوحدة البينية
6	ifAdminStatus	الحالة الإدارية للبينية(تعمل-متوقفة-تحت الاختبار)
7	ifHighSpeed	السرعة العالية للوحدة البينية
8	ifPromiscuousMode	نمط الاختلاط
9	ifConnectorPresent	ما إذا كان الوحدة البينية بها توصيلة فيزيقية
10	ifLinkUpDownTrapEnable	ما إذا كان الوحدة البينية تولد رسائل مصايد
11	ifRcvAddressTable	العناوين التي تستقبل منها الوحدة البينية حزم بيانات

- يقيس العنصر ifSpeed السرعة الحالية للوحدة البينية بت/ثانية. على سبيل المثال، للوحدة البينية ايثرنيت يقوم العنصر ifSpeed بإرجاع القيمة 10,000,000 بت/ثانية، وهي تساوي 10Mb/s. يفيد هذا العنصر في إيجاد السرعة الحالية للوحدة البينية التي ربما تتغير، مثل التي يمكن تخصيصها لسعة النطاق عند الطلب bandwidth-on-demand، عند وقوع حركة بيانات كثيفة heavy bursts traffic. و يستخدم العنصر ifHighSpeed فقط لقياس سرعات الوحدات البينية التي تصل سرعتها إلى 4.2Gb/sec أو أكثر. حيث إن طول هذا العنصر هو 64 خانة، و ذلك الطول يسمح بإنشاء عداد gauge يستطيع قياس هذه السرعات.

- يبين العنصر ifAdminStatus وجود حالة نشاطٍ إداريً، وذلك بواسطة طلب رجاء إعداد SNMP Set-Request . نستطيع أن نستخدم هذا العنصر عن بعد لتهيئة الوحدة البينية كي تعمل (أي تكون ON) أو لتتوقف (أي تكون Off).

- يخبرنا العنصر ifPromiscuousMode ما إذا كانت الوحدة البينية تقوم باستقبال جميع حزم البيانات من الوسط، سواء أكانت على عنوان محطة التشغيل أم لا، وهو يقوم بإرجاع القيمة نعم (true) أم لا (false). ربما يتم تهيئة الوحدة البينية كي تعمل في نمط الاختلاط ifPromiscuousMode لأسباب عديدة تشمل تحليل الشبكة Network Analysis.

- يخبرنا العنصر ifConnectorPresent عن وجود وصلة فيزيقية Physical Connector للوحدة البينية.

- يمكن أن نمثل الوحدة البينية الفيزيقية بواسطة مجموعة من الصفوف الوهمية virtual في الجدول ifTable، تسمى المستويات الفرعية sub-layers للوحدة البينية. عند هذه الحالة، إذا تغيرت حالة الوحدة البينية، فإن العديد من الوحدات البينية ربما ترسل رسائل traps لتطلب تشغيل الوصلة LinkUp، أو توقيف الوصلة LinkDown (كما يتطلب بروتوكول الوحدة البينية سنمب-ف1، سنمب-ف2). بسبب وجود هذه المجموعة من رسائل traps ،فإن واحدا منها سوف يكون زائدا redundant . وأن العنصر ifLinkUpDownTrapEnable سوف يجعل مهندس الشبكة يهيئ الوحدة البينية لكي ترسل traps تشغيل- وصلة، أو إيقاف- وصلة. وتحدد التوصيات RFC، أن المستويات الفرعية السفلى lowest للوحدة البينية فقط، هي التي تولد رسائل traps. يستطيع تطبيق إدارة التهيئة أن يستفسر من العنصر ifLinkUpDownTrapEnable لتحديد إن كانت الوحدة البينية ومستوياتها الفرعية تكون تهيئتها صحيحة.

- **<u>ثالثا: عناصر مجموعة البينية المستخدمة في إدارة الأداء</u>**

يبين الجدول4.7 قائمة عناصر مجموعة الوحدات البينية التي تستخدم في تطبيقات إدارة الأداء. ينبغي تصميم تطبيقات إدارة الأداء لمراقبة النسب المئوية للأخطاء في الوحدة البينية. ينبغي أن يكون التطبيق قادراً على إيجاد إجمالي عدد حزم البيانات أو الأخطاء في الوحدة البينية.

جدول4.7 عناصر مجموعة البينية التي تستخدم في تطبيقات إدارة الأداء.

مسلسل	العنصر object	المعلومات
1	**ifInDiscards**	معدل دخل المهملات
2	**ifOutDiscards**	معدل خرج المهملات
3	**ifInErrors**	معدل دخل الأخطاء
4	**ifOutErrors**	معدل خرج الأخطاء
5	**If`InOctets**	معدل الحروف المستقبلة
6	**ifOutOctets**	معدل الحروف المرسلة
7	**ifInUcastPkts**	معدل دخل حزم بيانات أحادية الإذاعة
8	**ifOutUcastPkts**	معدل خرج حزم بيانات أحادية الإذاعة
9	**ifInNUcastPkts**	معدل دخل حزم بيانات ليست أحادية الإذاعة
10	**ifOutNUcastPkts**	معدل خرج حزم بيانات ليست أحادية الإذاعة
11	**ifInUnknownProtos**	معدل دخل حزم بيانات بروتوكول غير معروف
12	**ifOutQLen**	إجمالي حزم البيانات في طابور الخرج.
13	**ifInMulticastPkts**	معدل دخل حزم بيانات عديدة الإذاعة
14	**ifInBroadcastPkts**	معدل دخل حزم بيانات عريضة الإذاعة
15	**ifOutMulticastPkts**	معدل خرج حزم بيانات عديدة الإذاعة
16	**ifOutBroadcastPkts**	معدل خرج حزم بيانات عريضة الإذاعة
17	**ifHCInOctets**	معدل الحروف المستقبلة، للوحدة البينية عالية السعة
18	**ifHCOutOctets**	معدل الحروف المرسلة، للوحدة البينية عالية السعة
19	**ifHCInUcastPkts**	معدل دخل حزم بيانات أحادية الإذاعة، للوحدة البينية عالية السعة
20	**ifHCOutUcastPkts**	معدل خرج حزم بيانات أحادية الإذاعة، للوحدة البينية عالية السعة
21	**ifHCInMulticastPkts**	معدل دخل حزم بيانات عديدة الإذاعة، للوحدة البينية عالية السعة
22	**ifHCOutMulticastPkts**	معدل خرج حزم بيانات عديدة الإذاعة، للوحدة البينية عالية السعة
23	**ifHCInBroadcastPkts**	معدل دخل حزم بيانات عريضة الإذاعة، للوحدة البينية عالية السعة
24	**ifHCOutBroadcastPkts**	معدل خرج حزم بيانات عريضة الإذاعة، للوحدة البينية عالية السعة

يستطيع التطبيق تحديد إجمالي عدد حزم البيانات المستقبلة من الوحدة البينية بواسطة جمع العنصر ifOutUcastPkts والعنصر ifOutNUcastPkts. كذلك نحصل على إجمالي عدد حزم البيانات المرسلة بواسطة الوحدة البينية، بجمع العنصر ifOutUcastPktsو العنصر ifOutNUcastPkts.

إجمالي حزم البيانات المرسلة = ifOutUcastPkts+ifOutNUcastPkts

إجمالي حزم البيانات المستقبلة = ifInUcastPkts+ifInNUcastPkts

وعند إضافة العناصر الخاصة بإعادة إذاعة كل حزم البيانات، أو إذاعة مجموعة حزم البيانات ، إلى جدول العنصر ifXTable ، تصبح المعادلات كما يلي:

إجمالي حزم البيانات المرسلة =
ifOutUcastPkts+ifOutBroadcastPkts+ifOutMulticastPkts

إجمالي حزم البيانات المستقبلة =
ifInUcastPkts+ifInBroadcastPkts+ifInMulticastPkts

يمكن حساب النسبة المئوية للأخطاء في الدخل والخرج في الوحدة البينية كما يلي:

النسبة المئوية للأخطاء في الدخل = ifInErrors / Total Packets Received

النسبة المئوية للأخطاء في الخرج = ifInErrors / Total Packets Received

يستطيع التطبيق استخدام طرق مماثلة لرصد عدد حزم البيانات المهملة discarded بواسطة الوحدة البينية، وذلك باستخدام العنصران ifInDiscards, ifOutDiscards. يمكن أن تنتج الأخطاء والمهملات من وحدة بينية لا تعمل بشكل سليم، أو مشاكل في وسط الاتصال، أو مشاكل في مخازن البيانات في الجهاز، أو من مشاكل أخرى.

ملاحظة

عندما يتم كشف الأخطاء، فإننا نستطيع اتخاذ إجراء لتصحيحها. لكن ينبغي أن نعي أنه ليس كل المهملات تمثل مشكلة. على سبيل المثال، إن الجهاز الذي يوجد به نسبة مرتفعة من المهملات، يمكن أن يكون ذلك بسبب أنه يستقبل العديد من حزم البيانات من بروتوكول غير معلوم. يمكن أن نجد عدد المهملات الناتجة من هذه الحالة في العنصر ifInUnknownProtos .

مثال: نفترض جهاز الشبكة الذي يمرر فقط بروتوكول IP. فإن الجهاز الذي له وحدة بينية على الإيثرنيت ؛ حيث يوجد العديد من الحواسيب الشخصية تكون شبكة من الخدم والعملاء تقوم بإرسال رسائل بينها، مثل إذاعات ايثرنيت Ethernet Broadcasts. بسبب أن جهاز الشبكة ينبغي أن يستقبل هذه الإذاعات، فهو بذلك يقوم باستقبال العديد من حزم البيانات التي لا يعرف كيفية معالجتها. وذلك بسبب زيادة العدد في العنصر ifInDiscards ، والعدد الموجود في العنصر ifInUnknownProtos . كما نجد في هذه الحالة، فإن الأعداد الضخمة في كلا العنصران ، ربما لا تبين وجود مشكلة.

يستطيع تطبيق إدارة الأداء استخدام العنصران ifInOctets, ifOutOctets لحساب النسبة المئوية لمعدل الاستخدام Utilization في الوحدة البينية . لإجراء هذه العملية الحسابية، فإن ذلك يتطلب إجراء التصويت poll مرتين مختلفتين، إحدهما لإيجاد إجمالي الحروف عند الزمن x ، والأخرى إيجاد إجمالي الحروف عند الزمن y . ونستخدم المعادلة التالية لحساب إجمالي عدد الحروف المرسلة والمستقبلة بين زمني التصويت x, y بالثانية، كما يلي:

إجمالي عدد الحروف (Total Bytes)

(ifInOctets at y – ifInOctets at x) +
(ifOutOctets at y – ifOutOctets at x)

إجمالي الحروف / الثانية = (Total Bytes) / (y – x)

ثم نحسب معدل استخدام خط الاتصال Line Utilization ، كما يلي:

في حروف *معدل الاستخدام = (إجمالي عدد الحروف / الثانية * 8) مقسوما على السرعة ifSpeed*

bytes إلى وحدة بت bits، حيث إن وحدة العنصر ifSpeed تكون بت / ثانية.

نلاحظ أن الوحدة البينية التي تجري عملية الاتصال في اتجاهين Full Duplex (خط مخصص لإرسال، و خط مخصص للاستقبال)، مثل وصلة التوالي، فإن هذه المعادلة سوف تحسب قيمة مضاعفة لمعدل استخدام الوحدة البينية.

على سبيل المثال، نفترض وصلة التوالي التي تعمل بسرعة 64 كيلوبايت/ثانية في اتجاهين. عندما نحسب إجمالي عدد حروف الدخل والخرج للوحدة البينية، فإننا سوف نحسب معدل استخدام الوصلة 128 كيلوبايت/ثانية. أحد الحلول لهذه المشكلة هو أن نحسب الأعداد المنفصلة لإجمالي حروف الدخل والخرج خلال المدة الزمنية المعطاة. بعد ذلك نأخذ العدد الأكبر لهاتين القيمتين، ونقسمه على قيمة العنصر ifSpeed (أو العنصر ifHighSpeed).

- **<u>توصيات خاصة بعناصر طول العداد Length Size</u>**

يبين الجدول4.8 بعض السرعات الممكنة للوحدات البينية، وطول عداد السرعات الواجب استخدامه في محطة التشغيل.

جدول**4.8**

سرعات البينية وطول العداد المستخدم.

سرعة البينية	طول العداد الواجب استخدامه
أقل من 20 ميجا بايت / ثانية	32 بيت لإجراء عد الحروف وحزم البيانات
من 20 إلي 650 ميجا بايت / ثانية	32 بيت لعد حزم البيانات، 64 بيت لعد الحروف
أكبر من 650 ميجا بايت / ثانية	64 بيت لعد حزم البيانات، وعد الحروف.

طبقا لهذه التوصيات، فقد تم إضافة ثمانية عناصر لجدول ifXTable وهي العناصر التي تبدأ بالحرفين HC وهى تعني High Capacity وتشير لاستخدام عدادات طولها

64 بيت. ينبغي أن تستخدم محطة التشغيل، هذه العناصر حسب القواعد الموضحة في الجدول4.7 السابق.

إن العنصر ifOutQLen يخبرنا ما إذا كان الجهاز يعاني مشاكل في إرسال البيانات الخارجة من الوحدة البينية. وأن قيمة هذا العنصر سوف تزداد عندما يزداد عدد حزم البيانات المنتظرة لمغادرة الوحدة البينية. تنتج مشاكل إرسال البيانات نتيجة أخطاء في الوحدة البينية، أو نتيجة عدم قدرة الجهاز على التعامل مع حزم البيانات بنفس السرعة التي تدخل بها. على الرغم من أن عدد حزم البيانات الضخمة المنتظرة في طابور الخرج output queue لا تسبب مشكلة ملحة، فإن تنامي وجودهما ربما يبين حدوث اختناق congestion في الوحدة البينية.

إن استخدام العنصرين ifOutDiscards, ifOutOctets، معاً ربما يعطينا بيان حدوث الاختناق في الشبكة. عندما يقوم جهاز الشبكة، بإهمال العديد من حزم البيانات التي تحاول مغادرة الوحدة البينية، كما هو مبين بواسطة العنصر ifOutDiscards، وأن إجمالي عدد حروف الخرج تقل، كما هو مبين بواسطة العنصر ifOutOctets، فإن الوحدة البينية ربما تكون مختنقة congested.

- **رابعا: عناصر مجموعة البينية المستخدمة في إدارة الحسابات**

يبين الجدول4.9 قائمة عناصر مجموعة الوحدات البينية المستخدمة في إدارة الحسابات.

الجدول4.9 عناصر مجموعة البينية المستخدمة في إدارة الحسابات.

مسلسل	العنصر object	المعلومات
1	If`InOctets	إجمالي الحروف المستقبلة
2	ifOutOctets	إجمالي الحروف المرسلة
3	ifInUcastPkts	إجمالي حزم بيانات أحادية الإذاعة المستقبلة
4	ifOutUcastPkts	إجمالي حزم بيانات أحادية الإذاعة المرسلة
5	ifInNUcastPkts	إجمالي حزم بيانات ليست أحادية الإذاعة المستقبلة
6	ifOutNUcastPkts	إجمالي حزم بيانات ليست أحادية الإذاعة المرسلة
7	ifInMulticastPkts	إجمالي حزم بيانات عديدة الإذاعة المستقبلة
8	ifOutMulticastPkts	إجمالي حزم بيانات عديدة الإذاعة المرسلة
9	ifInBroadcastPkts	إجمالي حزم بيانات عريضة الإذاعة المستقبلة
10	ifOutBroadcastPkts	إجمالي حزم بيانات عريضة الإذاعة المرسلة
11	ifHCInOctets	إجمالي الحروف المستقبلة، للوحدة البينية السريعة
12	ifHCOutOctets	إجمالي الحروف المرسلة، للوحدة البينية السريعة
13	ifHCInUcastPkts	إجمالي حزم بيانات أحادية الإذاعة، المستقبلة للبينية السريعة
14	ifHCOutUcastPkts	إجمالي حزم بيانات أحادية الإذاعة، المرسلة للبينية السريعة
15	ifHCInNUcastPkts	إجمالي حزم بيانات ليست أحادية الإذاعة، المستقبلة للبينية السريعة
16	ifHCOutNUcastPkts	إجمالي حزم بيانات ليست أحادية الإذاعة، المرسلة للبينية السريعة
17	ifHCInMulticastPkts	إجمالي حزم بيانات عديدة الإذاعة، المستقبلة للبينية السريعة
18	ifHCOutMulticastPkts	إجمالي حزم بيانات عديدة الإذاعة، المرسلة للبينية السريعة
19	ifHCInBroadcastPkts	إجمالي حزم بيانات عريضة الإذاعة، المستقبلة للبينية السريعة
20	ifHCOutBroadcastPkts	إجمالي حزم بيانات عريضة الإذاعة، المرسلة للبينية السريعة

- **<u>حساب فواتير الدفع بواسطة تحديد عدد الحروف المرسلة والمستقبلة</u>**

يستطيع تطبيق إدارة الحسابات استخدام العناصر الأربعة الآتية:

ifInOctets, ifOutOctets, ifHCInOctets, ifHCOutOctets

لتحديد عدد الحروف المرسلة والمستقبلة في الوحدة البينية؛ تساعد هذه البيانات جهاز الشبكة الذي يوجد به وحدة بينية متصلة بمحطة منفردة خاصة بحساب الفواتير Billing Entity . عندما تنتقل حركة الرسائل traffic التي تعبر هذه الوحدة البينية ، إلى محطة حساب فواتير أخرى؛ فإن نموذج الحسابات سوف لا يكون مناسبا. لكن، إذا لم تكن الوحدة البينية غير متصلة بمحطة منفردة خاصة بحساب فواتير الدفع بدون عبور

حركة الرسائل، فإنه لا يوجد حسابات ضرورية لإيجاد عدد الحروف التي ترسلها ، أو تستقبله محطة حساب فواتير الدفع من الشبكة. عندما يستخدم نموذج حساب فواتير الدفع عدد حزم البيانات بدلا من عدد الحروف، فإن العناصر من الرقم 3 إلى الرقم 10 المبينة في الجدول4.9، سوف تعطي عدد حزم البيانات اللازمة لإجراء عملية حساب فواتير الدفع. أما في حالة الوحدات البينية التي ترسل وتستقبل حزم بيانات عند سرعات عالية؛ فإننا نستخدم العناصر الخاصة بحسابات فواتير الدفع لحزم البيانات عند السرعات العالية، وتشمل العناصر من رقم 13 حتى الرقم 20 في الجدول4.9.

- **عناصر خاصة بتحديد المستويات الفرعية Sub-Layers للوحدة البينية**

إن كثيراً من محطات التشغيل Entities ربما يوجد بها وحدة بينية فيزيقية واحدة، لها خصائص وسط محددة لقواعد المعلومات الإدارية، التي تسكن أسفل المستوى الشبكي في النموذج المرجعي OSI. مثل: بروتوكول X.25 الذي يعمل أعلى طبقة برتوكول دخول الوصلة المتوازنة LAPB في الموصل V.35 Connector. في هذا المثال، نجد أن البروتوكول X.25 هو بروتوكول المستوى الشبكي، ويعمل أسفله البروتوكول LAPB وهو بروتوكول ربط البيانات، والبروتوكول V.35 يعمل في المستوى الفيزيقي. وأنه توجد قاعدة معلومات إدارية محددة ومميزة للوسط لكل من هذه المستويات التي تستخدم النموذج المرجعي OSI، للتعامل مع هذه المستويات البروتوكولية المتعددة. ويتم تخصيص صف في الجدول ifTable للتعبير عن كل مستوىً فرعيّ.

وكذلك جدول جديد آخر لقاعدة المعلومات الإدارية هو ifStackTable، لتحديد المستويات الفرعية العليا والسفلى للوحدة البينية. كما أن الجدول ifStackTable يوجد به طريقة تساعد في تحديد identify قاعدة المعلومات الإدارية الخاصة بالوسط لكل مستوى فرعي.

- **عناصر خاصة بالتعامل مع الدوائر الافتراضية Virtual Circuits للوحدة البينية**

تسمح تقنيات شبكات إقليمية معينة للعديد من الوصلات المنطقية، بأن تركب فوق وحدة بينية فيزيقية مفردة لإجراء الاتصالات، وتسمى هذه الوصلات بالدوائر الافتراضية. من أمثلة هذه التقنيات الشبكات التي تستخدم بروتوكول الاتصال X.25، ونظام ترحيل الأطر Frame Relay ، ونمط النقل غير المتزامن ATM . بسبب أن هذه الدوائر الافتراضية هي عبارة عن وصلة منطقية فوق وحدة بينية فيزيقية واحدة، فإنه يخصص لها صف منفرد في الجدول ifTable. وهذا الحل يكون منطقيا لأن قيمة عناصر قاعدة المعلومات الإدارية MIB في الجدول ifTable سوف تكون متطابقة لجميع الدوائر الافتراضية ، تاركة محطة التشغيل محتفظة بنسخ عديدة من نفس المعلومات. وأن تطبيقات إدارة الشبكة ينبغي أن تستفسر من قاعدة المعلومات الإدارية الخاصة بالوسط عن التقنية المعطاة للحصول على معلومات عن الدوائر الافتراضية. على سبيل المثال، عندما يحدد التطبيق أن الوحدة البينية تعمل باستخدام نظام مرحل الأطر، يمكن بعد ذلك أن تستفسر عن العناصر الموجودة في قاعدة المعلومات الإدارية الخاصة بمرحل الأطر.

- **عناصر خاصة بالتعامل مع البت، والحرف، والطول الثابت:**

تستخدم هذه العناصر في قاعدة المعلومات الإدارية للوحدات البينية للشبكات الخاصة التي تعمل بنظام حزم البيانات. وتحتوي قاعدة المعلومات الإدارية لهذه العناصر على المجموعات التالية:

أ- مجموعة المعلومات العامة ifGeneralGroup : تشمل العناصر التطبيقية لأنواع الوحدات البينية للشبكات الخاصة بالتعامل مع البت Bit-Oriented ، مثل دوائر DS1.

ب- مجموعة حزم البيانات ifPacketGroup : وتشمل العناصر التطبيقية لأنواع الوحدات البينية للشبكات الخاصة بالتعامل مع حزم البيانات Packet-Oriented، مثل شبكات X.25.

ج- كما تستخدم مجموعة عناصر ifHCPacketGroup: للوحدة البينية في الشبكات عالية السرعة.

د- أيضا، تستخدم مجموعة عناصر ifVHCPacketGroup: للوحدة البينية في الشبكات فائقة السرعة.

هـ- مجموعة الأطوال الثابتة ifFixedLengthGroup : تشمل العناصر التطبيقية لأنواع الوحدات البينية للشبكات التي ترسل بيانات ذات أطوال ثابتة، مثل خلايا المرحل في نظام النقل غير المتزامن Cell-Relay/ATM. كما أنها تطبق أيضا على عناصر الوحدات البينية التي تتعامل مع الحروف Character-Oriented مثل RS-232.

و- كما تستخدم مجموعة عناصر ifHCFixedLengthGroup : للوحدة البينية التي ترسل بيانات ذات أطوال ثابتة ، في الشبكات عالية السرعة.

أسئلة تقويم ذاتي

1. تحتوي مجموعة النظام System Group معلومات عن النظام الذي يوجد به محطة التشغيل Entity. اذكر عنصرين من مجموعة النظام، موضحا وظيفة كل منهما.

2. أ) ما وظيفة مجموعة البينية Interface Group ، المنبثقة من قاعدة المعلومات الإدارية MIB-II ؟ .

2. ب) اذكر عنصرين من مجموعة البينية، ووظيفة كل منهما، يستخدمان في:

أولا: إدارة الأعطال. ثانيا: إدارة التهيئة. ثالثا: إدارة الحسابات.

تابع أسئلة تقويم ذاتي

الجدول المبين أمامك يوضح مسميات عناصر مجموعة البينية ووظيفة كل منهما. قم بتوفيق مسميات العناصر مع ما تؤديه من وظيفة.

رقم	اسم العنصر	وظيفته	رقم الاجابة
1	ifTable	يحتوي معلومات عن الوحدات البينية في محطة التشغيل .	.....
2	ifEntry	عدد صحيح يبين فهرس مصفوفة مجموعات ifEntry .	.....
3	ifXTable	صف من المعلومات عن بينية محددة .	.....
4	ifNumber	يحتوي على سجلات records لعناصر ifEntry .	.....
5	ifIndex	جدول إضافات للعناصر الموجودة في الجدول ifTable .	.....

3. اكتب نبذه مختصرة عمَّا يلي:

أ) عناصر مجموعة البينية الخاصة بالتعامل مع المعلومة، والحرف، والطول الثابت.

ب) عناصر مجموعة البينية الخاصة بالتعامل مع الدوائر الافتراضية Virtual Circuits.

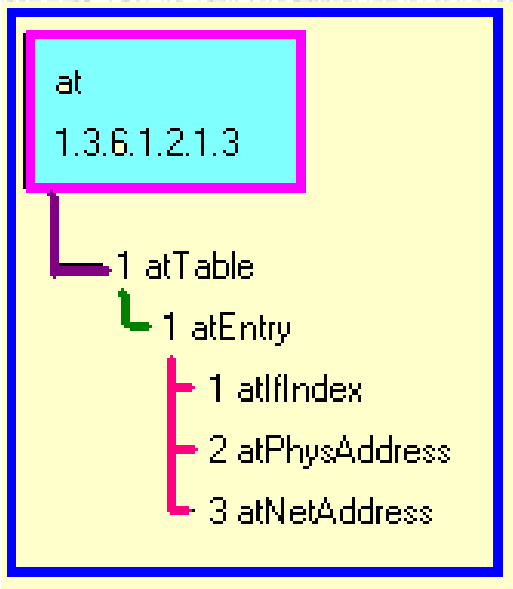
3.5 مجموعة ترجمة العنوان Address Translation Group

تم تعريف الشجرة الفرعية sub-tree لمجموعة ترجمة العنوان في قاعدة المعلومات الإدارية MIB-I. وهي تتكون من جدول واحد يحتوي على عنوان المستوى الشبكي، والعنوان الفيزيقي المكافئ له. يسمح هذا الجدول بإرسال الرسائل عبر اختيار المسار الأحسن إلى أن تصل إلى الهدف النهائي. و يستخدم عادة جهاز الموجه Router لإجراء ترجمة العنوان وتحديد مسار الرسائل كما هو مبين بالمثال الموضح في الشكل4.8.

الشكل4.8 استخدم الموجه لإجراء ترجمة العنوان وتحديد مسار الرسائل.

- **جدول ترجمة العنوان:**

يحتوي جدول ترجمة العنوان على تحويلات العناوين Address Mappings أو مكافئاتها Equivalences . إن العناوين التي نحتاج إدراجها في قائمة جدول ترجمة العنوان، هي العناوين التي نحتاج معرفتها لكي يتم إرسال الرسائل إلى الهدف. ويحتوي جدول ترجمة العنوان؛ كما هو موضح في الشكل4.9؛ على العناصر التالية:



الشكل4.9 قائمة جدول ترجمة العنوان.

أ- الفهرس atIfIndex هو الوحدة البينية المكافئة للمدخل.

ب- العنوان الفيزيقي atPhysicalAddress هو العنوان المباشر الموصل إلى الشبكة الفرعية.

ج- العنوان الشبكي atNetAddress هو العنوان المقابل للعنوان الفيزيقي، الذي نحتاجه لتحديد مسار الرسائل (مثل: IP) .

- **يتم ترجمة العنوان بعدة طرق منها:**

- يتم إدخالها يدوياً ، مثلا أرقام التليفونات.
- يتم حسابها بطريقة آلية.
- يتم اكتشافها آلياً، بواسطة بروتوكولات خاصة، مثل بروتوكول إقرار العنوان Address Resolution Protocol (ARP).

قد يوجد بعض الوحدات البينية التي لا تستخدم جداول الترجمة لتحديد العناوين المكافئة. عندما تكون جميع الوحدات البينية من هذا النوع، ينبغي أن يترك جدول ترجمة العناوين فارغا(أي به Zero Entry).

ولإجراء عملية توافق بين قاعدتي المعلومات MIB-I, MIB-II، فقد تم إدراج مجموعة ترجمة العنوان at الخاصة بقاعدة المعلومات الإدارية MIB-I بدون تعديلات في قاعدة المعلومات الإدارية MIB-II. كما أنه يتم وضع جداول ترجمة عناوين منفصلة داخل قاعدة المعلومات الإدارية لكل بروتوكول شبكي مختلف.

- **من أمثلة جداول ترجمة العناوين:**

- جداول ترجمة عناوين الوسط الإذاعي Broadcast Media، حيث يستخدم بروتوكول ARP، ويتم عمل نسخة مكافئة لجدول ترجمة العناوين تحفظ في مخزن ذاكرة الجهاز ARP Cache.
- جداول ترجمة عناوين شبكات X.25 ، حيث يتم ترجمة العناوين باستخدام نظام X.121 المكافئ.

أسئلة تقويم ذاتي

1. اشرح وظيفة مجموعة ترجمة العنوان، وبيِّن في أي قاعدة معلومات إدارية توجد هذه المجموعة.
2. اذكر خمسة عناصر معلوماتية تستخدم في جدول ترجمة العنوان ووظيفة كل منهما.
3. اذكر مثالين لجداول ترجمة عناوين لبعض الشبكات.

الخلاصة

عزيزي الدارس،

تستخدم قواعد المعلوماتِ الإدارية MIB، القواعدَ النحويةَ Syntax التي اقترحتها الهيئة الدولية للقياسات ISO وتعرف باسم "الرموز النحوية المثالية الأولى": Abstract Syntax Notation One "ASN.1" "أسن.1".

بينت الوحدة أنه يمثل كل جزءٍ من المعلومات في الشجرة قطب بعلامة Labeled Node. يحتوي كل قطب بعلامة على محدد للعنصر ، ووصف نصي مختصر. يتكون محدد العنصر من سلسلة من الأعداد الصحيحة، يفصلها نقط periods، وذلك لتسمية القطب node وترميز الجانب العرضي للشجرة "أسن.1" بدقة.

عددت الوحدة محتويات الجذر القطبي Root Node في الشجرة المستعرضة:

- ccitt (0) والتي يتم إدارتها بواسطة الهيئة الدولية CCITT.
- iso (1) والتي يتم إدارتها بواسطة الهيئة الدولية ISO.
- joint-iso-ccitt(2) والتي يتم إدارتها مشاركة بواسطة الهيئة الدولية CCITT والهيئة الدولية ISO.

بينت الوحدة أنه تحت محدد العنصر internet(1) يوجد أربع شجيرات فرعية :

- الشجرة الفرعية للدليل directory(1):

يتم الاحتفاظ بالشجرة الفرعية للدليل directory(1) للاستخدامات المستقبلية. وهي تحتوي على معلومات عن خدمات الدليل OSI التي تنظمها مجموعة التوصيات القياسية X.500 التي تحدد توزيع صيانة الملفات والأدلة.

- الشجرة الفرعية mgmt(2) :

وتشمل بعض العناصر من خلال كل مصنف category. وهي تستخدم لتخصيص المعلومات الإدارية للبروتوكول DOD.وتنقسم هذه العناصر إلى أحد عشر قسماً.

- الشجرة الفرعية Experimental(3):

إن القصد من البروتوكولات التجريبية Experimental Protocols وتطوير قاعدة إدارة المعلومات هو الدخول إلى الجانب القياسي لهذا الغرض تستخدم الشجرة الفرعية الثالثة وهي(3)experimental.

- الشجرة الفرعية الخاصة private(4) :

تستخدم الشجرة الفرعية الخاصة private(4) لتحديد العناصر الأحادية unilaterally في نظم إدارة الشبكات، حيث إن الجزء الذي يتم الدخول إليه غالبا لهذه الشجرة الفرعية هو أقطاب خاصة {private 1} أو أقطاب مؤسسة تجارية enterprises(1).

عددت الوحدة عناصر قاعدة معلومات "سنمب-ف1":

عنوان الشبكة- وعنوان بروتوكول الربط IP - وعداد موجب يتزايد فقط من 1 إلى 2^32-1 وطوله 32 معلومة- وعداد آخر يسمى Gauge موجباً يتزايد أو ينقص، وقيمته العظمي 2^32-1 - وعداد الزمن TimeTicks- وقواعد نحوية اختيارية يطلق عليها اسم Opaque تستخدم لوصف البيانات النصية.

كذلك عددت الوحدة أقسام قاعدة المعلومات الإدارية لبروتوكول سنمب-ف2:

- قواعد المعلومات الإدارية التي يستخدمها البروتوكول "سنمب-ف2".
- قواعد معلومات إدارية من مدير لآخر، Manage-to-Manager MIB.
- قواعد معلومات إدارية لطرفي الاتصالParty MIB .

عرَّفت الوحدة معدل التغير للعنصر بأنه كمية التغيرات لعنصر محدد بين الزمن t والزمن t+1 ، مقسوماً على الفرق الزمني بين t، t+1.

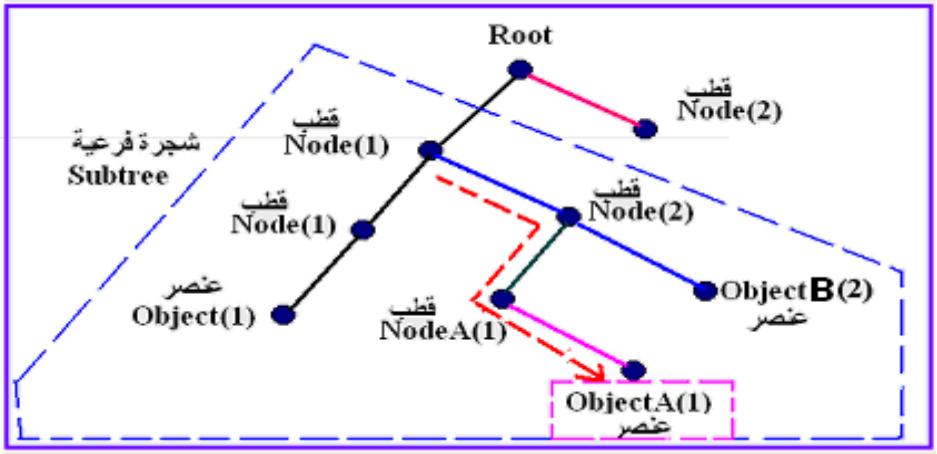
لمحة مسبقة عن الوحدة التالية

عزيزي الدارس،

تتناول الوحدة التالية باقي مجموعات العناصر المكونة لقاعدة المعلومات الإدارية الشهيرة MIB-II، التي تستخدم بوصفها مكوناً أساسياً في بروتوكولات إدارة الشبكات،وتعتبر الوحدة التالية مكملة لهذه الوحدة .

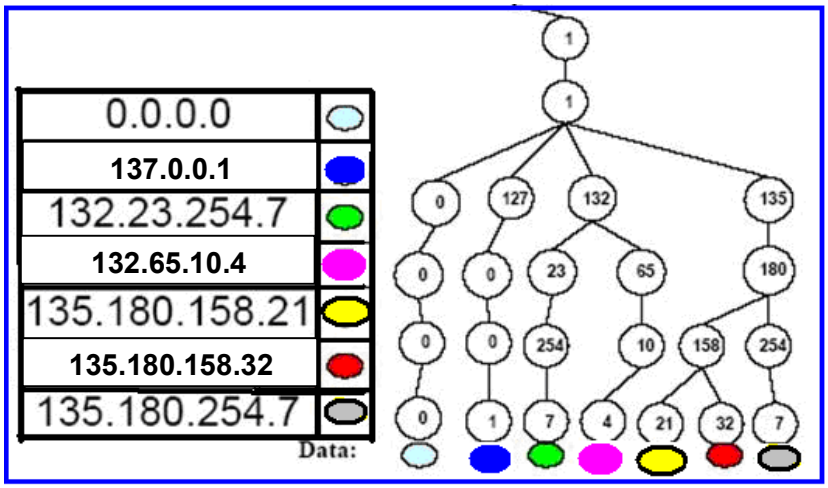
إجابات التدريبات

تدريب (1)



يكون محدد العنصر Object A هو 1.2.1.1

تدريب (2)



تدريب (3)

تستخدم الشجرة الفرعية الخاصة private(4) لتحديد العناصر الأحادية unilaterally في نظم إدارة الشبكات، حيث إن الجزء الذي يتم الدخول إليه غالباً لهذه الشجرة الفرعية هو أقطاب خاصة {private 1} أو أقطاب مؤسسة تجارية enterprises(1). يعرف

قطب المؤسسة enterprise node عن هيئة لها سجلاتها الخاصة، ذات امتداد محدد في قاعدة المعلومات الإدارية. كل فرع من هذه الشجرة الفرعية يتم تخصيصه لمؤسسة تجارية بمفردها. تستطيع المؤسسة التجارية بعد ذلك إنشاء خصائص attributes تتفرع من هذه الشجرة الفرعية لتحديد منتجاتها products.

مثال: عندما تستقبل شركة تسمى "ألمها " شجرة فرعية مخصص لها الرقم 22، فإنه يتم التعبير عن المحدد العنصري لها بالرقم 1.3.6.1.4.22 أو {enterprises 22}. وأن المنتج من شركة "ألمها " ، مثل قنطرة جديدة متعددة المنافذ، ربما يكون لها محدد عنصر رقمه 1.3.6.1.4.22.1.

مسرد المصطلحات

قواعد المعلومات الإدارية

تحتوي قواعد المعلومات الإدارية على المعلومات الحيوية الضرورية من أجل إجراء عمليات الإدارة، والتهيئة، والرصد بواسطة البروتوكول. فهي تعرف بدقة المعلومات المتاحة عن أجهزة الشبكة التي يمكن الوصول إليها Accessible بواسطة بروتوكول إدارة الشبكة.

البناء الشجري Tree Architecture

يستخدم لتنظيم جميع المعلومات المتاحة في قاعدة المعلومات الإدارية.

المعجم Lexigraphical

يستخدم في ترقيم كل العناصر الموجودة في شجرة قواعد إدارة المعلومات.

قطب المؤسسة enterprise node

عبارة عن هيئة لها سجلاتها الخاصة ذات امتداد محدد في قاعدة المعلومات الإدارية.

رقم تسلسل التشغيل Set Serial Number

هو عنصر منفرد Single Object توفره مجموعة التشغيل Set Group ، وهو يسمح لمديرين متعددين أن يرسلوا رسائل تشغيل SNMP Set إلى وكيل منفرد دون مشاكل أو معاناة. ويطلق على هذا العنصر

معدل التغير للعنصر Rate of Object

يعرف معدل التغير بأنه كمية التغيرات لعنصر محدد بين الزمن t والزمن t+1 ، مقسوماً على الفرق الزمني بين t، t+1 . كما في المعادلة التالية :

$$Rate\ of\ Object = \frac{Value\ of\ Object\ (at\ t+1) - Value\ of\ Object\ (at\ t)}{(t+1) - t}$$

مجموعة النظام System Group

تحتوي مجموعة النظام معلومات عن النظام الذي يوجد به محطة التشغيل entity . يفيد الكثير من هذه العناصر في إدارة الأداء وإدارة التهيئة.

عنصر "الهوية" sysObjectID

أحد مجموعة عناصر النظام الخاصة بإدارة الأعطال و يستخدم لبيان هوية عنصر النظام، ويفيد لتصنيف الموردين لأجهزة الشبكة، وكذلك البيانات المعاونة لمعرفة مصنعي الأجهزة.

عنصر "الخدمات" sysServices

أحد مجموعة عناصر النظام الخاصة بإدارة الأعطال وهو يحدد طبقة خدمات الجهاز في النموذج المرجعي OSI ذي الطبقات السبعة. تستخدم المعادلة ***2^(L-1)*** ، حيث ***L*** هو رقم المستوى المحدد لطبقة البروتوكول. وأن القيمة العائدة returned تساوي مجموع القيم لكل طبقة بروتوكول.

عنصر "التشغيل" sysUpTime

أحد مجموعة عناصر النظام الخاصة بإدارة الأعطال وهو يبين طول المدة التي اشتغل فيها النظام.

عنصر"جدول الفحص" ifTestTable

أحد مجموعة عناصر النظام الخاصة بإدارة الأعطال . يحدد جدول عناصر يتكون من صف واحد لكل وحدة بينية Interface في محطة التشغيل. يحدد هذا الجدول العناصر التي تسمح لتطبيق إدارة الشبكة بأن يختبر أنواعاً متعددةً من الأعطال في الوحدة البينية.

عنصر وصف النظام sysDescr

أحد مجموعة عناصر النظام الخاصة بإدارة التهيئة. هو عبارة عن نظام التشغيل المتاح أو البرمجيات المرجعية الخاصة بمحطة التشغيل. تفيد هذه البيانات في كل من إدارة تشغيل الجهاز وفحص الأعطال .

مكان النظام sysLocation

أحد مجموعة عناصر النظام الخاصة بإدارة التهيئة ، وهو يحدد مكان التواجد الفعلي للنظام .

مسؤول النظام sysContact

أحد مجموعة عناصر النظام الخاصة بإدارة التهيئة ، وهو يحدد الشخص الذي يتم الاتصال به عند وقوع مشاكل .

اسم النظام sysName

أحد مجموعة عناصر النظام الخاصة بإدارة التهيئة ، وهو يحدد اسم جهاز الشبكة .

مجموعة البينية Interface Group

توفر مجموعة البينية بيانات عن الوحدات البينية لأجهزة الشبكة. وتفيد في العمليات الإدارية الخاصة بالأعطال، والتهيئة، والأداء ، والحسابات. وتحتوي هذه المجموعة على جدول العناصر، كل صف فيه يمثل بينية واحدة في محطة التشغيل.

جدول عنوان المستقبل ifRcvAddreeTable

يحتوي "جدول عنوان المستقبل" على مدخل لكل عنوان في محطة التشغيل، لاستقبال حزم بيانية packets لوحدة بينية محددة.

الفهرس atIfIndex

هو الوحدة البينية المكافئة للمدخل.

العنوان الفيزيقي atPhysicalAddress

هو العنوان المباشر الموصل إلى الشبكة الفرعية.

العنوان الشبكي atNetAddress

هو العنوان المقابل للعنوان الفيزيقي، الذي نحتاجه لتحديد مسار الرسائل (مثل: IP) .

المصطلح بالإنجليزية	معناه بالعربية
Abstract Syntax Notation One (ASN.1)	الرموز النحوية المثالية الأولى
Address Mapping	تحويلات العناوين
Accessible	يمكن الوصول إليها
Address Translation Group	مجموعة ترجمة العنوان
Address Resolution Protocol(ARP)	بروتوكول إقرار العنوان
Adapter Cards	بطاقات المواءمة
Authentication	التوثيق
Ascending Order	ترتيب تصاعدي
Attributes	خصائص
Bandwidth-on-demand	سعة نطاق عند الطلب
Billing	حساب الفواتير
Bilingual	يعمل باللغتين
Broadcast	إذاعية
Broadcast Media	الوسط الإذاعي
Clusters	تجمعات
Congestion	اختناق
Coexistence	التوافق (التعايش)
Complete Object Identifier	محدد عنصر مكتمل
Contexts	الحوارات (السياق)
Community Strings	حروف مشاركة
Data Concentrator	مركز البيانات
Debugging	فحص الأعطال

Dialing Strings	**حروف الاتصال**
Dial-backup	**طلب خدمة النسخ الاحتياطي**
Dial-on-demand	**الاتصال عند الحاجة**
Disaster-recovery	**العلاج عند الكوارث**
Dynamic Decision	**اتخاذ قرار ديناميكي**
Enterprises	**مؤسسة تجارية**
Equivalences	**مكافئاتها**
Encryption	**تشفير**
Full Duplex	**الاتصال في اتجاهين**
Heavy bursts traffic	**حركة بيانات كثيفة**
Hierarchical	**هرمي**
incrementing once	**زيادة العد لمرة**
Labeled Node	**قطب بعلامة**
Lexigraphical	**معجم**
Leaf Nodes	**أقطاب ورقية**
Listening	**مصغية**
Medium	**وسط اتصال**
Message Translation	**تحويل الرسائل**
Multicast	**مجموعة مذاعة**
Node	**القطب**
Peak Business Period	**الذروة في العمل**
Periods	**نقط**
Physical Configuration	**التهيئة الفيزيقية**
Physical Connector	**وصلة فيزيقية**

Privileges	**امتيازات**
Primary	**الأساسية**
Proxy Agent	**وكيل مساعد**
Products	**منتجات**
Object Identifier (OID)	**محدد العنصر**
Object Resource	**مصادر العناصر**
Output queue	**طابور الخرج**
Unilaterally	**عناصر أحادية**
Unicasts	**مذاعة لفرد واحد**
Utilization	**معدل الاستخدام**
Redundant	**زائدة**
Root Node	**الجذر القطبي**
Robotics	**آليات**
Sites	**مواقع**
Sub Trees	**الشجيرات الفرعية**
Structure Format	**فورمات هيكلية**
Syntax	**القواعد النحوية**
Tree Architecture	**البناء الشجري**
Traversal Tree	**الشجرة المستعرضة**
Virtual Circuits	**الدوائر التصورية (الافتراضية)**

المراجع

1- Understanding SNMP MIBs: by David T. Perkins,
www.amazon.com/Understanding-SNMP-MIBs-David-Perkins/.

2- SNMP Tutorial Part 2: The Management Information Base (MIB)
www.dpstele.com/layers/l2/snmp_l2_tut_part2.php

3- SNMP MIB Resource: www.snmplink.org/snmpresource/mib/

4- Total SNMP: Exploring the Simple Network Management
www.amazon.ca/Total-SNMP-Exploring-Management-Protocol/

5- Reading the MIB Variable Descriptions
www.download-est.oracle.com/docs/

6- A Practical Guide to SNMPv3 and Network Management
www.linuxjournal.com/article/3562

7- Formal specification of SNMP MIB's
www. ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=770698

8- A Closer Look at MIB-II (Essential SNMP)
www.unix.org.ua/orelly/networking_2ndEd/snmp/ch02_05.htm

9- Network Management: A Practical Perspective ,by Allan Leinwand, Karen Fang-Conroy. Info at Addison-Wesley, 1997.

10 - RFCs: Requests for Comments, http://ietf.org/rfc.html

11- IETF: The Internet Engineering Task Force, http://www.ietf.cnri.reston.va.us/

12- mibDepot is an online SNMP MIB reference site,
http //www.mibdepot.com/index.shtml

الوحدة الخامسة
قواعد معلومات إدارة الشبكات
(الجزء الثاني)

محتويات الوحدة

المقدمة

تمهيد

عزيزي الدارس،

نرحب بك إلى الوحدة الخامسة من مقرر " استخدام وإدارة الشبكات2"، و ندرس في هذه الوحدة باقي مجموعات العناصر المكونة لقاعدة المعلومات الإدارية الشهيرة MIB-II، التي تستخدم بوصفها مكوناً أساسياً في بروتوكولات إدارة الشبكات. وتعتبر هذه الوحدة مكملة للوحدة الرابعة التي تم تناولها سابقا.

القسم الأول يتناول مجموعة بروتوكول الإنترنت IP Group حيث يشرح القسم العناصر المعلوماتية التي تستخدم في إدارة الأعطال، والتهيئة، والأداء ، والحسابات.

أما القسم الثاني فيأتي متناولاً مجموعة بروتوكول رسائل تحكم الإنترنت ICMP، ويبين القسم قائمة عناصر ICMP التي تستخدم في إدارة الأداء، ويقدم تلخيصاً لوظائف العديد من هذه العناصر. القسم الثالث يتناول مجموعة بروتوكول النقل TCP وهي مجموعة عناصرTCP الخاصة بإدارة التهيئة، ومجموعة عناصرTCP الخاصة بإدارة الأداء، ومجموعة عناصرTCP الخاصة بإدارة الحسابات، ومجموعة عناصرTCP الخاصة بإدارة الأمن . القسم الرابع يتناول عناصر مجموعة بروتوكول UDP وهو بروتوكول لا يتيح رسائل شكر تؤكد وصول رسائل داتاجرام إلى الهدف، لهذا السبب يطلق عليه عديم الاتصالية connectionless، وعديم الاعتمادية unreliable،. لذلك تحتوي مجموعة UDP على عدد محدود من العناصر. يتناول القسم الخامس مجموعة بروتوكول EGP و مجموعة بروتوكول CMOT، كذلك يتناول القسم عيوب البروتوكول EGP ومعالجتها بواسطة BGP ويتضمن القسم كذلك مجموعة عناصر الإرسال Transmission Group، أما القسم السادس فيتناول عناصر مجموعة بروتوكول SNMP .

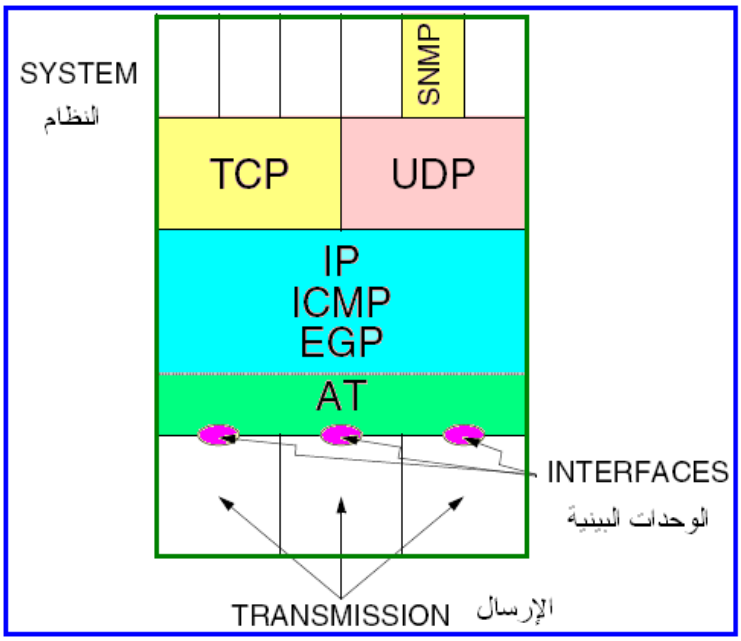
أهداف الوحدة

عزيزي الدارس، بعد فراغك من دراسة هذه الوحدة ينبغي أن تكون قادراً على أن:

- **تشرح** مجموعة بروتوكول الإنترنيت IP وبناءها الهيكلي.
- **تشرح** مع الأمثلة تطبيقات عناصر IP في إدارة الأعطال،التهيئة، الأداء، الحسابات.
- **تصف** مجموعة عناصر بروتوكول رسائل تحكم الانترنيت ICMP، وتطبيقاتها.
- **تطبق** مجموعة عناصر بروتوكول النقل TCP وبناءها الهيكلي.
- **تصف** تطبيقات عناصرTCP في إدارة التهيئة، الأداء، الحسابات، الأمن مع تقديم أمثلة لها.
- **تشرح** مجموعة بروتوكول UDP، وبناءها الهيكلي.
- **تشرح** مع الأمثلة تطبيقات عناصر UDP في إدارة الأداء، الحسابات، التهيئة، الأمن، مع أمثلة.
- **تكتب** نبذة مختصرة عن مجموعة بروتوكول EGP، وعيوبه ومعالجتها بواسطة BGP .
- **تعطي** نبذة مختصرة عن مجموعة بروتوكول CMOT.
- **تصف** بعض مجموعة عناصر الإرسال Transmission-Group.
- **تستخدم** مجموعة بروتوكول SNMP وتطبيقاتها في إدارة الأعطال، الأداء،الحسابات، الأمن، التهيئة وتقديم أمثلة لها.
- **تبين** كيفية تطوير قاعدة المعلومات الإدارية MIB-II وعناصرها لتحسين إدارة الشبكات.

تمهيد

يوضح الشكل 5.1 تسكين بروتوكولات هذه المجموعات، بقاعدة المعلومات الإدارية MIB-II في المركم البروتوكولي Protocol Stack للنموذج المرجعي لنظام TCP/IP.

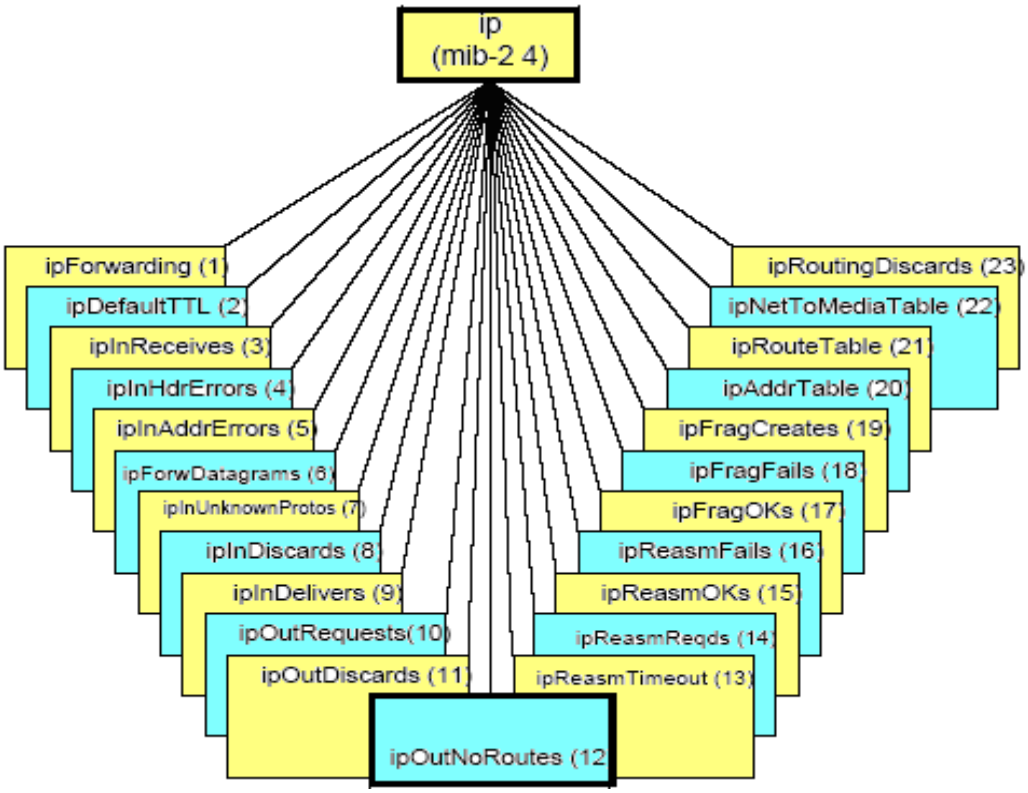


الشكل 5.1 تسكين بروتوكولات مجموعات MIB-II، في المركم البروتوكولي لنموذج TCP/IP.

وسوف نتناول بالتفصيل – مع بعض الإيجاز – شرح تطبيقات هذه العناصر في إدارة الشبكة شاملاً ذلك إدارة التهيئة، والأداء، والحسابات، والأعطال، والأمن.

1 . مجموعة بروتوكول الإنترنيت IP Group

يستخدم بروتوكول الإنترنيت IP نمطاً غير اتصالي Connectionless لإرسال رسائل داتاجرام. يوضح الشكل5.2 مسميات مجموعة عناصر بروتوكول IP. توفر مجموعة عناصر بروتوكول IP معلومات عنIP في محطة التشغيل.



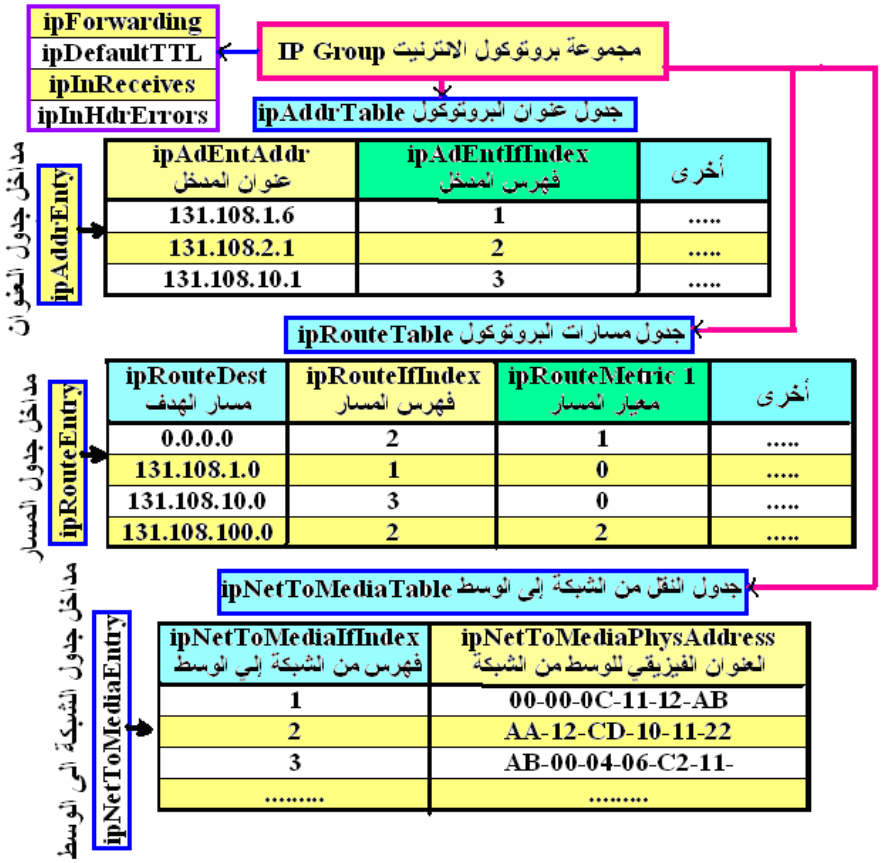
الشكل5.2 مجموعة عناصر بروتوكول IP.

ويوضح الشكل5.3 بناءً هيكلياً مبسطاً لمجموعة عناصر معلومات بروتوكول IP. ويتكون البناء الهيكلي من أربعة أقسام معلوماتية هي:

- عناصر تعطي معلومات عن الأخطاء وأنواع حزم بيانات IP.
- جدول معلومات عن عناوين IP لمحطة التشغيل.

- جدول مسارات IP لمحطة التشغيل.
- تحويلات Mapping عناوين IP إلى عناوين البروتوكولات الأخرى، وهذه الخصائص تسبق مرحلة ترجمة العنوان.

وسنشرح في الفقرات التالية العناصر المعلوماتية التي تستخدم في إدارة الأعطال، والتهيئة، والأداء، والحسابات.



الشكل5.3 بناء هيكلي مبسط لمجموعة عناصر معلومات بروتوكول IP.

أسئلة تقويم ذاتي

اختر الإجابة الصحيحة

تحتوي قاعدة المعلومات الإدارية MIB-II على مجموعات عديدة من العناصر المعلوماتية التي تستخدم في بروتوكولات المستوى TCP/IP ، تشمل هذه المجموعات على ما يلي:

أ) CMOT, EGB . ب) ARP, BGP.

ج) ICMP, IP . د) TCP, UDP.

هـ) جميع مجموعات أ، ج، د .

توفر مجموعة عناصر بروتوكول IP معلومات عن تشغيل محطة الشبكة في النمط غير الاتصالي، وتنقسم هذه المعلومات إلى أربعة أقسام هي (أكمل الإجابات):

أ) عناصر تعطي معلومات عن ..... .

ب) جدول معلومات يبين ..... .

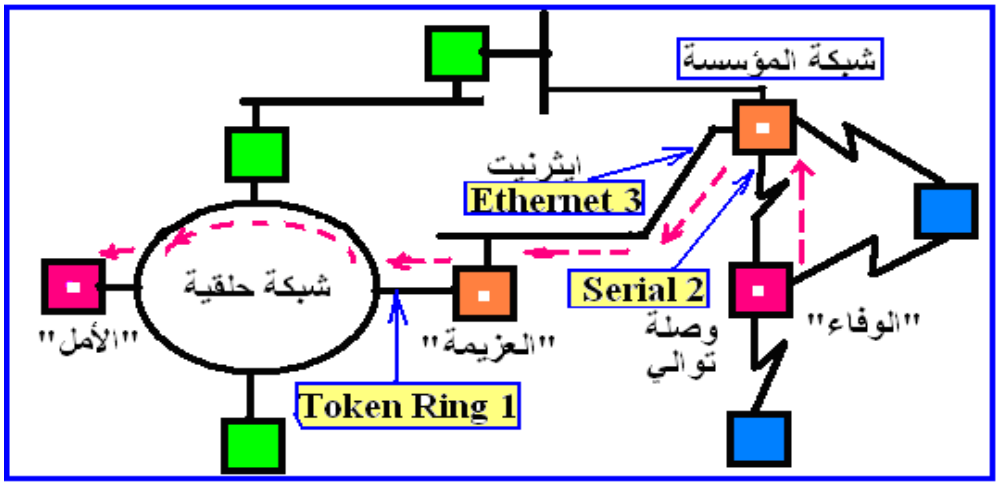
ج) جدول مسارات يحدد ..... .

د) تحويلات لعناوين من ..... إلى ..... .

1.1 عناصر مجموعة IP المستخدمة في إدارة الأعطال

إن جميع العناصر الموجودة في جدول تحديد المسارات ***ipRoutTable***، المذكورة في الشكل5.3 تكون مفيدة لإدارة الأعطال، مثل تتبع مشاكل المسار، والأجهزة التي تعلن عن معلومات مسارات غير صحيحة. يمكن أن يستخدم تطبيق إدارة الأعطال هذه العناصر للاستفسار عن جدول تحديد المسارات IP لجهاز، واكتشاف المسارات خلال الشبكة. كما أن عناصر نوع المسار ***ipRouteType, ipRouteProto*** يمكن أن تحدد لنا كيفية معرفة معلومات المسار.

مثال تطبيقي: نفترض في الشبكة الموضحة في الشكل5.4 ، أن مركز الاتصال "الوفاء" لا يستطيع الاتصال بمركز الاتصال "الأمل". ونريد تشخيص أعطال هذه المشكلة.



الشكل5.4 ضبط إعداد الشبكة بين مركزي اتصال الوفاء والأمل.

يمكنا أولا: فحص خريطة الشبكة في نظام الإدارة لنتأكد أن جميع أجهزة الشبكة تعمل وهي في حالة تشغيل. لأنه يوجد عديد من المسارات الممكنة من مركز الاتصال "الوفاء" إلى مركز الاتصال "الأمل". ونريد أن نجد أياً من هذه المسارات يستخدم.

ثانيا: يمكن أن يستخدم تطبيق إدارة الأعطال العناصر ***ipRouteDest, ipRouteIfIndex, ipRouteNextHop*** للاستفسار من مركز الاتصال "الوفاء" ،

والسؤال عن خطوة الاتصال التالية Next Hop إلى مركز الاتصال "الأمل" ، والتي يمكن أن تكون حاسب المؤسسة Enterprise، من خلال الوحدة البينية Serial2. يستخدم العنصر ***ipRouteDest*** لإيجاد مدخل المسار الصحيح للوصول إلى مركز الاتصال "الأمل" ، ويعطي العنصر ***ipRouteNextHop*** عنوان النقلة التالية Next Hop، ويعطي العنصر ***ipRouteIfIndex*** بينية الإرسال الخارج Outbound Interface من محطة التشغيل. وأن القيمة الراجعة بواسطة العنصر ***ipRouteIfIndex*** تكون مرتبطة بالعنصر ***ifIndex*** من مجموعة البينية. يمكن بذلك أن نجد الحروف "Serial2" في العنصر ***ifDescr***.

ثالثا: ينبغي في الخطوة التالية أن نسأل مركز اتصال المؤسسة Enterprise عن نفس المعلومات. نعرف أن مركز اتصال المؤسسة Enterprise يوصل إلى مركز الاتصال "الأمل"، بواسطة إرسال بيانات خلال الجهاز "العزيمة" بواسطة البينية Ethernet3. بالتالي، نكتشف أن "العزيمة" يرسل بيانات مباشرة إلى مركز الاتصال "الأمل"، بواسطة البينية Token-Ring1 . بإجراء هذه العملية، سوف نعرف أن مركز الاتصال "الوفاء" ليس له مسار صحيح إلى "الأمل".

رابعا: إن بيانات مجموعة IP الأخرى، يمكن أن تساعدنا في حل هذه المشكلة، وهذه العناصر موضحة في قائمة الجدول ***ipNetToMediaTable***. إن هذه العناصر تخبرنا عن تحويل عناوين IP إلى عناوين بروتوكول آخر. أحد الأمثلة الشائعة، هو جدول بروتوكول إقرار العنوان ARP الذي يحول عناوين IP إلى عناوين MAC. بالرجوع إلى الشكل5.4 ، وكجزء من حل المشكلة، يقوم تطبيق إدارة الأعطال بالاستفسار من مركز الاتصال "العزيمة" عن العناوين التالية:

ipNetToMediaPhysAddress, ipNetToMediaIfIndex, ipNetToMediaNetAddress

في كل صف من الجدول ***ipNetToMediaTable***. فنجد أن صفاً واحداً في الجدول لا يحتوي على مدخل إلى مركز الاتصال "الأمل"، يوجد في البينية Token-Ring1. بذلك نعرف أن مركز الاتصال "العزيمة" قام بالاتصال مع مركز الاتصال "الأمل".

خامسا: يمكنا بعد ذلك، نداء مدير النظام الخاص بمركز الاتصال "الوفاء" لإيجاد ما إذا كان أي عتاد أو برنامج في النظام قد تم تغييره حديثا. فنعرف أن الوحدة البينية لحلقة Token-Ring في مركز الاتصال "الوفاء" قد تم تغييرها صباحا. فنستنتج أن جدول ***ipNetToMediaTable*** (أو الذاكرة ARP Cache في هذه الحالة) تكون قديمة out-of-date في مركز الاتصال "العزيمة". وأن تحويل عنوان IP إلى عنوان Token Ring MAC يكون لبطاقة الوحدة البينية القديمة، والتي لم تعد موجودة.

سادسا: يمكننا الآن، أن نقرر تصليح المشكلة في مركز الاتصال "العزيمة" بواسطة مسح الذاكرة ARP Cache. بعد ذلك، في المرة القادمة، فإن مركز الاتصال "العزيمة" يحتاج الاتصال مع "الوفاء" ، ويقوم "العزيمة" بإرسال ARP ويكتشف الترجمة الصحيحة بين عنوان IP الخاص بمركز الاتصال "الوفاء"، والعنوان الجديد الخاص بالوحدة البينية Token Ring MAC.

2.1 عناصر مجموعة IP المستخدمة في إدارة التهيئة

يبين الجدول5.1 قائمة عناصر مجموعة IP الخاصة بتطبيقات إدارة التهيئة، ووظيفة كل منها. يوجد بعض أجهزة الشبكة يتم تهيئتها لإرسال رسائل داتاجرام ، مثل الموجهات. يقوم تطبيق إدارة التهيئة بالاستفسار من الجهاز للحصول على عنصر المرسال ***ipForwarding*** يستطيع إخبارنا عن تشغيل Functionality محطة التشغيل Entity.

جدول 5.1

عناصر مجموعة IP المستخدمة في إدارة التهيئة

نوع العنصر	المعلومات
ipForwarding	تهيئة الجهاز لإرسال IP
ipAddrTable	عناوين IP في الجهاز
ipRouteTable	جدول مسارات IP

<u>على سبيل المثال:</u> عندما يستفسر التطبيق من جهاز عن عنصر خدمات النظام ***sysServices*** ويجد أن الجهاز يخدم المستوى الشبكي (المستوى الثالث). بعد ذلك، ربما نريد أن نعرف ما إذا كان هذا الجهاز يمرر رسائل داتاجرام IP بواسطة المرسال ***ipForwarding***. – في هذه الحالة – فإن موجه Apple-talk يمكن أن يرجع القيمة ***sysServices*** مبينا أنه يقوم بخدمة المستوى الشبكي، لكن ربما يظهر المرسال ***ipForwarding*** أن الجهاز لا يحدد مسار IP.

عندما نعرف عنوان الشبكة، وقناع الشبكة الفرعية sub-net mask ، والعنوان الإذاعي Broadcast Address، المخصص لجهاز، يكون ذلك ذا قيمة كبيرة لإدارة التهيئة. إن الجدول ***ipAddrTable*** يعطينا معلومات عن عناوين IP الحالية في محطة التشغيل. يسمى كل صف في الجدول ***ipAddrTable*** بالمدخل ***ipAdrEntry***. داخل كل مدخل، تخبرنا العناصر ***ipAdEntIfIndex, ipAdEntAddr*** عن عناوين IP لربط علاقة جدول الدخول ***ipAddrTable*** مع مدخل جدول مجموعة البينية ***ifTable***.

يعطي العنصر ***ipAdEntNetMask*** قناع عنوان الشبكة الفرعية، ويخبرنا العنصر ***ipAdEntBcastAddr*** عن العنوان الإذاعي. نلاحظ على الرغم من ذلك، أن قاعدة المعلومات الإدارية، تحدد هذه العناصر في نمط القراءة فقط. لذلك لأغراض إدارة

التهيئة فإن التطبيق، أو مهندس الشبكة يستطيع الاستفسار عن هذه المعلومات، ولكن لا يستطيع تغييرها.

يعرِّف الجدول ***ipRouteTable*** عدداً من العناصر في نمط القراءة والكتابة. لأغراض إدارة التهيئة، يستطيع التطبيق إدخال مسارات جديدة بواسطة العنصر ***ipRouteDest*** ، وأن يغير نوع المسار باستخدام العنصر ***ipRouteType*** . بالإضافة إلى ذلك، أنه من الممكن تهيئة مقاييس metrics تحديد المسار بواسطة ضبط العناصر التالية:

ipRouteMetric3, ipRouteMetric4, ipRouteMetric1, ipRouteMetric2, ipRouteMetric5.

يسمح ضبط هذه العناصر لمهندس الشبكة أن يتحكم في مسارات حزم بيانات IP التي تمر وتعبر من خلال شبكة البيانات. ربما نرغب في التحكم في هذه المسارات لأسباب تقنية (مثل التحويل عن مسار يعاني طريقه من الأخطاء)، أو أسباب نظامية Policy-Based-Reasons (مثل: تحديد مسار في الشبكة تكون تكلفته أقل من المسار المستخدم).

أسئلة تقويم ذاتي

اشرح بمثالٍ تطبيقي يوضح طريقة استخدام عناصر مجموعة IP في الآتي:

أ) إدارة الأعطال. ب) إدارة التهيئة .

أكمل الجدول التالي والذي يبين قائمة عناصر مجموعة IP الخاصة بتطبيقات إدارة التهيئة، ووظيفة كل منها.

نوع العنصر	المعلومات
ipForwarding	.....
ipAddrTable	.....
ipRouteTable	.....

3.1 عناصر مجموعة IP المستخدمة في إدارة الأداء

يبين الجدول5.2 قائمة عناصر مجموعة IP الخاصة بتطبيقات إدارة الأداء. بسبب العدد الضخم لهذه العناصر، فإننا سوف نشرح بعض العناصر الهامة وتطبيقاتها.

الجدول5.2

عناصر مجموعة IP المستخدمة في إدارة الأداء و وظائفها

الرقم	العنصر	المعلومات
1	ipInReceives	معدل دخل رسائل داتاجرام
2	ipInHdrErrors	معدل دخل أخطاء المقدمة Header
3	ipInAddrErrors	معدل دخل أخطاء العنوان
4	ipForwDatagrams	معدل دخل داتاجرام الموجهة
5	ipInUnknownProtos	معدل دخل داتاجرام لبروتوكول غير معروف
6	ipInDiscards	معدل دخل داتاجرام المهملة
7	ipInDelivers	معدل دخل رسائل داتاجرام
8	ipOutRequests	معدل خرج رسائل داتاجرام
9	ipOutDiscards	معدل خرج داتاجرام المهملة
10	ipOutNoRoutes	معدل الإهمال بسبب نقص معلومات المسار
11	ipRoutingDiscards	معدل مدخلات تحديد المسار المهملة
12	ipReasmReqds	معدل داتاجرام المستقبلة وتحتاج إعادة تجميع
13	ipReasmOKs	معدل داتاجرام المعاد تجميعها بنجاح
14	ipReasmFails	معدل تجزئة إعادة التجميع الفاشلة
15	ipFragOKs	معدل التجزئة الناجح
16	ipFragFails	معدل التجزئة الفاشل
17	ipFragCreates	معدل التجزئة المنشأ

- **<u>التطبيق الأول : قياس حركة مرور الرسائل Traffic</u>**

يستطيع تطبيق إدارة الأداء استخدام عناصر مجموعة IP لقياس النسبة المئوية لحركة مرور الرسائل الداخلة والخارجة من محطة التشغيل. على سبيل المثال، إن إجمالي عدد حزم البيانات المستقبلة بواسطة محطة التشغيل، تكون متاحة بواسطة حساب مجموع العنصرين ***ifInUcastPkts, ifInNUcastPkts*** لكل وحدة بينية. بعد ذلك نقسم ***ipInReceives*** على هذا المجموع، وبذلك يتم إيجاد النسبة المئوية لرسائل داتاجرام IP المستقبلة.

يمكن إجراء حسابات مماثلة باستخدام العنصر ***ipOutRequests*** لرسائل داتاجرام المرسلة بواسطة محطة التشغيل. إن العنصر ***ipOutRequests*** يعد فقط عدد رسائل داتاجرام المرسلة بواسطة محطة التشغيل، وليس رسائل داتاجرام الموجهة forwarded. بالنظر إلى معدل التغير في العناصر "***ipOutRequests*** ***ipInReceives*** " يمكنا إيجاد المعدل الذي عنده تقوم محطة التشغيل باستقبال، و إرسال رسائل داتاجرام IP.

- **<u>التطبيق الثاني: حساب عدد الرسائل المهملة Discarded</u>**

تقوم محطة التشغيل بعدّ counts عدد المرات التي تُهْمَلُ فيها رسائل داتاجرام. يقوم العنصر ***ipInDiscards*** بعدّ الرسائل التي تهمل عند المدخل. بينما العنصر ***ipOutDiscards*** يقوم بعدّ الرسائل التي تهمل عند المخرج. يحدث إهمال رسائل داتاجرام عادة بسبب نقص في مصادر النظام System Resources ، أو أسباب أخرى، لا تسمح بإجراء المعالجة المناسبة لرسائل داتاجرام.

- **<u>التطبيق الثالث: حساب معدل الأخطاء Errors</u>**

يمكن أن تحدث الأخطاء بسبب أن رسائل داتاجرام تأتي إلى محطة التشغيل وتكون مقدمة IP غير صحيحة Invalid IP Header ، ويتم عدّها بواسطة محطة التشغيل في العنصر ***ipAddrErrors*** . إن النسبة المئوية المرتفعة لحزم بيانات IP التي ينتج عنها أخطاء ربما تؤدي إلي مشكلة في أداء التطبيق الذي يستخدم بروتوكول IP لإجراء عملية التوصيل delivery. <u>يستطيع التطبيق حساب النسبة المئوية للأخطاء من رسائل داتاجرام IP كما يلي:</u>

النسبة المئوية لأخطاء IP عند الدخل =   ***(ipInDiscards + ipInHdrErrors + ipInAddrErrors) / ipInReceivers***
النسبة المئوية لأخطاء IP عند الخرج =   ***(ipOutDiscards + ipOutHdrErrors + ipOutAddrErrors) / ipOutRequests***

نستطيع أيضا، استخدام عناصر مجموعة البينية لمقارنة إجمالي عدد حزم البيانات عند الخرج لجميع الوحدات البينية، وعلاقته بمعدل أخطاء الخرج IP . تبين لنا هذه المقارنة ما إذا كانت النسبة المئوية الكبيرة لحزم بيانات الخرج من محطة التشغيل ، قد نتج عنها أخطاء خرج IP.

- **<u>التطبيق الرابع: تأثير التجزئة IP Fragmentation على الأداء</u>**

يمكن لبعض عناصر مجموعة IP حساب الأخطاء التي تنتج من تجزئة IP وذلك بحساب النسبة المئوية ومعدلات رسائل داتاجرام المجزئة ، والأخطاء المصاحبة لها ، نستطيع إثبات ما يلي:

أ- أنه من المفيد معرفة أن الجهاز يقوم بإرسال أو استقبال نسبة مئوية مرتفعة من رسائل داتاجرام المجزأة.

ب- أن النسبة المئوية المرتفعة لرسائل داتاجرام IP التي تسبب أخطاء التجزئة يمكن أن يكون لها انعكاس على أداء التطبيق الذي يستخدم بروتوكول IP عند إجراء عملية النقل delivery في الشبكة.

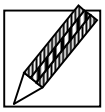
يمكن أن تحدث التجزئة عندما تعبر حزم بيانات IP الشبكة التقنية التي تدعم فقط أطوال حزم بيانات أصغر من الوحدة البينية للنظام. يمكن أن يحدث ذلك عندما يتم ضبط الحاسوب المضيف للوحدة البينية من نوع FDDI كي ترسل أطراً Frames عند سرعة 4500 bytes (طول حزمة الإطار المسموح في حلقة FDDI). وأن الإطار يحتاج مسارا من خلال الاثيرنيت Ethernet (أقصى طول إطار يكون 1500Bytes) كي يصل إلى الهدف.

على الرغم من أن التجزئة هي جزء معياري standard في البروتوكول IP فإن أداء التجزئة غالبا يؤدي إلى أداء إرسال أبطأ في الأجهزة الموجودة وسط الشبكة، مثل أجهزة المفاتيح والموجهات.

- **<u>التطبيق الخامس : تأثير المهملات على مصادر الشبكة</u>**

يمكن أن يعرفنا العنصر ***ipRoutingDiscards*** ما إذا كانت محطة التشغيل تقوم بإهمال مداخل تحديد مسار IP صالح valid أم لا. بسبب نقص المصادر Lack of Resources ، فإن معدل مداخل تحديد مسار IP المهملة، يمكن أن تساعدنا في إيجاد ما إذا كانت محطة التشغيل، لا يوجد بها مصادر كافية لتوفير الأداء اللازم للشبكة.

تدريب (1)



تقوم محطة التشغيل بتخزين مؤقت لعدد ضخم من رسائل داتاجرام ، وضح ثم اشرح كيف يؤثر هذا على مصادر الشبكة.

- **<u>التطبيق السادس: تحديد عدد المسارات غير الصحيحة</u>**

يقوم العنصر ***ipOutNoRoutes*** بعدِّ عدد المرات التي لا يوجد فيها مسار صحيحٌ لرسائل داتاجرام في محطة التشغيل. عندما يزداد معدل هذا العنصر، فإن محطة التشغيل تكون غير قادرة على توجيه رسائل داتاجرام إلى الهدف. ويزداد هذا العنصر لرسائل داتاجرام المرسلة والموجهة بواسطة محطة التشغيل.

<u>على سبيل المثال</u>: عندما تقوم محطة التشغيل بتوصيل رسائل داتاجرام إلى الهدف، وحدث خطأ بعد ذلك، فإن هذا يسبب فقدان محطة التشغيل لمسار الهدف، وأن هذا العنصر يحتمل أن يزداد إلى أن يدرك نظام المصدر أن الهدف لا يمكن الوصول إليه من خلال هذه المحطة.

- **<u>التطبيق السابع: تأثير البروتوكول غير المعروف على مصادر الشبكة</u>**

عندما تضطر محطة التشغيل إلى معالجة عدد ضخم من رسائل داتاجرام، التي لا يوجد لها دعم محلي لبروتوكول الطبقة العليا Upper-Layer Protocol، الذي يتم قياسه بواسطة العنصر ***ipUnknownProtos*** ؛ فإن هذا ربما يسبب الاهتمام بالأداء. في هذه الحالة، فإن محطة التشغيل التي تستقبل رسالة داتاجرام تقوم بفحصها من الأخطاء،

وتحدد إن كان الهدف يكون لعنوان IP محلي. عندما ترغب محطة التشغيل– الآن– إهمال رسالة داتاجرام بسبب أن هدفها يكون الوصول إلى بروتوكول المستوى الأعلى غير المعروف؛ فإن هذا يسبب ضياع المصادر . عندما يحدث ذلك بمعدلات مرتفعة، يمكن أن نتتبعه بواسطة فحص العنصر ***ipUnknownProtos*** مع مرور الوقت، وربما يسبب مشكلة أداء.

<u>على سبيل المثال</u>: نفترض أن شبكة بيانات بها مجموعة من خادمات إخبارية news servers ، التي تعرض الأخبار على الموظفين في المؤسسة. يمكن للموظف أن يوصل حاسوبه الشخصي PC كتطبيق عملي إلى الخادمات الإخبارية. بعد ذلك يمكن أن يقرأ هذه الأخبار والبحث في محتوياتها وتخزين المقالات محليا. يستخدم التطبيق المكتوب بواسطة المؤسسة نظام الدخل / الخرج الأساسي للشبكة (NetBIOS)، فوق بروتوكول IP لحمل حزم البيانات بين خادمات الأخبار، والعملاء. إن بروتوكول المستوى الأعلى هو الذي يضمن أن رسائل IP داتاجرام تصل باعتمادية. يتم تنصيب NetBIOS فقط على الحواسيب الشخصية للعملاء وخادمات الأخبار.

عندما يحاول موظف توصيل تطبيق الحاسوب الشخصي إلى خادم مختلف (لا يقوم بتشغيل NetBIOS فوق IP)، فإن ذلك لا يدعم NetBIOS ، فيزداد قيمة العنصر ***ipUnknownProtos*** . عندما يحاول عدد من الحواسيب الشخصية تكرار محاولة التوصيل بالخادم الذي لا يدعم NetBIOS ، فإن ذلك قد يسبب مشكلة في الأداء.

- **<u>التطبيق الثامن: حساب معدل التراسل</u>**

يبين العنصر ***ipFolwDatagrams*** معدل التراسل Forwarding Rate للجهاز بالنسبة إلى رسائل IP داتاجرام. عندما تتم عملية إجراء التصويت مرتين للنظام، تستغرق المرة الواحدة زمن "X" ثانية، والمرة التالية تستغرق زمن "Y" ثانية، فإن المعادلة التالية تبين معدل تراسل حزم بيانات IP في الثانية.

معدل الإرسال IP Forwarding Rate =
(ipForwDatagrams at "Y" − ipForwDatagrams at "X") / (Y − X)
معدل الاستقبال IP Input Rate =
(ipInReceives at "Y" − ipInReceives at "X") / (Y − X)

عندما يتم رصد هذه المعدلات بواسطة تطبيق المرصد application monitor، نستطيع تحديد ما إذا كان النظام يقوم بتوصيل forwarding حزم بيانات IP بسرعة كافية تحقق متطلبات الشبكة.

يقوم العنصر ***ipInReceives*** بإعطاء إجمالي عدد حزم بيانات IP المستقبلة بواسطة محطة التشغيل. عندما تقوم محطة التشغيل بعد ذلك بتوصيل هذه الحزم، فإن معدل الإرسال ينبغي أن يساوي معدل الدخل IP input . لجعل هذه الحسابات أكثر دقة، نقوم بطرح معدل أخطاء الدخل، وحزم البيانات IP التي تم إرسالها إلى النظام. إن إجراء هذا العمل، يعني أننا نقوم بمقارنة بين معدل الإرسال فقط، مع معدل حزم البيانات IP المستقبلة التي ليس بها أخطاء، أو ليست لهذه المحطة.

4.1 عناصر مجموعة IP المستخدمة في إدارة الحسابات

يحدد العنصران ***ipOutRequests***، ***ipInDelivers*** إجمالي عدد حزم البيانات IP التي ترسلها وتستقبلها محطة التشغيل على الترتيب. تكون هذه المعلومات مهمة في تحديد فواتير الدفع Billing لمستخدمي الشبكة. للأغراض الحسابية، فإن استخدام العنصر ***ipInDelivers*** يعطينا عدد حزم بيانات IP التي تم تسليمها إلى بروتوكولات الطبقة العليا بدون خطأ.

أسئلة تقويم ذاتي

بالاستعانة بجدول مجموعة عناصر بروتوكول IP المستخدمة في إدارة الأداء، اشرح كيف تحسب الآتي:

أ) عدد الرسائل المهملة. ب) معدل الأخطاء. ج) عدد المسارات الغير صحيحة. د) معدل التراسل.

يبين الجدول التالي بعض عناصر مجموعة IP الخاصة بتطبيقات إدارة الأداء قم بتوفيق الإجابات الصحيحة.

رقم العنصر	العنصر	المعلومات	رقم الإجابة
1	ipInReceives	معدل دخل أخطاء العنوان	.....
2	ipInHdrErrors	معدل خرج رسائل داتاجرام	.....
3	ipInAddrErrors	معدل دخل رسائل داتاجرام	.....
4	ipForwDatagrams	معدل خرج داتاجرام المهملة	.....
5	ipInUnknownProtos	معدل الإهمال بسبب نقص معلومات المسار	.....
6	ipInDiscards	معدل دخل داتاجرام المهملة	.....
7	ipRoutingDiscards	معدل مدخلات تحديد المسار المهملة	.....
8	ipOutRequests	معدل دخل أخطاء المقدمة Header	.....
9	ipOutDiscards	معدل دخل داتاجرام الموجهة	.....
10	ipOutNoRoutes	معدل دخل داتاجدرام لبروتوكول غير معروف	.....

2.مجموعة عناصر بروتوكول رسائل تحكم الإنترنيت ICMP

إن بروتوكول رسائل تحكم الإنترنيت ICMP هو المسؤول عن حمل تقارير الأخطاء ورسائل التحكم إلى أجهزة IP. وتحتوي قاعدة المعلومات الإدارية في محطة التشغيل على العناصر التي تعطينا معلومات عن مجموعة عناصر ICMP . يبين الجدول5.3 قائمة عناصر ICMP التي تستخدم في إدارة الأداء. ولكثرة عدد هذه العناصر فإننا سوف نقوم بتلخيص وظائف العديد منها تباعا.

الجدول5.3

عناصر مجموعة ICMP المستخدمة في إدارة الأداء ووظائفها

الرقم	العنصر	المعلومات
1	icmpInMsga	معدل دخل الرسائل
2	icmpInErrors	معدل دخل الأخطاء
3	icmpInDestUnreachs	معدل دخل رسائل لم تصل للهدف
4	icmpInTimeExcds	معدل دخل رسائل الزائد وقتها
5	icmpInParmProbs	معدل دخل رسائل بها مشكلة معامل
6	icmpInSrcQuenchs	معدل دخل رسائل إخماد مصدر
7	icmpInRedirects	معدل دخل رسائل معاد توجيهها
8	icmpInEchos	معدل دخل رسائل الصدى
9	icmpInEchoReps	معدل دخل رسائل استجابة صدى
10	icmpInTimestamps	معدل دخل رسائل أختام زمنية
11	icmpInTimestampReps	معدل دخل رسائل استجابة أختام زمنية
12	icmpInAddrMasks	معدل دخل رسائل طلب قناع عنوان
13	icmpInAddrMaskReps	معدل دخل رسائل استجابة طلب قناع عنوان
14	icmpOutMsgs	معدل خرج الرسائل
15	icmpOutErrors	معدل خرج رسائل الأخطاء
16	icmpOutDestUnreachs	معدل خرج رسائل لم تصل للهدف
17	icmpOutTimeExcds	معدل خرج رسائل الزائد وقتها
18	icmpOutParmProbs	معدل خرج رسائل بها مشكلة معامل
19	icmpOutSrcQuenchs	معدل خرج رسائل إخماد مصدر
20	icmpOutRedirects	معدل خرج رسائل معاد توجيهها
21	icmpOutEchos	معدل خرج رسائل الصدى
22	icmpOutEchoReps	معدل خرج رسائل استجابة صدى
23	icmpOutTimestamps	معدل خرج رسائل أختام زمنية
24	icmpOutTimestampReps	معدل خرج رسائل استجابة أختام زمنية
25	icmpOutAddrMasks	معدل خرج رسائل طلب قناع عنوان
26	icmpOutAddrMaskReps	معدل خرج رسائل استجابة طلب قناع عنوان

ينبغي على محطة التشغيل أن تقوم بمعالجة كل حزمة بيانات ICMP يتم استقبالها، وأن إجراء هذا العمل يمكن أن يؤثر سلبيا على إجمالي أداء محطة التشغيل. أثناء فترات التشغيل العادية، فإن حركة مرور الرسائل في الشبكة، تستنفذ قدرة معالجة أقل ما يمكن. أما في أوقات الازدحام (وقت الذروة)، فيتم إرسال أعداد ضخمة من حزم بيانات ICMP ، وقد يتطلب ذلك مصادر كافية كي لا يتأثر أداء محطة التشغيل. إضافة إلى ذلك، فإن بعض حزم بيانات ICMP المستقبلة، مثل رسائل الصدى Echo ، تحتاج بناء حزم بيانات استجابة صدى Echo Response، التي تستهلك قدرة معالجة أكبر.

التطبيق الأول: حساب عدد حزم بيانات ICMP المرسلة والمستقبلة ومعدلاتها

لحساب النسبة المئوية لحزم بيانات ICMP المرسلة والمستقبلة الخاصة بالتطبيق، يجب أولا معرفة إجمالي عدد حزم بيانات ICMP المرسلة والمستقبلة بواسطة محطة التشغيل، ويتم ذلك – كما شرحنا سابقا– بواسطة إيجاد إجمالي عدد حزم البيانات في الدخل والخرج عند كل وحدة بينية. بعد ذلك، نقسم هذا المجموع على ***icmpInMsgs,*** ***icmpOutMsgs*** لنحصل على إجمالي النسبة المئوية لحزم بيانات ICMP المرسلة أو المستقبلة. بواسطة جعل التطبيق يقوم بإجراء عملية التصويت Polling عدة مرات لهذه العناصر، نستطيع معرفة معدل خروج ودخول حزم بيانات ICMP من محطة التشغيل. إن محطة التشغيل التي تقوم بإرسال أو استقبال العديد من حزم البيانات، لا يعني بالضرورة أنه توجد مشكلة في الأداء. لكن معرفتنا لهذه الإحصاءات قد يساعدنا كثيرا في حل مشاكل مستقبلية ذات علاقة بتحسين الأداء أو توسعة الشبكة.

على سبيل المثال: نفترض وجود مستخدم يعاني من بطء في جلسة Session الدخول عن بعد إلى المحطة المتصلة بالشبكة. ونريد فحص سبب العطل.

أولا: يمكن أن نتخذ إجراءً بفحص إدارة الأعطال، لمعرفة ما إذا كنا سنجد خطأ بين المستخدم ومحطة الشبكة، أو لا.

ثانيا: يمكن بعد ذلك أن نستخدم تطبيق إدارة الأداء لكي نرسم بيانيا حمل المعالج Processor Load في المحطة. عندما نجد أن حمل المعالج عالياً جدا ، ويصل تقريبا إلى 70% ، مع وجود قمم Spikes تصل لأعلى من 90%.

ثالثا: يمكنا بعد ذلك، فحص تطبيق إدارة الحسابات لإيجاد عدد المستخدمين، والعمليات في المحطة. فنجد أن عددا صغيرا منهم فقط يمكن أن ينشئ رسما توضيحيا يبين معدل حزم البيانات الداخلة والخارجة لمحطة الشبكة. فنجد أن معدل حزم البيانات مرتفعا، ويصل تقريبا إلى أقصى أداء في بطاقة الوحدة البينية.

رابعا: بإمعان النظر، نجد أن كثيرا من حزم البيانات تكون ICMP . مرة أخرى، نقوم بفحص عمليات النظام، فنجد في هذه المرة، أن أحد المستخدمين يبدو أنه يقوم بإرسال مستمر لحزم بيانات صدى ICMP Echoes (عمليات pings) لكل نظام في الشبكة. يكون الغرض من هذا العمل، هو تحقيق إمكانية الوصول Reachability لكل نظام في شبكة البيانات. على الرغم من اتخاذ هذا الإجراء، فإن هذه العملية تستهلك مصادر نظام كافية تسبب مشكلة في أداء محطة التشغيل التي يتصل منها المستخدم.

أيضا، يمكن لعناصر مجموعة ICMP أن تبين نوع حزم بياناتICMP . بمعرفة معدل العناصر التالية:

icmpInEchos, icmpOutEchos,
.icmpInEchoReps, icmpOutEchoReps

خامسا: يمكنا عزل مشاكل الأداء، مثل المشكلة التي تم شرحها في المثال السابق.

إن محطة التشغيل التي بها عدد كبير من الرسائل المعاد توجيهها ***icmpInRedirects***، يمكن أن تبين مشاكل جدول المسارات، وأداء الشبكة. أيضا، إن محطة التشغيل التي ترسل عدداً كبيراً من الرسائل المعاد توجيهها ***icmpOutRedirects*** ، قد يعني أن محطة التشغيل تقوم بتغيير قيم جدول المسارات، وتخبر المصدر أن يغير مسار حزم البيانات إلى مسار آخر. بالإضافة، أنه عندما تقوم محطة التشغيل بإرسال أو استقبال أخطاء IP عديدة، يمكن للتطبيق أن يستخدم عناصر

icmpInErrors, incmpOutErrors لتحديد ما إذا كانت حزم بيانات ICMP هي التي تسبب المشكلة.

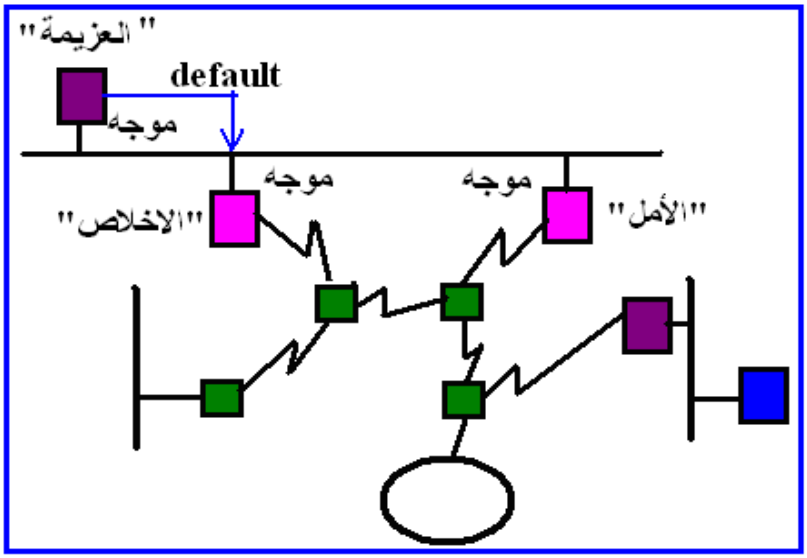
- **<u>التطبيق الثاني: حزم البيانات Redirect (المعاد توجيهها)</u>**

يوجد نوع آخر من رسائل ICMP هي حزم البيانات Redirect ، يمكن أن تعطينا فكرة معينة عن مشاكل أداء الشبكة. ترسل حزم البيانات Redirect إلى مصدر رسائل داتاجرام IP، عندما ينبغي على محطة الاستقبال تحديد مسار رسالة داتاجرام IP خارجة من نفس الوحدة البينية التي تم استقبال الرسالة منها. إن استقبال العديد من رسائل ICMP Redirect يمكن أن يدل ضمنيا على أن محطة المصدر تقوم بإرسال رسائل داتاجرام IP إلى مكان غير صحيح كي يحدد مسارها، وأن هذه الرسائل ينبغي أن ترسل إلى مكان مختلف. ويحدث هذا عادة، عندما يوجد خيار لمحطة التشغيل في اختيار موجهات IP التي تحدد مسار رسائل داتاجرام IP من خلالها.

<u>على سبيل المثال</u>: يوضح الشكل5.5 ، أنه يمكن ضبط موجه "العزيمة" لتحديد مسار جميع رسائل داتاجرام IP ، من خلال وحدة بينية محلية ايثرنيت للموجه "الإخلاص". لكن المسار الأحسن إلى الهدف، يكون من خلال موجه "الأمل". ينتج عن ذلك، أن موجه "الإخلاص" يرسل لموجه "العزيمة" رسالة Redirect. من الناحية النظرية، ينبغي على موجه "العزيمة" تغيير مساره إلى الهدف، وأن يرسل رسائل داتاجرام IP متلاحقة من خلال موجه "الأمل". لكن الحاسوبات المضيفة Hosts لا تؤدي عادة هذه الوظيفة. عندما يستمر الحاسوب المضيف في إرسال رسائل داتاجرام IP إلى الهدف من خلال موجه "الإخلاص"، فإنه ينتج عن ذلك أن يقوم كل موجه بإرسال رسالة ICMP Redirect .

يمكن إيجاد المعدل الذي عنده يقوم الحاسوب المضيف بإرسال رسائل ICMP Redirect بواسطة استخدام العنصر ***icmpInRedirects*** ، وتحديد ما إذا كانت مشكلة الأداء في الشبكة هي سبب قيام الحاسوب المضيف المصدر بالإرسال إلى موجه مبدئي غير صحيح.

في الشكل5.5، تم تهيئة موجه "العزيمة" لاستخدام موجه "الإخلاص"؛ ضبط مبدئيdefault؛ لتحديد مسار الرسائل من خلال بطاقة وحدة بينية ايثرنيت، لكن المسار الأحسن إلى الهدف يكون من خلال موجه "الأمل". ينتج عن هذه التهيئة، أن يقوم موجه "الإخلاص" بإرسال رسالة ICMP Redirect إلى موجه "العزيمة" .



الشكل5.5 مثال لتطبيق إدارة الأداء باستخدام عنصر ICMP Redirect.

أسئلة تقويم ذاتي

ما هي مهام مجموعة عناصر بروتوكول رسائل تحكم الانترنيت ICMP ؟.

يستخدم بروتوكول ICMP حزم Redirect .

أ) اذكر فيم تستخدم هذه الحزم ؟ .

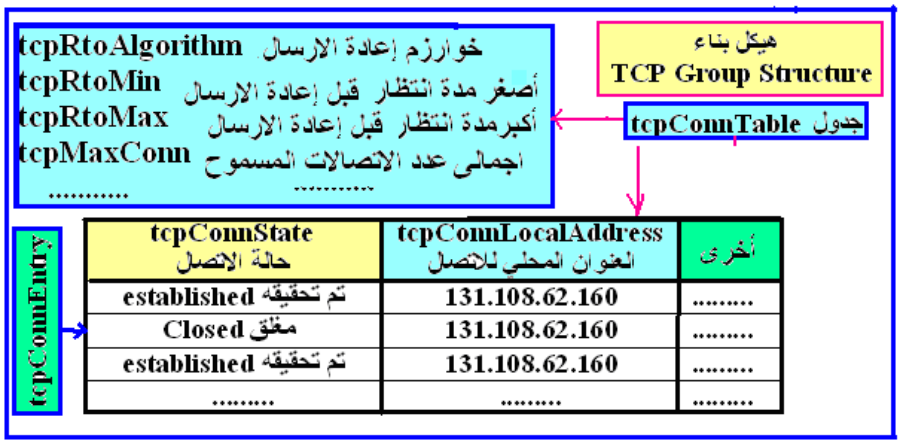
ب) اشرح مثالا تطبيقيا يوضح استخدامها في شبكة البيانات ؟

يبين الجدول التالي بعض عناصر مجموعة ICMP المستخدمة في إدارة الاداء ووظائفها قم بتوفيق الإجابات الصحيحة.

رقم العنصر	العنصر	المعلومات	رقم الإجابة
1	icmpInMsgs	معدل دخل رسائل معاد توجيهها	.....
2	icmpInEchos	معدل خرج الرسائل	.....
3	icmpInTimestamps	معدل خرج رسائل معاد توجيهها	.....
4	icmpInDestUnreachs	معدل دخل رسائل أختام زمنية	.....
5	icmpInRedirects	معدل دخل رسائل لم تصل للهدف	.....
6	icmpOutMsgs	معدل خرج رسائل الأخطاء	.....
7	icmpOutErrors	معدل خرج رسائل طلب قناع عنوان	.....
8	icmpOutAddrMasks	معدل خرج رسائل استجابة صدى	.....
9	icmpOutEchoReps	معدل دخل الرسائل	.....
10	icmpOutRedirects	معدل دخل رسائل صدى	.....

3. مجموعة عناصر بروتوكول النقل TCP

يقوم بروتوكول النقل TCP بتوفير اتصالاً معتمداً بين التطبيقات. يتعامل بروتوكول TCP مع تحكم التدفق Flow Control، واختناق الشبكة Network Congestion، والقطاعات المفقودة Lost Segments المعاد إرسالها. يمكن أن تساعد مجموعة TCP في إدارة التهيئة، والأداء، و الحسابات. تنقسم عناصر مجموعة TCP إلى عناصر عامة حول نظام بروتوكول TCP وجدول لقيم اتصال خالٍ. يتغير هذا الجدول عند بداية أو نهاية كل اتصال يقوم به بروتوكول TCP . يوضح الشكل5.6 بناء هيكلي مبسط لمجموعة TCP.



الشكل5.6 بناء هيكلي مبسط لمجموعة TCP.

1.3 مجموعة عناصرTCP الخاصة بإدارة التهيئة

يبين الجدول5.4 مجموعة عناصر بروتوكول النقل TCP الخاصة بتطبيقات إدارة التهيئة. إن تهيئة خوارزم إعادة الإرسال TCP و محددات الأزمنة timers المرافقة له، يمكن أن يؤثر بقسوة drastically على تطبيقات الأداء التي تستخدم هذا البروتوكول في نقل الرسائل. عندما تستخدم نظم مختلفة، مخططات schemes إعادة إرسال

مختلفة، يمكن أن ينتج عن ذلك اختناق شبكي، أو توزيع سعة نطاق غير عادلة unfair.

الجدول5.4

العنصر	المعلومات
tcpRtoAlgorithm	خوارزم إعادة الارسال
tcpRtoMin	أصغر مدة انتظار قبل إعادة الارسال
tcpRtoMax	اكبرمدة انتظار قبل إعادة الارسال
tcpMaxConn	اجمالى عدد الاتصالات المسموح
tcpCurrEstab	عدد التوصيلات الحالية

التطبيق الأول: تحديد تهيئة المسار

بواسطة جعل التطبيق يستفسر عن العناصر التالية:

tcpRtoMax, tcpRtoMin, tcpRtoAlgorithm,

يمكن أن نعرف ما إذا كانت التهيئة الحالية لبروتوكول TCP تؤدي عملها جيدا داخل النظام المحيط بالوسط الشبكي.

إن النظام الذي يستخدم موقت timer إعادة إرسال ثابت، ربما يميل إلى استهلاك سعة نطاق غير لازمة مقارنة بالموقت الذي يستخدم خوارزم جان جاكوبسون Jan Jacobson (هو خوارزم يستخدم في التحكم لتجنب حدوث اختناق شبكي).

قد يحتاج تعديل عناصر تحديد تهيئة المسار إلى بذل بعض الجهد، أو ربما يكون الأمر مستحيلا. في بعض النظم، يتطلب عملية تعديل موقتات timers إعادة الإرسال TCP إعادة بناء نظام التشغيل. على الرغم من ذلك، يكون خوارزم إعادة إرسال TCP جزء مكمل لنظام تشغيل الجهاز، ولا يمكن تغييره. حيث أن عملية تغيير خوارزم موقت إعادة الإرسال في النظام، يتطلب عادة تنصيب installing مركم Stack بروتوكول TCP جديد.

- **التطبيق الثاني: حساب إجمالي عدد وصلات TCP**

يمكن أن يساعدنا العنصر ***tcpMaxConn*** في تهيئة الشبكة لمعالجة عدد توصيلات TCP البعيدة الضرورية. عندما يكون إجمالي جميع عدد وصلات TCP الممكنة لا يكفي اختيارات المستخدم، فقد يحتاج إلى نظام آخر. أو عندما يسمح النظام بالتوسع expansion ، يمكن أن نضيف مصادر تسمح بإضافة مزيد من وصلات TCP. لاحظ أن عدد الوصلات الحالية الموجودة في العنصر tcpCurrEstab، يمكن أن تؤثر على اتخاذنا قرارا بخصوص إجمالي عدد وصلات TCP التي قد نحتاج إليها.

أيضا، إن عدد الوصلات TCP الموجودة في النظام، يمكن أن تؤثر على أداء النظام. على سبيل المثال، فإن النظام الذي يستطيع التعامل مع عشر جلسات دخول عن بعد، وحاول خدمة مائة جلسة ،فإن ذلك يؤثر سلبيا على أداء النظام.

2.3 مجموعة عناصر TCP الخاصة بإدارة الأداء

يبين الجدول5.5 مجموعة عناصر بروتوكول النقل TCP الخاصة بتطبيقات إدارة الأداء. نناقش تباعا بعض التطبيقات الهامة التي توضح وظائف هذه العناصر.

الجدول5.5

عناصر مجموعة TCP المستخدمة في إدارة الأداء

الرقم	العنصر	المعلومات
1	tcpAttemptFails	عدد المحاولات الفاشلة لإجراء اتصال
2	tcpEstabResests	مرات إعادة التشغيل من الاتصال المحقق
3	tcpRetransSegs	عدد القطاعات البيانية التي تم إعادة إرسالها
4	tcpInErrs	عدد الحزم المستقبلة و بها أخطأ
5	tcpOutRsts	عدد مرات إعادة تشغيل اتصال
6	tcpInSegs	معدل دخل قطاعات البيانات
7	tcpOutSegs	معدل خرج قطاعات البيانات

- **التطبيق الأول: حساب عدد محاولات رفض reject الاتصال**

يمكن أن تفشل محاولة تحقيق اتصال TCP لأسباب مختلفة، مثلا: ربما لا يوجد نظام الهدف، أو ربما يوجد عطل بالشبكة. إن معرفة عدد محاولات رفض reject الاتصال، يمكن أن يساعدنا في التحديد الكمي لاعتمادية الشبكة network reliability. إن معدلات الرفض الأقل؛ من المرجح؛ أنها تبين شبكة بيانات أكثر اعتمادية. أيضا في الحالة التي ينهي فيها بروتوكول TCP العديد من الجلسات المخفقة أثناء عملية "شرط الإعادة reset condition" ، ربما تبين أن الشبكة فقيرة الاعتمادية unreliable. يمكن أن يستخدم العنصران ***tcpAttemptFails, tcpEstabResets*** لمساعدتنا في قياس معدل الرفض rejection rate في الشبكة.

- **التطبيق الثاني: حساب عدد القطاعات Segments المعاد إرسالها**

يبين العنصر ***tcpRetransSegs*** عدد قطاعات TCP التي يقوم النظام بإعادة إرسالها. إن إرسال قطاعات TCP، لا يعكس مباشرة وجود مشكلة في الأداء. ولكن يمكن لعدد إعادة الإرسال أن يخبرنا ما إذا كانت محطة التشغيل ينبغي عليها أن ترسل نسخاً عديدةَ من البيانات، كجهد يبذل لتأمين الاعتمادية.

عندما يقوم النظام باستقبال قطاعات TCP عن طريق الخطأ، فإن القيمة ***tcpInErrs*** سوف تزداد. إن مشاكل استقبال قطاعات TCP مع زيادة قيمة العنصر ***tcpInErrs*** ، ربما تكون بسبب أن نظام المصدر يقوم بإجراء عملية احتواء encapsulating قطاعات البيانات بطريقة غير صحيحة. وأن جهاز الشبكة الذي يقوم بتوصيل forwarding هذه القطاعات يكون خطأ، أو ربما لأسباب أخرى. في غالبية الحالات، فإن قيمة هذا العنصر سوف ترتفع نتيجة حدوث بعض الأخطاء الأخرى في النظام.

- **التطبيق الثالث: حساب عدد مرات إعادة التشغيل**

يعطي العنصر ***tcpOutRsts*** عدد المرات إلي تقوم فيها محطة التشغيل بإجراء إعادة تشغيلreset اتصال. تحاول محطة التشغيل، إعادة تشغيل اتصال نتيجة عدم اعتمادية

الشبكة، حيث يرجو المستخدم إجراء ذلك، أو وجود مشكلة مصادر، أو أن الأسباب الحقيقية لإعادة التشغيل تكون خاصة بمحطة التشغيل.

عندما يقوم التطبيق بإجراء عملية التصويت polling للعناصر ***tcpInSegs,*** ***tcpOutSegs*** مع الوقت، فإن ذلك يمكننا من فحص معدل قطاعات TCP أثناء دخولهم وخروجهما من محطة التشغيل. وأن هذا المعدل يمكن أن يؤثر على أداء محطة التشغيل، أو التطبيق الذي يعتمد على بروتوكول TCP من أجل الاتصال.

3.3 مجموعة عناصر TCP الخاصة بإدارة الحسابات

يبين الجدول5.6 مجموعة عناصر بروتوكول النقل TCP الخاصة بتطبيقات إدارة الحسابات.

الجدول5.6

عناصر مجموعة TCP المستخدمة في إدارة الحسابات

الرقم	العنصر	المعلومات
1	tcpActiveOpents	عدد المرات التي قام فيها النظام بفتح اتصال
2	tcpPassiveOpents	عدد المرات التي قام فيها النظام باستقبال طلب بفتح اتصال
3	tcpInSegs	إجمالي القطاعات المستقبلة
4	tcpOutSegs	إجمالي القطاعات المرسلة
5	tcpConnTable	عدد التوصيلات الحالية

- **<u>التطبيق الأول: حساب عدد اتصالات TCP وفواتير الدفع</u>**

تحتاج المؤسسة الموجود بها الشبكة البيانات أن تعرف عدد اتصالات TCP من والى النظام من أجل تقييم الاستخدام الحالي لمصادر الشبكة. يفيد هذا التقييم في إعادة تهيئة النظام، أو شراء نظم إضافية. يبين العنصرين ***tcpActiveOpens,*** ***tcpPassiveOpens*** إجمالي عدد مرات الاتصال من والى النظام، على الترتيب. ويبين العنصرين ***tcpInSegs, tcpOutSegs*** عدد قطاعات TCP الداخلة والخارجة

من محطة التشغيل على الترتيب. تكون هذه المعلومات ذات فائدة في حساب فواتير دفع مستخدمي الشبكة.

يبين العنصر ***tcpConnTable*** حالة عدد اتصالات TCP الحالية، والعنوان والمنفذ المحلي، وعنوان ومنفذ TCP البعيد. إن هذه القيم تحفظ الحالة الحالية لبروتوكول TCP في محطة التشغيل، ويمكن أن تتغير عند أي لحظة. بجعل تطبيق إدارة الحسابات يقوم بعملية تصويت للعنصر ***tcpConRemAddress*** ، يمكنا تحديد عناوين النظام البعيدة الحالية لوصلة TCP.

المعلومات التي نحصل عليها تخص فقط عنوان النظام البعيد، وليس المستخدم البعيد.

عندما تقوم محطة التشغيل بإجراء هذا التصويت لهذا العنصر كل خمس عشرة دقيقة، يمكن لمديرين النظام معرفة النظم البعيدة التي تستعمل مصادرهم، ومدة الاستخدام. يمكن للتطبيق بعد ذلك، أن ينشئ فواتير الدفع نظير استخدام المحطة المحلية لهؤلاء المستخدمين الذين يمتلكون النظم البعيدة، ويستخدمون محطة التشغيل المحلية.

أيضا، يحتوي العنصر ***tcpConnTable*** على معلومات عن منفذ TCP للمصدر والهدف لكل اتصال حالي. تستخدم تطبيقات الشائعة منافذ معرّفة جيدا، وهذا يسهل إمكانية تتبع التطبيق الذي يحدث أو التطبيق الذي يستلم اتصال TCP. إن رقم المنفذ يفرق بين تطبيق الدخول البعيد، مثل شبكة Telnet، وتطبيق نقل الملفات FTP. تفيد هذه البيانات أغراض الحسابات، وتحديد سبب اتصالات TCP من والى محطة التشغيل.

4.3 مجموعة عناصر TCP الخاصة بإدارة الأمن

أيضا، تفيد المعلومات الموجودة في العنصر ***tcpConnTable*** في إدارة الأمن، وذلك بتتبع النظم البعيدة التي تصل إلى المصادر من خلال بروتوكول TCP. يمكن أن تشكل هذه المعلومات تقارير أساسية توضح أن محطة التشغيل لم تسمح بإجراء اتصالات من أجانب Foreign، أو نظم غير محظورة unrestricted systems . قد تؤثر فترة التصويت بشكل كبير في فعالية هذا التقرير – حيث أن المقتحم intruder قد يحتاج فقط إلى ثوانٍ معدودة لتجميع معلوماته قبل فك breaking الاتصال. إذا لم يقع التصويت خلال هذه الثواني القليلة، فإن جميع سجلات المهاجمة intrusion سوف تفقد.

أسئلة تقويم ذاتي

ارسم شكلا يوضح البناء الهيكلي لمجموعة عناصر بروتوكول النقل TCP ؟

بالاستعانة بجداول مجموعة عناصر TCP ، اكتب ملخصاً يشرح كيفية استخدامها في عمل ما يلي:

أ) إدارة التهيئة ؟ ب) إدارة الأداء ؟

اذكر مجموعة العناصر المعلوماتية لمجموعة بروتوكول TCP المستخدم في حساب كل من الآتي:

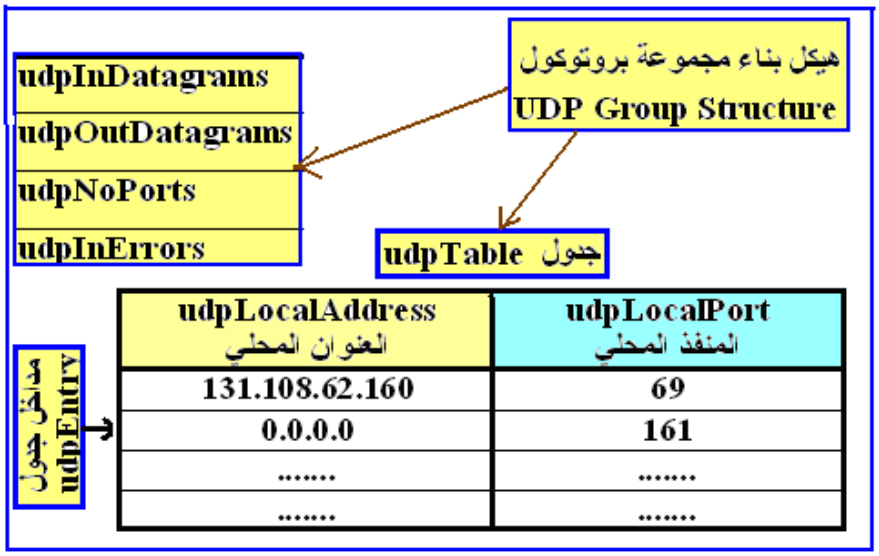
أ) عدد القطاعات البيانية المطلوب إرسالها ؟.

ب) حساب عدد مرات إعادة التشغيل ؟ .

ج) عدد اتصالات TCP التي تستخدم لحساب فواتير مستخدمي الشبكة؟

4. عناصر مجموعة بروتوكول UDP

يستخدم بروتوكول UDP في طبقة النقل Transport Layer، ويقوم بإرسال واستقبال رسائل داتاجرام Datagram بوساطة التطبيق. وهذه الاتصالات عادة تعتمد على اعتمادية الشبكة، لأن بروتوكول UDP، لا يتيح رسائل تأكيد Acknowledgements تؤكد وصول رسائل داتاجرام إلى الهدف؛ لهذا السبب يطلق عليه عديم الاتصالية connectionless، وعديم الاعتمادية unreliable،. لذلك تحتوي مجموعة UDP على عدد محدود من العناصر. توفر هذه العناصر معلومات حول بروتوكول UDP في محطة التشغيل، ومداخل entries حول تطبيقات UDP الحالية التي تسمح برسائل داتاجرام في محطة التشغيل. يوضح الشكل5.7 الهيكلي البنائي لمجموعة UDP.



يوضح الشكل5.7 هيكلي بنائي مبسط لمجموعة UDP.

بسبب أن UDP لا يقوم بإنشاء اتصالات، فإن جدول UDP لا يعطي بيانات عن الاتصالات الحالية – حيث أنها لا توجد أبدا (لأن رسائل داتاجرام نفسها تحتوي على عنوان الهدف). بدلا من ذلك، فإن الجدول يخبرنا عن كل منفذ محلي موجود، وعنوان شبكة ذات علاقة. ويمكن أن تساعدنا عناصر مجموعة UDP في إدارة الأداء

والحسابات. وأن هذه الوظائف تشبه وظائف عناصر مجموعة TCP لنفس مناطق إدارة الشبكة.

1.4 عناصر مجموعة UDP الخاصة بإدارة الأداء

يبين الجدول5.7 عناصر مجموعة UDP الخاصة بتطبيقات إدارة الأداء. إن معالجة رسائل داتاجرام UDP يمكن أن يؤثر على أداء محطة التشغيل، ولهذا فإن إجراء عملية التصويت لمعرفة قيم العناصر ***udpOutDatagrams, udpInDatagrams*** مع مرور الوقت يتيح لنا معرفة بيانات هامة عن معدل الدخل والخرج لرسائل داتاجرام.

الجدول5.7

عناصر مجموعة UDP المستخدمة في إدارة الأداء

الرقم	العنصر	المعلومات
1	udpInDatagrams	معدل دخل رسائل داتاجرام
2	udpOutDatagrams	معدل خرج رسائل داتاجرام
3	udpNoPorts	معدل رسائل داتاجرام التي لم ترسل لمنفذ صحيح
4	udpInErrors	معدل رسائل داتاجرام المستقبلة بها خطأ

- **<u>التطبيق الأول: تحديد بعض مشاكل محطة التشغيل</u>**

يخبرنا العنصر ***udpNoPorts*** عن محطة تشغيل رسائل داتاجرام لتطبيق غير معروف أو تطبيق معروف لكن حاليا غير مشغل. عندما تكثر هذه الرسائل بشكل واضح، فإن ذلك يمكن أن يسبب مشكلة في أداء محطة التشغيل. تستقبل محطة التشغيل عادة رسائل داتاجرام عندما يستخدم تطبيق UDP حزم بيانات إذاعية IP في توصيل المعلومات. عندما نجد إذاعة IP، فإن كل جهاز IP يقوم بالتقاط حزم البيانات المذاعة، ويقوم بتوصيلها إلى UDP . تقوم الأجهزة التي يعمل بها التطبيق فقط، وكذلك منفذ port حزم بيانات UDP المناسب باستقبال هذه الحزم، وجميع التطبيقات الأخرى تقوم بتدوين هذه الحزم في العنصر ***udpNoPorts***.

على سبيل المثال: يستخدم بروتوكول TFTP مع البروتوكول UDP للسماح بجهاز الشبكة أن يرسل ويستقبل ملف واحد بدون استخدام كلمة مرور Password. يوفر خادم بروتوكول TFTP ملف بواسطة الإصغاء listening لمنفذ UDP للعميل TFTP للسؤال عن الملف– في كثير من الحالات فإن العميل TFTP سوف يرسل رسالة إذاعية IP كي يجدها خادم TFTP في الشبكة. إن النظم التي يوجد بها الخادم المصغي Server Listening سوف تستقبل الرسالة المذاعة ، وترسل الملف إلى العميل، كلما أمكن. جميع الحاسوبات المضيفة IP الأخرى، التي لا تصغي في منفذ بروتوكول TFTP سوف تقوم بزيادة قيمة العنصر ***udpNoPorts*** الخاص بها.

- **التطبيق الثاني: إيجاد أخطاء محددة في الشبكة**

يمكن أن يخبرنا العنصر ***udpInErrors*** عن أخطاء محددة في الشبكة. لقد تم تصميم البروتوكول UDP ليكون بسيطا، لذلك فهو فقط يقوم بفحص الإضافات الدورية CRC في جزء البيانات لرسالة داتاجرام. إن بيانات UDP داتاجرام يمكن أن تحتوي على أخطاء CRC لأسباب عديدة، منها البرامج، وأخطاء وصلة الربط Link، أو أخطاء جهاز الشبكة. [إن النظام الذي يستقبل رسائل داتاجرام بكثرة، يقوم العنصر ***udpInErrors*** بعدها،] يمكن أن تؤدي إلى أداء ضعيف في التطبيق عند استقبال المعلومات. على سبيل المثال، يستخدم بروتوكول"سنمب" بروتوكول UDP للنقل. عندما يعاني نظام إدارة الشبكة مشاكل من استقبال بيانات داتاجرام خاصة بالبروتوكول "سنمب" من نظام بعيد، فإن العداد ***udpInErrors*** المحلي يمكن أن يوضح أن رسالة داتاجرام تحتوي على معلومات "سنمب" التي من المحتمل أن لا تعبر الشبكة بنجاح.

2.4 عناصر مجموعة UDP الخاصة بإدارة الحسابات

يبين الجدول5.8عناصر مجموعة UPD الخاصة بتطبيقات إدارة الحسابات. حيث يمكن أن نستخدم العنصرين ***updOutDatagrams, udpInDatagrams*** لتحديد عدد رسائل داتاجرام UPD التي ترسلها وتستقبلها محطة التشغيل، على الترتيب. بهذه

الطريقة يمكن أن نعرف الاحتياجات إلى البروتوكول UPD والتطبيقات التي تستخدمه في محطة التشغيل.

الجدول5.8

عناصر مجموعة UDP المستخدمة في إدارة الحسابات

الرقم	العنصر	المعلومات
1	udpInDatagrams	إجمالي رسائل داتاجرام المستقبلة
2	udpOutDatagrams	إجمالي رسائل داتاجرام المرسلة
3	udpTable	المنافذ الحالية التي تقبل داتاجرام

يحتوي الجدول ***udpTable*** على عناصر مشابهة للموجودة في الجدول ***tcpConnTable***، وهذا الجدول يتكون من مجموعة من المداخل ***udpEntry***، كل منها يحتوي على العناصر ***udpLocalAddress, udpLocalPort*** . بينما يعطي العنصر ***udpLocalAddress*** عنوان IP المحلي لمنفذ الإصغاء Listening Port، يعطي العنصر ***udpLocalPor***t رقم المنفذ.

بسبب أن بروتوكول UDP غير اتصالي connectionless، فإن مداخل الجدول udpTable تظل صالحة طوال المدة التي يقوم فيها التطبيق بالإصغاء إلى المنفذ. وهذه الخاصية تمكننا من رصد خدمات الشبكة التي توفرها لمحطة التشغيل. نستطيع فحص وجود هذه الخدمات في الشبكة لمعرفة ما إذا كانت مصادر الشبكة الموجودة تكون مناسبة.

3.4 عناصر مجموعة UDP الخاصة بإدارة التهيئة

إن رصد الخدمات المتاحة في الشبكة، يعتمد على إدارة التهيئة. يمكننا؛ بواسطة فحص الجدول ***udpTable***؛ تحديد ما إذا كانت تطبيقات محطة التشغيل قد تمت تهيئتها بشكل صحيح. على سبيل المثال، عندما يكون معروفا أن محطة التشغيل يوجد بها تطبيق يوفر إجراء عملية الطباعة عن بعد من منفذ UDP. بعد ذلك، يمكننا بسهولة التحقق من تهيئة هذه المعلومات بواسطة استخدام الجدول ***udpTable***.

4.4 عناصر مجموعة UDP الخاصة بإدارة الأمن

أيضا، يمكن لإدارة الأمن أن تستخدم المعلومات الموجودة في الجدول ***udpTable***. حيث يمكن لتطبيق إدارة الأمن إجراء عملية التصويت لمعلومات ***tcpConnTable*** فحص دخول غير مفوض unauthorized access، إذ يستطيع التطبيق إجراء فحص، كي يتأكد من أن محطة التشغيل، لا تقوم بتشغيل تطبيق غير آمن، مستخدما بروتوكول UDP.

على سبيل المثال: نفترض أن قسم الرواتب في شبكة أحد المؤسسات، قد قرر أن تطبيق "إيجاد راتب الموظف"، يتم تشغيله فقط على حاسب واحد محدد مختص بذلك. فإن التطبيق يستقبل ويرسل رسائل داتاجرام لإيجاد راتب الموظف من منفذ UDP المخول بذلك. يمكن لأداة إدارة الأمن، أن تفحص جدول ***udpTable*** في جميع النظم، وتتحقق ما إذا كان هذا المنفذ المحلي موجودا، وبذلك تساعد في ضبط تحكم الدخول إلى المعلومات الحساسة.

أسئلة تقويم ذاتي

ارسم شكلا يوضح البناء الهيكلي لمجموعة عناصر بروتوكول UDP؟.

اشرح كيفية الاستعانة بعناصر مجموعة بروتوكول UDP في الآتي:

أ) إدارة أداء الشبكة ؟ . ب) إدارة الأمن ؟

أكمل الجدول التالي والذي يبين عناصر مجموعة UPD الخاصة بتطبيقات إدارة الحسابات ؟.

رقم	العنصر	المعلومات
1	udpInDatagrams	؟.....
2	udpOutDatagrams	؟.....
3	udpTable	؟.....

5. مجموعة عناصر بروتوكول EGP و بروتوكول CMOT ومجموعة عناصر الإرسال

1.5 مجموعة عناصر بروتوكول EGP

عزيزي الدارس،

يستخدم البروتوكول EGP في إخبار أجهزة شبكة IP عن إمكانية الوصول Reachability لشبكات IP الأخرى. إن بروتوكول EGP لا يعطي المسار بكامله Entire Route إلى الشبكة الأخرى، لكنه يساعد الجهاز من معرفة في أي اتجاه توجد الشبكة.

يمكن تجميع شبكات IP إلى مناطق منطقية تسمى "النظم المستقلة Autonomous Systems" وهي عبارة عن شبكة واحدة، أو شبكات فرعية مصاحبة، أو تجميع شبكي مع شبكات فرعية تحت نفس الإدارة. يمكن لجهازين من الشبكة موجودين في نظامين مستقلين مختلفين مشاركة معلومات إمكانية الوصول من خلال بروتوكول EGP .

هذه، سوء تهيئة أو تغير في مستقبل أداء EGP لهذا الجهاز.

1.1.5 عيوب البروتوكول EGP ومعالجتها بواسطة BGP

لقد استخدم البروتوكول EGP في بدايات تطوير شبكة الإنترنيت، بسبب صغر حجم هذه الشبكة في الماضي، وذلك لأن بروتوكول EGP يتميز بأنه بسيط، وسريع، وغير معقد. مع ازدياد حجم شبكة الإنترنيت أصبح البروتوكول EGP غير مناسب، ولا يستخدم حاليا إلا في الشبكات الخاصة الكبيرة Large Private Networks. إن المشاكل الأساسية التي يعاني منها بروتوكول EGP أنه لا يستطيع اكتشاف العروات Loops التي تحدث في البروتوكول، كما أنه لا يحدد جدول المسارات routing ، فهو فقط يحدد معلومات إمكانية الوصول Reachability. كما أنه ليست لديه مقدرة التوسع

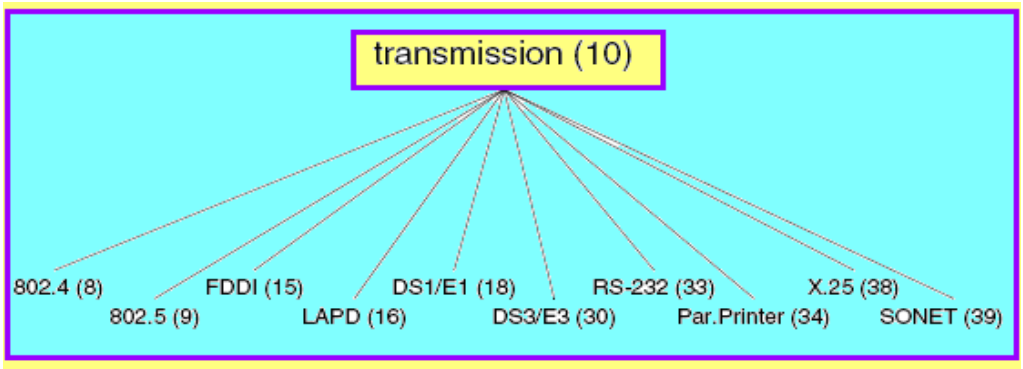
scale up مع ازدياد حجم الشبكة. لهذه الأسباب توقف استخدام بروتوكول EGP مع تطور شبكات الإنترنيت، وقد حل محله البروتوكول BGP ، الذي عالج جميع المشاكل التي واجهها البروتوكول EGP . وبناءً على هذه التطورات فإنه يمكن تطوير قاعدة المعلومات الإدارية MIB-II لتشمل عناصر مجموعة جديدة، هي عناصر بروتوكول BGP كي تحل محل مجموعة EGP عند إدارة شبكات مثل الإنترنيت.

2.5 مجموعة بروتوكول CMOT

توجد مجموعة CMOT ضمن قائمة عناصر مجموعات قاعدة المعلومات الإدارية MIB-II فقط لأسباب تاريخية. فقد كانت تستخدم في السابق كبروتوكول يساعد في النقل من "سنمب" إلى CMIS/CMIP. بسبب عدم استخدام بروتوكول CMOT، فإنه لا يوجد حالياً عناصر في هذه المجموعة.

3.5 مجموعة عناصر الإرسال -Transmission Group

إن مجموعة الإرسال تعطينا معلومات عن وسط محدد يعمل كوحدات بينية للنظام. يتم تعريف قواعد معلومات إدارة لكل أنواع الوسائط، على سبيل المثال: FDDI, Token Ring(IEEE 802.5). ويوضح الشكل5.8 بعض أنواع التقنيات المختلفة التي تستخدم في نظم الإرسال.



شكل5.8 نموذج يبين بعض العناصر الخاصة لمجموعة الإرسال.

أسئلة تقويم ذاتي

اكتب نبذة مختصرة عن البروتوكولين EGP, BGP.
اكتب ملخصاً يشرح بعض تطبيقات مجموعة عناصر الإرسال.
اذكر معاني المصطلحات الآتية: ARP, CMOT, TFTP .

6. عناصر مجموعة بروتوكول SNMP

تعطينا مجموعة SNMP معلومات عن الأخطاء، وحزم البيانات الداخلة والخارجة من محطة التشغيل. تفيد هذه العناصر في تطبيقات إدارة الشبكة. يمكن استخدام تطبيقات إدارة الأعطال لمراقبة مشاكل SNMP مثل الأخطاء ومعدلاتها. يمكن أن نستخدم تطبيقات إدارة الأداء في حساب معدل حزم بيانات SNMP الداخلة والمغادرة لمحطة التشغيل. يمكن استخدام تطبيقات إدارة الحسابات وهذه العناصر لإيجاد العدد الفعلي لحزم بيانات SNMP المرسلة والمستقبلة بواسطة محطة التشغيل. إضافة إلى استخدام بعض عناصر SNMP في تحقيق إدارة الأمن وإدارة التهيئة ، كما سوف يتم شرحه تباعاً في الفقرات التالية.

1.6مجموعة عناصر SNMP المستخدمة في تطبيقات إدارة الأعطال

يبين الجدول5.9 عناصر مجموعة SNMP المستخدمة في إدارة الأعطال. كل عنصر منها يعطي معلوماتٍ عن أخطاء SNMP. على الرغم من أن الوكيل الذي يستقبل أو يرسل هذه الأخطاء قد لا يظهر مشكلة مع الشبكة نفسها، فهي تخبرنا أن محطة التشغيل لا تتعامل مع حزم بيانات SNMP بطريقة صحيحة.

الجدول5.9

عناصر مجموعة "سنمب" لإدارة الأعطال ووظائفها

الرقم	العنصر	المعلومات
1	snmpInASNParseErrs	إجمالي دخل أخطاء "أسن.1"
2	snmpInTooBigs	إجمالي دخل أخطاء "أكبر من اللازم"
3	snmpInNoSuchNames	إجمالي دخل أخطاء "لا يوجد هذا الاسم"
4	snmpInBadValues	إجمالي دخل أخطاء "القيم السيئة"
5	snmpInReadOnlys	إجمالي دخل أخطاء "القراءة فقط"
6	snmpInGenErrs	إجمالي دخل أخطاء "الخطأ-الناشئ"
7	snmpOutTooBigs	إجمالي خرج أخطاء "أكبر من اللازم"
8	snmpOutNoSuchNames	إجمالي خرج أخطاء "لا يوجد هذا الاسم"
9	snmpOutBadValues	إجمالي خرج أخطاء "القيم السيئة"
10	snmpOutGenErrs	إجمالي خرج أخطاء "الخطأ-الناشئ"

يمكن أن يبين نوع وعدد الأخطاء، إن محطة التشغيل تستقبل حزم بيانات SNMP بها أخطاء من أجهزة الشبكة. تكمن حلول هذه الأخطاء غالبا، في التهيئة الخاصة بالمدير أو الوكيل SNMP . إذا لم تصلح إعادة التهيئة هذه الأخطاء، فإن المشكلة ربما تكون بسبب بروتوكول SNMP في المدير أو الوكيل.

2.6 مجموعة عناصر SNMP المستخدمة في تطبيقات إدارة الأداء

يبين الجدول5.10 عناصر مجموعة SNMP المستخدمة في إدارة الأداء. مثل أنشطة محطة التشغيل الأخرى، حيث إن بروتوكول SNMP يمكن أن يؤثر على أداء النظام. إذا أردنا أن نعرف النسبة المئوية للمصادر التي تستخدمها محطة التشغيل للتعامل مع بروتوكول SNMP، يمكن أن نجد معدل حزم بيانات SNMP الداخلة والخارجة بواسطة العنصرين ***snmpInPkts***, ***snmpOutPkts***. وأن العناصر الأخرى المذكورة في الجدول5.10 تمكنا من إيجاد نوع حزم بيانات SNMP التي تتعامل معها محطة

التشغيل. بواسطة رصد هذه المعدلات، نستطيع اقتراح سبب ارتفاع معدل حزم بيانات SNMP في الدخل أو الخرج.

الجدول5.10

عناصر مجموعة "سنمب" لإدارة الأداء ووظائفها

الرقم	العنصر	المعلومات
1	snmpInPkts	معدل حزم دخل سنمب
2	snmpOutPkts	معدل حزم سنمب المرسلة
3	snmpInTotalReqVars	معدل دخل طلبات حصول وحصول تالي
4	snmpInTotalSetVars	معدل دخل طلبات إعداد
5	snmpInGetRequests	معدل دخل طلبات حصول
6	snmpInGetNexts	معدل دخل طلبات حصول تالي
7	snmpInSetRequests	معدل دخل طلبات إعداد
8	snmpInGetResponses	معدل دخل حصول استجابات
9	snmpInTraps	معدل دخل رسائل مصيدة
10	snmpOutGetRequests	معدل خرج طلبات حصول
11	snmpOutGetNexts	معدل خرج طلبات حصول تالي
12	snmpOutSetRequests	معدل خرج طلبات إعداد

<u>على سبيل المثال</u>: إن المعدل المرتفع للعنصرين ***snmpInGetRequests***, ***snmpOutGetResponses*** قد يظهر لنا أن المدير يقوم حاليا بتجميع معلومات من محطة التشغيل.

3.6 مجموعة عناصر SNMP المستخدمة في تطبيقات إدارة الحسابات

يمكن أن يستخدم تطبيق إدارة الحسابات بعض العناصر التي استخدمت في إدارة التهيئة وإدارة الأداء، كما هو مبين في الجدول5.11 ، لإيجاد إجمالي عدد حزم بيانات SNMP المرسلة والمستقبلة. وهذه المعلومات مفيدة لحساب فواتير استخدام الشبكة، عندما نستخدم نموذج حساب الفواتير بناء على حزم البيانات المرسلة أو المستقبلة.

الجدول 5.11

عناصر مجموعة "سنمب" لإدارة الحسابات ووظائفها

الرقم	العنصر	المعلومات
1	snmpInPkts	إجمالي دخل حزم سنمب
2	snmpOutPkts	إجمالي حزم سنمب المرسلة
3	snmpInTraps	إجمالي دخل رسائل مصيدة
4	snmpOutTraps	إجمالي خرج رسائل مصيدة

على سبيل المثال: نفترض أن قسم التسويق في شبكة أحد المؤسسات التجارية يستلم الفاتورة كل شهر نظير عدد حزم البيانات التي يستقبلها من الشبكة. وأن شبكة قسم التسويق تم توزيعها على جهازين بالشبكة، كلاً منهما يتم إدارته بواسطة مؤسسة خارجية مسؤولة عن الشبكة. إن حروف المشاركة التي تم تهيئتها في جهازي الشبكة تكون معروفة فقط للمؤسسة الإدارية الخارجية، لضمان أنه لا يستطيع المستخدمون الآخرون أن يستفسروا من الجهازين من خلال SNMP. لذلك، بسبب أن عملية الفواتير تحسب التكاليف بناء على حزم البيانات المستقبلة، فإن حزم بيانات SNMP المستقبلة من الجهازين لا ينبغي أن تدرج في حساب الفاتورة النهائية لقسم التسويق.

يمكن أن يعطينا العنصران ***snmpInTraps*** ، ***snmpInPkts*** ، عدد حزم البيانات التي ينبغي أن تطرح عند حساب الفاتورة النهائية.

4.6 مجموعة عناصر SNMP المستخدمة في تطبيقات إدارة الأمن

يبين الجدول5.12 عناصر مجموعة SNMP المستخدمة في تطبيق إدارة الأمن، والمختصة بتتبع محاولات التوثيق الفاشلة. إن الإجراءات التي تتخذ لذلك تشمل فحص محاولات إدخال كلمات سر غير ناجحة من أجل الدخول لجهاز الحاسوب، أو حروف

مشـــــاركة غيـــــر صـــــالحة فـــــي بروتوكـــــول SNMP. يقـــــوم العنصـــــر ***snmpInBadCommunityNames*** بعدّ عدد المرات التي يقوم فيهـــا المســـتخدم أو التطبيق بمحاولة الاتصال عن طريق بروتوكول SNMP فـــي محطـــة التشـــغيل، ولا يعطي حروف المشاركة الصحيحة. عندما تستقبل المحطـــة حـــروف مشـــاركة غيـــر صحيحة، تقوم بإرسال رسالة trap إلى المدير تعلمه بوجود خطأ توثيق.

الجدول5.12

عناصر مجموعة "سنمب" لإدارة الأمن ووظيفتها

الرقم	العنصر	المعلومات
1	snmpInBadCommunityNames	إجمالي الحزم التي بها "حروف مشاركة" غير صحيحة.
2	snmpInBadCommunityUses	إجمالي الحزم التي بها "حروف مشاركة" لا تسمح بتشغيل طلبات رجاء.

يستخدم العنصر ***snmpInBadCommunityUses*** لعدّ عدد مرات حزم بيانات SNMPالتي تستقبل فيها حروف مشاركة لا تسمح بتشغيل العملية المطلوبة. يمكن ضبط حروف مشاركة مختلفة للعديد من أجهزة الشبكة، لإجراء عمليات مختلفة. على سبيل المثال، يمكن لحروف مشاركة وحيدة تفويض إجراء عمليتين مثل: Get-Request, Get-Next-Request، وأخرى يمكن أن تسمح بإجراء ثلاث عمليات مثل: Get-Request, Get-Next-Request, Set-Request.

إن المؤسسة التي تدير جهاز الشبكة، قد تعرف حروف المشاركة التي تسمح بإجراء جميع عمليات SNMP (وتشمل Get-Request, Get-Next-Request, Set-Request). لكن يمكن أن تحدد السماح للعامة فقط بأن تستخدم حروف المشاركة التي تسمح بالوصول إلى عمليات Get-Request, Get-Next-Request. في هذه الحالة، فهي تفعل ذلك كي تضمن أن موظفي المؤسسة هم فقط الذين يمكنهم تهيئة أجهزة الشبكة من خلال عمليات طلب الإعداد Set-Request.

عندما تزداد قيم هذين العنصرين، فإن تطبيق إدارة الأمن يقوم بتحذيرنا بإرسال رسالة، أو من خلال نافذة التحذير Pop-Up Window. وأيضا، يمكن أن يتم تخزين هذه الوقائع في قاعدة البيانات العلاقية، لاستخدامها في تحليلات مستقبلية. يمكن أن تظهر هذه التحليلات أن الأحداث التي وقعت على أساس زمني، يمكن أن تقودنا إلى أن نستنتج، أنه ربما تكون الإدارة التي تقوم بإجراء عملية التصويت على الجهاز، لا تعرف حروف المشاركة الصحيحة.

5.6 مجموعة عناصر SNMP المستخدمة في تطبيقات إدارة التهيئة

ينبغي على محطة التشغيل أن تكون قادرة على إرسال رسالة trap لبيان فشل التوثيق، عندما تستقبل حزم بيانات بها حروف مشاركة غير صحيحة. بسبب أن حروف المشاركة تكون مكتوبة بشفرة أسكي؛ فإن هذه الطريقة يمكن أن تسبب مشاكل أمن خطيرة. يمكن أن تتغلب محطة التشغيل على ذلك بواسطة إرسال رسالة إعداد ***snmpEnableAuthenTraps*** لتمكين (إرسال) أو عدم تمكين (عدم إرسال) رسالة المصيدة Trap.

أسئلة تقويم ذاتي

اكتب ملخصاً لشرح استخدام مجموعة عناصر بروتوكول SNMP الموجودة في قاعدة معلومات MIB-II في التطبيقات التالية:

أ) إدارة الأعطال. ب) إدارة الأداء. ج) إدارة الحسابات. د) إدارة التهيئة.

في عناصر مجموعة SNMP لادارة الأمن :

أ) حدد العنصر الذي يقوم بعدِّ عدد المرات التي يقوم فيها المستخدم أو التطبيق بمحاولة الاتصال عن طريق بروتوكول SNMP في محطة التشغيل، ولا يعطي حروف المشاركة الصحيحة.

ب) حدد العنصر الذي يستخدم لعدِّ عدد مرات حزم بيانات SNMP التي تستقبل فيها حروف مشـــاركة لا تســـمح بتشغيل العمليـــة المطلوبة.

أسئلة تقويم ذاتي

الجدول التالي (الموضح أمامك) يبين مجموعة عناصر بروتوكول SNMP في قاعدة المعلومات الإدارية MIB-II والخاصة بإدارة الأعطال. قم بتوفيق مسميات العناصر مع ما يقابلها من وظائف واستخدامات.

عناصر مجموعة "سنمب" لإدارة الأعطال ووظائفها "قم بتوفيق الوظائف"

الرقم	العنصر	المعلومات	الإجابات
1	snmpInASNParseErrs	إجمالي دخل أخطاء "القيم السيئة"	.....
2	snmpInTooBigs	إجمالي دخل أخطاء "أكبر من اللازم"	.....
3	snmpInNoSuchNames	إجمالي دخل أخطاء "القراءة فقط"	.....
4	snmpInBadValues	إجمالي دخل أخطاء "أسن.1"	.....
5	snmpInReadOnlys	إجمالي خرج أخطاء "أكبر من اللازم"	.....
6	snmpInGenErrs	إجمالي دخل أخطاء "الخطأ-الناشئ"	.....
7	snmpOutTooBigs	إجمالي دخل اخطاء "لا يوجد هذا الاسم"	.....
8	snmpOutNoSuchNames	إجمالي خرج أخطاء "الخطأ-الناشئ"	.....
9	snmpOutBadValues	إجمالي خرج أخطاء "لا يوجد هذا الاسم"	.....
10	snmpOutGenErrs	إجمالي خرج أخطاء "القيم السيئة"	.....

الخلاصة

يستخدم بروتوكول الإنترنت IP نمطاً عير اتصالي لإرسال داتاجرام.

عرضت الوحدة بناءً هيكلياً مبسطاً لمجموعة عناصر معلومات بروتوكول IP. ويتكون البناء الهيكلي من أربعة أقسام معلوماتية: عناصر تعطي معلومات عن الأخطاء وأنواع حزم بيانات IP، جدول معلومات عن عناوين IP لمحطة التشغيل، جدول مسارات IP لمحطة التشغيل، تحويلات Mapping عناوين IP إلى عناوين البروتوكولات الأخرى، وهذه الخصائص تسبق مرحلة ترجمة العنوان.

عددت الوحدة عناصر مجموعة IP المستخدمة في إدارة التهيئة: تهيئة الجهاز لإرسال IP "ipForwarding"، عناوين IP في الجهاز " ipAddrTable "-جدول مسارات IP " ipRouteTable".

قدمت الوحدة شرحاً لبعض العناصر الهامة وتطبيقاتها المستخدمة في إدارة الأداء:

- قياس حركة مرور الرسائل Traffic:يمكن حساب مجموع العنصرين ifInUcastPkts, ifInNUcastPkts لكل وحدة بينية. بعد ذلك نقسم ipInReceives على هذا المجموع، وبذلك يتم إيجاد النسبة المئوية لرسائل داتاجرام IP المستقبلة.
- حساب عدد الرسائل المهملة Discarded: يقوم العنصر ipInDiscards بعدِّ الرسائل التي تهمل عند المدخل. بينما العنصر ipOutDiscards يقوم بعدِّ الرسائل التي تهمل عند المخرج.
- حساب معدل الأخطاء Errors :يقوم العنصر ipAddrErrors بعد الرسائل التي تأتي إلى محطة التشغيل وبها مقدمة IP غير صحيحة Invalid IP Header.
- تأثير التجزئة IP Fragmentation على الأداء: يمكن لبعض عناصر مجموعة IP حساب الأخطاء التي تنتج من تجزئة IP وذلك بحساب النسبة المئوية ومعدلات رسائل داتاجرام المجزأة ، والأخطاء المصاحبة لها.

- تأثير المهملات على مصادر الشبكة:يعرفنا العنصر ipRoutingDiscards ما إذا كانت محطة التشغيل تقوم بإهمال مداخل تحديد مسار IP صالح valid أم لا.

- تحديد عدد المسارات غير الصحيحة:يقوم العنصر ipOutNoRoutes بعدِّ عدد المرات التي لا يوجد فيها مسار صحيحٌ لرسائل داتاجرام في محطة التشغيل.

- تأثير البروتوكول غير المعروف على مصادر الشبكة:عندما تضطر محطة التشغيل إلى معالجة عدد ضخم من رسائل داتاجرام، التي لا يوجد لها دعم محلي لبروتوكول الطبقة العليا Upper-Layer Protocol، الذي يتم قياسه بواسطة العنصر ipUnknownProtos ؛ فإن هذا ربما يسبب الاهتمام بالأداء.

- حساب معدل التراسل: يبين العنصر ipFolwDatagrams معدل التراسل Forwarding Rate للجهاز بالنسبة إلى رسائل IP داتاجرام.

عرضت الوحدة مجموعة عناصر بروتوكول رسائل تحكم الإنترنيت ICMP

- حساب عدد حزم بيانات ICMP المرسلة والمستقبلة ومعدلاتها لحساب النسبة المئوية لحزم بيانات ICMP المرسلة والمستقبلة الخاصة بالتطبيق؛ يجب أولا معرفة إجمالي عدد حزم بيانات ICMP المرسلة والمستقبلة بواسطة محطة التشغيل.

- حزم البيانات Redirect (المعاد توجيهها):ترسل حزم البيانات Redirect إلى مصدر رسائل داتاجرام IP، عندما ينبغي على محطة الاستقبال تحديد مسار رسالة داتاجرام IP خارجة من نفس الوحدة البينية التي تم استقبال الرسالة منها.

عرضت الوحدة كذلك مجموعة عناصر TCP الخاصة بإدارة التهيئة:

- تحديد تهيئة المسار بوساطة جعل التطبيق يستفسر عن العناصر التالية:
tcpRtoMax, tcpRtoMin, tcpRtoAlgorithm.

- حساب إجمالي عدد وصلات TCP: يمكن أن يساعدنا العنصر tcpMaxConn في تهيئة الشبكة لمعالجة عدد توصيلات TCP البعيدة الضرورية.

عرضت الوحدة مجموعة عناصر TCP الخاصة بإدارة الأداء.

– حساب عدد محاولات رفض reject الاتصال: يمكن أن تفشل محاولة تحقيق اتصال TCP لأسباب مختلفة، مثلا: ربما لا يوجد نظام الهدف، أو ربما يوجد عطل بالشبكة. يستخدم العنصرانtcpAttemptFails, tcpEstabResets لمساعدتنا في قياس معدل الرفض rejection rate في الشبكة.

– حساب عدد القطاعات Segments المعاد إرسالها:يبين العنصر tcpRetransSegs عدد قطاعات TCP التي يقوم النظام بإعادة إرسالها.

– حساب عدد مرات إعادة التشغيل: يعطي العنصر tcpOutRsts عدد المرات التي تقوم فيها محطة التشغيل بإجراء إعادة تشغيلreset اتصال.

قدمت الوحدة مجموعة عناصرTCP الخاصة بإدارة الحسابات:

– حساب عدد اتصالات TCP وفواتير الدفع:يبين العنصران tcpActiveOpens, tcpPassiveOpens إجمالي عدد مرات الاتصال من وإلى النظام، على الترتيب. ويبين العنصران tcpInSegs, tcpOutSegs عدد قطاعات TCP الداخلة والخارجة من محطة التشغيل على الترتيب. تكون هذه المعلومات ذات فائدة في حساب فواتير دفع مستخدمي الشبكة.

قدمت الوحدة كذلك عناصر مجموعة UDP الخاصة بإدارة الأداء:

– تحديد بعض مشاكل محطة التشغيل:يخبرنا العنصر udpNoPorts عن محطة تشغيل رسائل داتاجرام لتطبيق غير معروف أو تطبيق معروف لكن حاليا غير مشغل.

– إيجاد أخطاء محددة في الشبكة: يمكن أن يخبرنا العنصر udpInErrors عن أخطاء محددة في الشبكة.

ناقشت الوحدة عناصر مجموعة UDP الخاصة بإدارة الحسابات: حيث يمكن أن نستخدم العنصرين updOutDatagrams, udpInDatagrams لتحديد عدد رسائل داتاجرام UPD التي ترسلها وتستقبلها محطة التشغيل، على الترتيب.أما العنصر udpTable فهو يحدد المنافذ الحالية التي تقبل داتاجرام.

بينت الوحدة عيوب البروتوكول EGP ومعالجتها بواسطة BGP إن المشاكل الأساسية التي يعاني منها بروتوكول EGP أنه لا يستطيع اكتشاف العروات Loops التي تحدث في البروتوكول، كما أنه لا يحدد جدول المسارات routing ، فهو فقط يحدد معلومات إمكانية الوصول Reachability. كما أنه ليست لديه مقدرة التوسع scale up مع ازدياد حجم الشبكة. لهذه الأسباب توقف استخدام بروتوكول EGP مع تطور شبكات الإنترنيت، وقد حل محله البروتوكول BGP ، الذي عالج جميع المشاكل التي واجهها البروتوكول EGP .

وضحت الوحدة مجموعة بروتوكول CMOT توجد مجموعة CMOT ضمن قائمة عناصر مجموعات قاعدة المعلومات الإدارية MIB-II فقط لأسباب تاريخية.أما مجموعة عناصر الإرسال فهي تعطينا معلومات عن وسط محدد يعمل كوحدات بينية للنظام.

عرضت الوحدة عناصر مجموعة بروتوكولSNMP

المستخدمة في تطبيقات إدارة الأعطال. كل عنصر من هذه المجموعة يعطي معلومات عن أخطاء SNMP. تكمن حلول هذه الأخطاء غالباً، في التهيئة الخاصة بالمدير أو الوكيل SNMP .

مجموعة عناصر SNMP المستخدمة في تطبيقات إدارة الأداء، نوجد معدل حزم بيانات SNMP الداخلة والخارجة بواسطة العنصرين snmpInPkts, snmpOutPkts.

مجموعة عناصر SNMP المستخدمة في تطبيقات إدارة الحسابات، نجد فيها العناصر التالية : العنصر snmpInPkts لإجمالي دخل حزم سنمب ، العنصرsnmpOutPkts لإجمالي حزم سنمب المرسلة ، العنصر snmpInTraps لإجمالي دخل رسائل مصيدة، العنصر snmpOutTraps لإجمالي خرج رسائل مصيدة.

مجموعة عناصر SNMP المستخدمة في تطبيقات إدارة الأمن يقوم العنصر snmpInBadCommunityNames بعدّ عدد المرات التي يقوم فيها المستخدم أو

التطبيق بمحاولة الاتصال عن طريق بروتوكول SNMP في محطة التشغيل، ولا يعطي حروف المشاركة الصحيحة.

يستخدم العنصر snmpInBadCommunityUses لعدّ عدد مرات حزم بيانات SNMPالتي تستقبل فيها حروف مشاركة لا تسمح بتشغيل العملية المطلوبة.

لمحة مسبقة عن الوحدة التالية

عزيزي الدارس ،

الوحدة التالية تأتي متناولة قواعد المعلومات الإدارية MIB الخاصة برصد الشبكات عن بعد، وهما: RMON1, RMON2 وهذه القواعد المعلوماتية تعتبر امتدادا لقاعدة المعلومات الإدارية MIB-II المستخدمة في بروتوكولات SNMP.

إجابات التدريبات

تدريب (1)

عندما تقوم على محطة التشغيل بتخزين مؤقت Buffering لعدد ضخم من رسائل داتاجرام؛ فإن هذا يمكن أن يستهلك سعة الذاكرة. عندما تنفد الذاكرة المؤقتة لمحطة التشغيل، فإنها ربما تهمل مدخلات تحديد المسار routing entries ، لكي توفر ذاكرة مؤقتة أكثر. لكن مدخلات تحديد المسار التي تم إهمالها قد تكون ضرورية لإجراء عملية توصيل forward رسائل داتاجرام المخزنة في الذاكرة المؤقتة. ينبغي بعد ذلك ، على محطة التشغيل إعادة بناء مدخلات تحديد المسار التي سبق وأن أهملتها. وهذا بدوره يحتاج مصادر شبكة أكثر، أو إهمال رسائل داتاجرام المخزنة في الذاكرة المؤقتة بسبب نقص معلومات تحديد المسار.

مسرد المصطلحات

بروتوكول رسائل تحكم الإنترنيت ICMP

هو المسئول عن حمل تقارير الأخطاء ورسائل التحكم إلى أجهزة IP.

خوارزم جان جاكوبسون Jan Jacobson

هو خوارزم يستخدم في التحكم لتجنب حدوث اختناق شبكي.

بروتوكول UDP

يستخدم بروتوكول UDP في طبقة النقل Transport Layer، ويقوم بإرسال واستقبال رسائل داتاجرام Datagram بواسطة التطبيق.

بروتوكول EGP

يستخدم البروتوكول EGP في إخبار أجهزة شبكة IP عن إمكانية الوصول Reachability لشبكات IP الأخرى.

النظم المستقلة Autonomous Systems

هي عبارة عن شبكة واحدة، أو شبكات فرعية مصاحبة، أو تجميع شبكي مع شبكات فرعية تحت نفس الإدارة.

المصطلح بالإنجليزية	معناه بالعربية
Acknowledgement	شكر
Autonomous Systems	النظم المستقلة
Application Monitor	تطبيق المرصد
ARP (Address Resolution Protocol)	بروتوكول تحديد العنوان
BGP(Border Gateway Protocol)	بروتوكول مسارات الحدود
Billing	فواتير الدفع
Buffering	تخزين مؤقت
Broadcast Address	العنوان الإذاعي
Cache	ذاكرة
Congestion	اختناق
CMIP (Common Management Information Protocol)	بروتوكول معلومات الإدارة الشائع
CMIS (Common Management Services) Information	خدمات المعلومات الإدارية
CMOT (Common Management Information) Services Over TCP	بروتوكول خدمات المعلومات الإدارية الشائعة المحمل فوق طبقة النقل
Connectionless	غير اتصالي
Drastically	بقسوة
EGP(Exterior Gateway Protocol)	بروتوكول تحديد المسار الخارجي
Entire Route	المسار بكاملة
Expansion	توسع
Encapsulating	احتواء
Flow Control	تحكم التدفق

Foreign	أجنبي
Forwarded	الموجهة
Functionality	تشغيل
Forwarding Rate	معدل التراسل
Fragmentation	تجزئة
ICMP(Internet Control Message Protocol)	بروتوكول رسائل تحكم الإنترنيت
IP(Internet Protocol)	بروتوكول الإنترنيت
Installing	تنصيب
Intruder	مقتحم
Intrusion	مهاجمة
Invalid Header	مقدمة غير صحيحة
Lack of Resources	نقص المصادر
Listening Port	منفذ الإصغاء
Lost Segments	القطاعات المفقودة
Mapping	تحويلات
Metrics	مقاييس
Network reliability	اعتما دية الشبكة
News Servers	خادمات إخبارية
(NetBIOS)	نظام الدخل / الخرج الأساسي للشبكة
Out-of-date	قديمة
Outbound Interface	بينية الإرسال الخارج
Pop-Up Window	نافذة التحذير
Policy-Based-Reasons	أسباب نظامية

Reach ability	إمكانية الوصول
Redirect	معاد توجيهها
Rejection rate	معدل الرفض
Reset condition	شرط إعادة التشغيل
Routing entries	مدخلات تحديد المسار
Schemes	مخططات
Scale up	مقدرة التوسع
Server Listening	الخادم المصغي
Session	جلسة
Sub-net mask	قناع الشبكة الفرعية
Spikes	قمم
Stack	مركم
System Resources	مصادر النظام
Timers	محددات الأزمنة
TCP(Transport Control Protocol)	بروتوكول تحكم النقل
Group Transmission	مجموعة الإرسال
TFTP(Trivial File Transfer Protocol)	بروتوكول نقل الملفات العادي
UDP(User Datagram Protocol)	بروتوكول مستخدم داتاجرام
Unauthorized access	دخول غير مفوض
Upper-Layer Protocol	بروتوكول الطبقة العليا
Unfair	غير عادلة
Unreliable	فقيرة الاعتمادية
Unrestricted systems	نظم غير محظورة

المراجع

1- Formal specification of SNMP MIB's:
www.ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=770698.

2- A Closer Look at MIB-II (Essential SNMP):
www.unix.org.ua/orelly/networking_2ndEd/snmp/ch02_05.htm

3- Network Management: A Practical Perspective ,by Allan Leinwand, Karen Fang-Conroy. Info at Addison-Wesley, 1997.

4 - RFCs: Requests for Comments, http://ietf.org/rfc.html

5- IETF: The Internet Engineering Task Force,
http://www.ietf.cnri.reston.va.us/

6- mibDepot is an online SNMP MIB reference site,
http //www.mibdepot.com/index.shtml

7- Understanding SNMP MIBs: by David T. Perkins,
www.amazon.com/Understanding-SNMP-MIBs-David-Perkins/.

8- SNMP Tutorial Part 2: The Management Information Base (MIB)
www.dpstele.com/layers/l2/snmp_l2_tut_part2.php

9- SNMP MIB Resource www.snmplink.org/snmpresource/mib/

10- Reading the MIB Variable Descriptions
www.download-est.oracle.com/docs/


الوحدة السادسة
رصد الشبكات عن بعد
RMON1 and RMON2

محتويات الوحدة

المقدمة

تمهيد

عزيزي الدارس،

مرحباً بك في هذه الوحدة السادسة **من** مقرر" استخدام وإدارة الشبكات2". نشرح قواعد المعلومات الإدارية MIB الخاصة برصد الشبكات عن بعد وهما RMON1, RMON2، ويمكن أن نطلق عليهم بالعربية "رمون1، رمون2. وهذه القواعد المعلوماتية تعتبر امتدادا لقاعدة المعلومات الإدارية، MIB-II المستخدمة في بروتوكولات SNMP. وهي توفر معلومات مفيدة للغاية في جميع مجالات إدارة الشبكات. ويتناول القسم الأول من هذه الوحدة أجهزة رصد الشبكة عن بعد، أما القسم الثاني من الوحدة فيعدد أهداف قاعدة المعلومات الإدارية للرصد عن بعد، القسم الثالث من الوحدة يتناول مجموعة عناصر قواعد المعلومات الإدارية RMON1, RMON2، تُعين دراسة هذه الوحدة الدراسية، مهندسي الشبكات ومطوري البرمجيات في فهم وتطبيق هذه المعلومات لإدارة الشبكات بكفاءة ومهارة عالية. ويشمل ذلك: تطبيقات إدارة التهيئة، والأداء، والأعطال، والأمن، والحسابات.

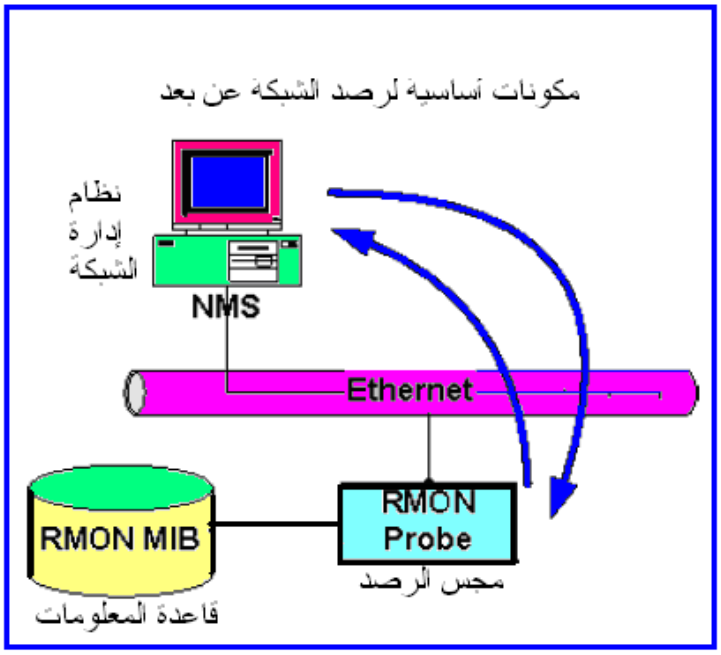
أهداف الوحدة

عزيزي الدارس، بعد فراغك من دراسة هذه الوحدة ينبغي أن تكون قادراً على أن:

- **تصف** بالرسم مكونات أجهزة رصد الشبكة عن بعد.
- **تعدد** أهداف قاعدة المعلومات الإدارية للرصد عن بعد.
- **تذكر** مجموعات عناصر قواعد المعلومات الإدارية RMON1, RMON2، وتبين الفرق بينهما.
- **تبين** وظائف مجموعة التاريخ ومجموعة الإنذار وإدارة الأداء واستخداماتها.
- **تشرح** باستخدام الأشكال مجموعة الحاسب المضيف واستخداماتها في إدارة الأداء والحسابات.
- تصف خصائص مجموعة القمة N للحاسب المضيف واستخداماتها.
- **تشرح** باستخدام الأشكال مجموعة المصفوفة وهيكلها البنائي، وتوضّح استخداماتها في فحص أداء الشبكات.
- **تصف** مجموعة المرشحات وهيكلها البنائي، وتصف استخداماتها في إدارة الشبكات عن بعد.
- **توضح** كيفية أداء مجموعة مسك الحزم ومجموعة الأحداث، وتبين استخداماتها.
- **تعدد** وظائف مجموعات قاعدة المعلومات الإدارية رمون-2، وتبين استخداماتها في إدارة الشبكات عن بعد.
- **تقارن** وتميز بين بروتوكولات SNMP، CMIP، RMON عند إدارة الشبكات.

1. أجهزة رصد الشبكة عن بعد

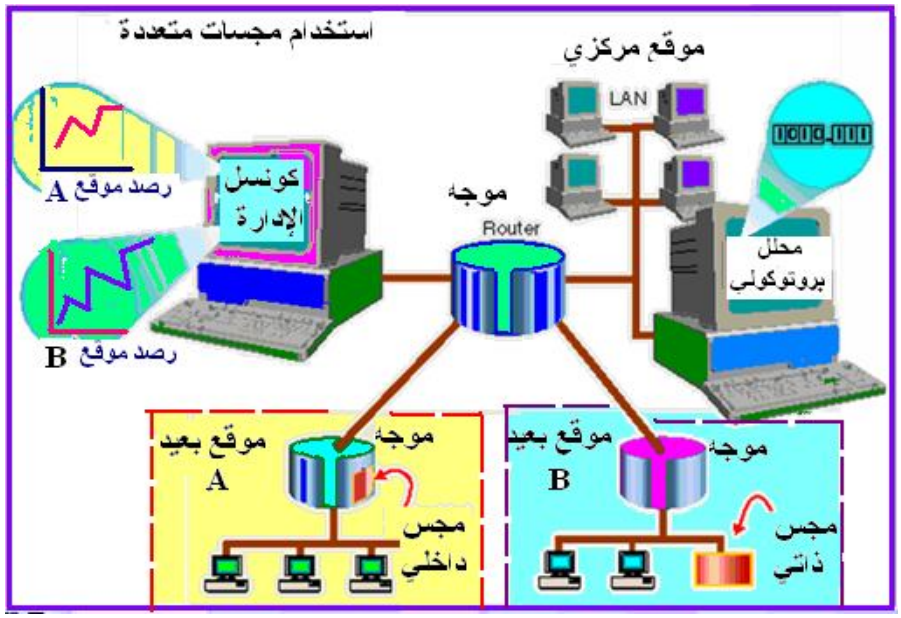
إن الغرض من جهاز رصد الشبكة عن بعد، هو المساعدة في إجراء عمليات إدارة الشبكة على قطاع شبكي Network Segment محدد. يوضع هذا الجهاز (أو المجس Probe) على قطاعات الشبكة. ويقوم برصد هذه القطاعات الشبكية وتجميع الإحصاءات. يوضح الشكل 6.1 المكونات الأساسية لرصد الشبكة عن بعد، وتشمل نظام إدارة الشبكة، جهاز الرصد (المجس)، وقاعدة المعلومات الخاصة بالرصد، و القطاع الشبكي لإيثرنيت، الذي يتم رصد بياناته.



شكل6.1 مكونات رصد الشبكة عن بعد.

يمكن أن يكون هذا المجس عبارة عن برنامج مشغل على حاسوب شخصي، أو جهاز الوكيل Agent، كما هو موضح في الشكل 6.2. يمكن أن يوجد بمجس الرصد وحدات بينية على قطاعات متعددة من الشبكة، ويستطيع المجس تجميع البيانات من كل قطاعٍ على حدة. كما يمكن أن يحتوي المجس على ذاكرة خاصة، ومعالج وبطاقة الشبكة

المخصصين لإجراء الوظائف الخاصة بإدارة الشبكة. يكون جهاز رصد الشبكة عن بعد مسئولا عن تجميع الإحصاءات المعرفة في قاعدة المعلومات الإدارية RMON MIB.

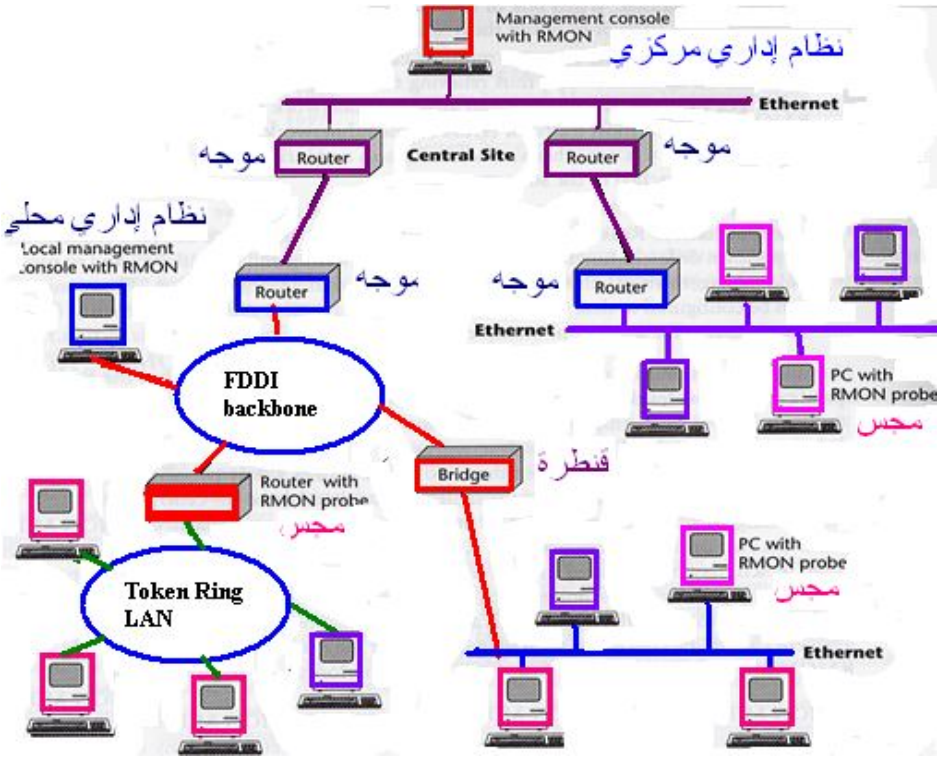


شكل6.2 موضع مجس الرصد في نظام رصد الشبكة عن بعد.

إن قاعدة المعلومات "رمون–ميب RMON-MIB"، تمت معايرتها standardized من أجل العمل على قطاعات الشبكات المحلية ايثرنيت، لكن هذا لا يمنع تقنيات الشبكات الأخرى من استخدامها. فقد تم توسعتها لتشمل إدارة شبكات مثل Token Ring، وشبكات FDDI ، كما هو موضح في الشكل6.3 .

يمكن للمؤسسة أن تضع جهاز رصد الشبكة عن بعد في كل قطاع شبكي، كما موضح في الشكل6.3.عند تطبيق هذه الطريقة، يستطيع مدير الشبكة المركزي تجميع الإحصاءات الخاصة بقاعدة معلومات "رمون–ميب" من كل قطاع شبكي. إن شراء جهاز مخصص لكل قطاع شبكي قد يكون مكلفا للعديد من المؤسسات. في بعض الحالات، عندما يوجد جهاز رصد شبكة عن بعد، من أجل الوصول لإدارة

الشبكة، ربما يوازن هذه التكلفة. يوجد العديد من هذه المنتجات متاحة في الأسواق مثل منتجات شركة برمجيات فرنتير Frantier ، وأرمون ARMON، وشركة أكسون Axon.



شكل6.3

1.1 مجس الرصد غير المحجوز NonDedicated

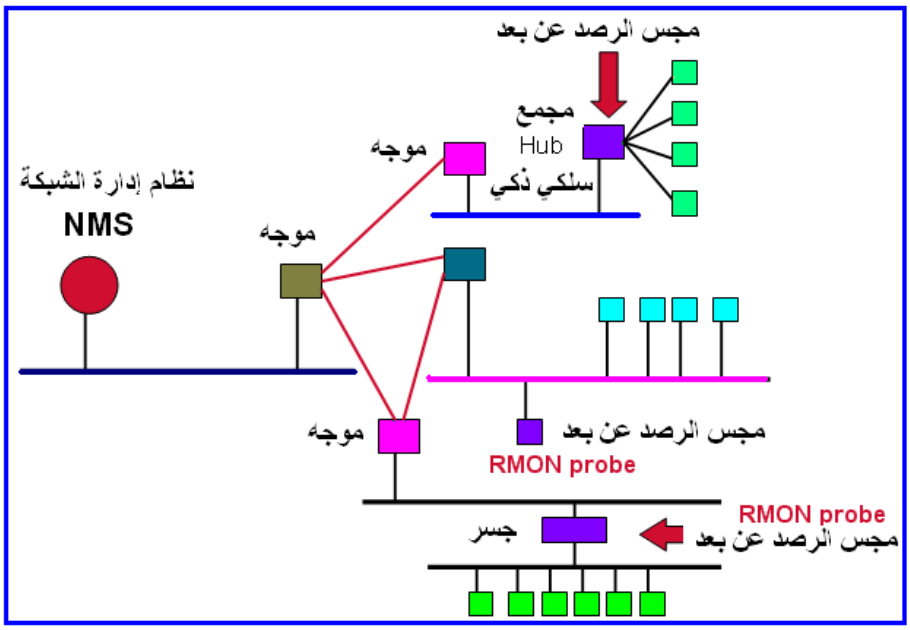
يوجد حل آخر، وهو شراء برنامج يستطيع إجراء رصد الشبكة عن بعد، بواسطة جهاز غير محجوز Nondedicated. حيث نستطيع شراء البرنامج للعديد من محطات العمل التي تستطيع إضافة رصد الشبكة عن بعد، ضمن وظيفة محطة العمل مثل منتجات شركة HP-NetMetrix. على الرغم من ذلك، فإن إجراء رصد الشبكة عن بعد يتطلب توفير وحدات بينية للجهاز تعمل في نمط الاختلاط Promiscuous، إلى الإصغاء لكل إطار في قطاع الشبكة. حيث يسمح هذا النمط من التشغيل ، بأن تقوم بطاقة الشبكة

بتمرير جميع حزم البيانات التي يستقبلها إلى المعالج، وليس فقط الحزم الخاصة بالعنوان الموجود بالوحدة MAC. ويمكن أن يؤدي ذلك إلى بطء أداء الوحدات البينية في محطات عمل الشبكة. وأن كل أجهزة الشبكة– تقريبا– سوف تعاني من تأثير الأداء عندما يتم وضع وحداتها البينية في نمط الاختلاط.

على سبيل المثال، يحتاج جهاز الموجّه أن يفحص فقط مقدمة الإطار في الايثرنيت لتحديد ما إذا كان يحتاج تحديد المسار Routing. لكن عندما يكون الموجه هو نفسه أيضا جهاز الرصد عن بعد – كما هو موضح في الشكل 6.3 – فقد يحتاج إلى فحص الإطار بكامله (لكل إطار) بغض النظر إن كان سيحدد له المسار أم لا.

2.1 المجمع السلكي الذكيIntelligent Wiring Hub

يوجد اختيار آخر من أجل رصد الشبكة عن بعد، وهو بوضع المجس الوظيفي داخل مجمع سلكي ذكيIntelligent Wiring Hub . مثل هذا المجمع متوفر في الأسواق. يوصل المجمع السلكي في نهاية النظم، ويتم وضع المجس في مكان مناسب. يوضح الشكل6.4، مجسات "رمون" مختلفة موزعة داخل قطاعات الشبكة. وكذلك يتضح فيه تسكين مجس الرصد داخل أجهزة الشبكة المتعددة، أو في وحدة بمفرده. ليس من الضروري أن يقوم مجس الرصد عن بعد، بتنفيذ كل عناصر قواعد المعلومات الإدارية الخاصة بالرصد. في الواقع، فإنه بخلاف قاعدة المعلومات الإدارية MIB-II، فإن المجس "رمون RMON" ، يمكن أن ينفذ فقط مجموعة مختارة أو مجموعات من عناصرRMON MIB ويظل محققا لمعايير قاعدة المعلومات.


مجس الرصد عن بعد
مجمع
Hub
سلكي ذكي
موجه
نظام إدارة الشبكة
NMS
موجه
موجه
مجس الرصد عن بعد
RMON probe
RMON probe
جسر
مجس الرصد عن بعد

الشكل6.4

أسئلة تقويم ذاتي

اختر الإجابة الصحيحة للجمل التالية:

مجس الرصد هو عبارة عن:

أ) برنامج يمكن تشغيله على جهاز الحاسب بالشبكة.

ب) برنامج يمكن تشغيله على جهاز الوكيل بالشبكة.

ج) برنامج يمكن تشغيله على جهاز الموجه بالشبكة.

د) أ و ب و ج .

هـ) لا شيء مما سبق.

يمكن توسعة قاعدة المعلومات الإدارية المستخدمة في رصد الشبكة المحلية عن بعد RMON-MIB للعمل في بيئة شبكات:

أ) ايثرنيت. ب) Token Ring

ج) FDDI د) أ ، ب ، ج.

هـ) لا شيء مما سبق.

تشمل المكونات الأساسية لرصد الشبكة عن بعد الأجهزة التالية:

أ)..... . ب) ..... .

ج) ..... . د) ..... .

اذكر وظيفة الأجهزة التالية عند رصد الشبكة عن بعد :

أ) مجس الرصد غير المحجوز Nondedicated .

ب) المجمع السلكي الذكي Intelligent Wiring Hub.

2. أهداف قاعدة المعلومات الإدارية للرصد عن بعد

يوجد خمسة أهداف رئيسية لقاعدة المعلومات الإدارية وهي:

أ- إجراء بعض العمليات دون الاعتماد على الاتصال بالشبكة Off-Line Operation.

ب- أخذ المبادرة بإجراء عملية الرصد Preemptive Monitoring.

ج- الكشف عن المشاكل وتدوينها Problem Detection and Reporting.

د- إتاحة بيانات القيمة المضافة Value-Added Data.

ه- توفير الدعم لمديرين متعددين Multiple Managers .

<u>ونشرح هذه الأهداف تباعا:</u>

1.2 إجراء بعض العمليات دون الاعتماد على الاتصال بالشبكة Off-Line Operation

يستطيع جهاز رصد الشبكة عن بعد توفير إجراءات بعض العمليات أثناء عدم الاتصال Offline بالشبكة. ويفيد هذا الهدف في الفترات التي عندها لا يمكن للجهاز أن يكون متصلاً بصفة مستمرة مع نظام إدارة الشبكة المركزي، حيث إنه في بعض الحالات لا يستطيع المجس الاتصال بمدير الشبكة المركزي، بسبب عطل في الشبكة، أو انقطاع Outage الشبكة. في حالات أخرى عندما يتم حساب تكاليف استخدام الشبكة؛ فإنه من المناسب أن يقوم مجس الرصد بالاتصال بالنظام المركزي، عندما يقع حادث حرج بالشبكة، وبذلك يتم توفير تكاليف الاتصال بالشبكة.

2.2 أخذ المبادرة بإجراء عملية الرصد Preemptive Monitoring

يستطيع مجس الرصد المعاونة في المبادرة بإجراء عملية الرصد على قطاع الشبكة بواسطة استمرار رصد القطاع، وإخبار نظام الإدارة المركزي في حالة وجود عطل.

يمكن ضبط مجس الرصد بإجراء تشخيص الأعطال بشكل مستمر ومراقبة أداء الشبكة. يمكن إرسال نتائج عمليات تشخيص الأعطال وتدوينها في سجل الأداء. عندما لا يوجد مشكلة، يمكن لمجس الرصد أن يوفر معلومات عن القطاع الشبكي قبل وبعد حدوث العطل.

3.2 الكشف عن المشاكل وتدوينها

Problem Detection and Reporting

إن عملية الكشف عن المشكلة وتدوينها، يمكن أن يتحقق بواسطة قيام مدير الشبكة بتهيئة مجس الرصد بأن يتذكر شروطاً معينة في القطاع، ويشمل ذلك الأخطاء. عندما يتحقق هذا الشرط، يقوم مجس الرصد بتسجيله، وإخبار نظام إدارة الشبكة. تساعد الخاصية لجهاز الرصد عن بعد، في تقليل كمية حركة مرور الرسائل بين نظام إدارة الشبكة المركزي وأجهزة القطاع. بسبب أن مجس الرصد يقوم برصد القطاع؛ فليس من الضروري أن يقوم نظام إدارة الشبكة بالقيام برصده أيضا.

4.2 إتاحة بيانات القيمة المضافة Value-Added Data

يمكن لمجس الرصد أن يوفر بيانات القيمة المضافة من أجل إدارة الشبكة. إن مجس الرصد هو جهاز يتم حجزه Dedicated لأجل الرصد، ومسموح له أن يقضي وقتا لتفسير Interpreting المعلومات حول القطاع الشبكي. على سبيل المثال، يستطيع مجس الرصد إيجاد قطاع الحواسيب المضيفة Hosts التي تولد معظم الأخطاء، أو معظم حركة الرسائل الإذاعية Broadcast Traffic . يستطيع المجس أيضا، تحديد الحواسيب المضيفة التي تقوم غالبا بإجراء عمليات الاتصال، ومتى تم ذلك. تكون هذه المعلومات ذات فائدة عظيمة في حل مشاكل الشبكة في القطاع.

5.2 توفير الدعم لمدرين متعددين Multiple Managers

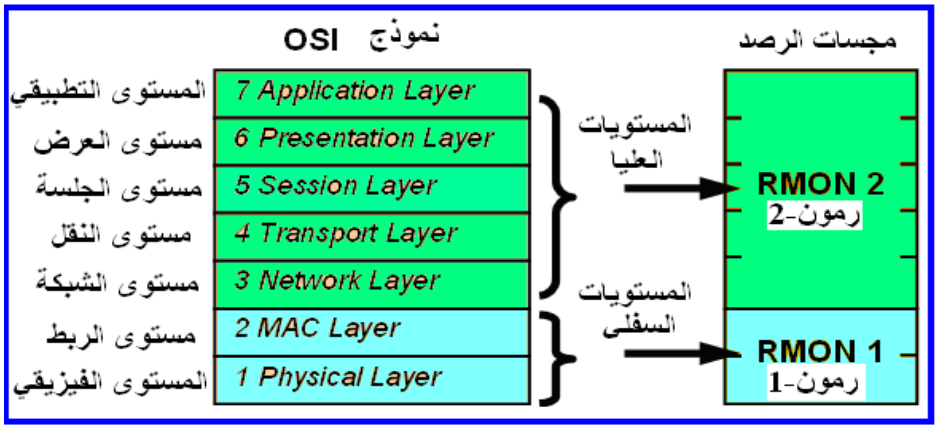
الهدف الأخير لجهاز الرصد عن بعد، هو توفير الدعم اللازم للعديد من المديرين. يوجد الكثير من المؤسسات بها نظم إدارة شبكات متعددة، التي تحتاج أن تستفسر عن عمليات الشبكة. يستطيع مجس الرصد عن بعد، الاستجابة لكل مديرين هذه المؤسسات، وتوفير بيانات القيمة المضافة، أو كشف المشكلة Problem Detection لكل مدير على حدة. في معظم الحالات، سوف يتطلب ذلك من مجس الرصد، أن يخصص مصادر لإجراء عملية الاتصال، لكل مدير على حدة.

أسئلة تقويم ذاتي

عدد أهداف قاعدة المعلومات الإدارية للرصد عن بعد.

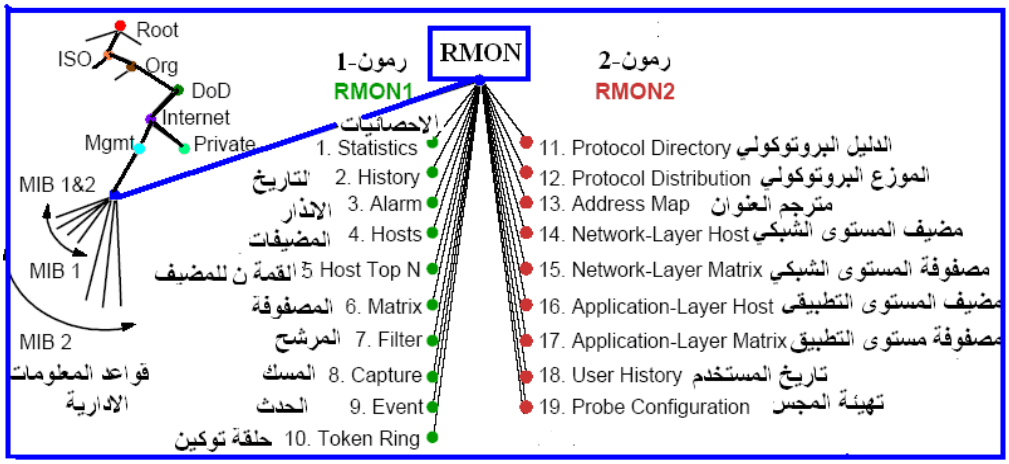
3. مجموعات عناصر قواعد المعلومات الإدارية RMON1, RMON2

تختص قاعدة المعلومات الإدارية "رمون-1 " بإدارة الشبكات المحلية، التي تتعامل فقط مع المستويين الأول والثاني في النظام المرجعي OSI، كما هو مبين في الشكل 6.5. وتختص قاعدة المعلومات الإدارية "رمون-2 RMON2 " بالتعامل مع إدارة المستويات العليا.



شكل6.5

يوضح الشكل6.6 قائمة مجموعة "رمون–1" ، و "رمون–2"، وموضعهما بالنسبة إلى مؤسسة المعايير الدولية ISO، و معايير IETF. وهما يحتويان على تسع عشرة مجموعة، مبينة أسماؤهم في الشكل6.6، والتي سيتم شرحها بالتفصيل تباعا في هذه الوحدة الدراسية.



شكل 6.6

1.3 مجموعة الإحصاءات Statistics Group

تحتوي مجموعة الإحصاءات على العناصر Objects التي يتم قياسها لكل وحدة بينية ايثرنيت في جهاز الرصد عن بعد. يتم حفظ الإحصاءات الخاصة ببينية ايثرنيت منفصلة عن البينيات Interfaces الأخرى. تسمح هذه الخاصية بأن يستطيع مجس الرصد توفير بيانات عن قطاعات عديدة، في نفس الوقت. تفيد هذه الإحصاءات في إجراء عمليات إدارة الأعطال، والتهيئة، والأداء.

إن كل بينية ايثرنيت Ethernet Interface، يخصص لها مجموعة إحصاءات منفصلة توضع في صف منفصل داخل جدول قاعدة المعلومات الإدارية، يسمى "جدول إحصاءات ايثرنيت etherStatsTable"، ويسمى كل صف فيه "مدخل إحصاءات ايثرنيت etherStatsEntry "، يتم تحديد الصف بواسطة رقم محدد هو" فهرس إحصاءات ايثرنيت etherStatsIndex"، كما هو موضح في الشكل 6.7 .

جدول المجموعات الإحصائية
etherStatsTable

etherStatsIndex فهرس إحصائيات ايثرنيت	etherStatsDataSource مصدر بيانات إحصائيات ايثرنيت	.....
1	ifIndex.1	.....
2	ifIndex.2	.....
3	ifIndex.4	.....
4	ifIndex.5	.....
5	ifIndex.10	.....
6	ifIndex.12	.....

كل صف يمثل مدخل إحصائيات ايثرنيت etherStatsEntry

شكل6.7 يوضح هيكلاً بنائياً مختصراً لمجموعة الإحصاءات.

1.1.3 عناصر مجموعة الإحصاءات الخاصة بإدارة الأعطال

تتيح مجموعة الإحصاءات عناصر كثيرة تساعدنا في عزل الأعطال في قطاع الشبكة، مع استخدام مجس الرصد. يبين الجدول 6.1 عناصر مجموعة الإحصاء التي تستخدم في تطبيق إدارة الأعطال.

جدول 6.1 عناصر مجموعة الإحصاء المستخدمة في إدارة الأعطال لشبكة ايثرنيت.

جدول عناصر مجموعة الإحصاء المستخدمة في إدارة الأعطال

رقم	Object العنصر	Information المعلومات
1	etherStatsDropEvents	عدد المرات التي يعاني فيها مجس رمون نقص في المصادر بسبب قلتها.
2	etherStatsBroadcastPkts	عزل المشاكل الإذاعية
3	etherStatsCRCAlignErrors	عزل قطاعات بها حزم لها أخطاء
4	etherStatsUndersizePkts	عزل قطاعات بها حزم أطوالها أقل.
5	etherStatsOversizePkts	عزل قطاعات بها حزم أطوالها أزيد.
6	etherStatsFragments	عزل قطاعات بها تقسيمات
7	etherStatsJabbers	عزل قطاعات بها جابرز (حزم أطول من 1518 حرف، هو أقصى طول حزمي في شبكة ايثرنيت).

يخبرنا عنصر الأحداث الساقطة etherStatsDropEvents عن عدد المرات التي تنفذ فيها مصادر مجس الرصد عن بعد، من أجل تحقيق أنشطته. وهذا الرقم لا يساوي عدد حزم البيانات الساقطة dropped أو غير المعالجة، لكنه يحدد عدد المرات التي يجد فيها المجس تحقق شرط المشكلة. عندما يزداد عنصر الأحداث الساقطة etherStatsDropEvents باستمرار، فقد نرغب في زيادة المصادر Resources للمجس أكثر، وذلك بزيادة ذاكرته أو إبعاد بعض الوحدات البينية للشبكة عن مجس الرصد المحجوز Dedicated. يمكن بعد ذلك، وضع هذه الوحدات البينية للشبكة في مجسات رصد جديدة مع المصادر التي تخصص لهما.

من المهم رصد العناصر المبينة في الجدول 6.1 عندما تتغير قيمة العنصر بنسبة أكثر من 2% مع الوقت. يمكن إجراء ذلك، دون استخدام مصادر كثيرة في مجس الرصد، أو سعة نطاق الشبكة. وذلك بواسطة إجراء عملية التصويت polling لهذه العناصر خلال فترات زمنية طويلة، مثلا كل عدد قليل من الساعات. عندما نلاحظ زيادة في أي عنصر، نستطيع استخدام مجس الرصد، لتجميع الإحصاءات وإرسال إنذار alarm لنظام إدارة الشبكة. بهذه الطريقة، يمكن تقليل optimize استعمال مجس الرصد، وتخصيص مصادره عند الضرورة فقط، لتحقيق إدارة الأعطال.

يبين الجدول 6.1 معلومات إحصائية أخري مفيدة للغاية، توضح استخدامات باقي عناصر المجموعة الإحصائية. من هذه العناصر: عنصر التقسيم etherStatsFragments ، حيث يبين أن الحزمة المقسمة أصبحت أقل من 64 حرفاً (وهو أقل طول إطار مسموح في ايثرنيت). وتنتج هذه المشكلة– عادة – بسبب وسط الاتصال، وينبغي عند حدوث ذلك أن يقوم مهندس الشبكة بفحص العتاد hardware في قطاع الشبكة.

أيضا، من هذه العناصر: عنصر جابرز etherStatsJabbers، وهو يبين لنا أن طول إطار بيانات في شبكة ايثرنيت، قد زاد عن قيمته العظمي المخصصة للشبكة وهي 1518 حرفاً. في هذه الحالة تقوم الشبكة بإرسال إشارة jabber عبر ايثرنيت. وينبغي على المحطة المرسلة أن ترى إشارة jabber عبر وصلة الأثير، وبعدها تبدأ الإرسال دون تخطي الطول المسموح للإطار.

2.1.3 عناصر مجموعة الإحصاءات الخاصة بإدارة التهيئة

تفيد عناصر المجموعة الإحصائية في تحقيق إدارة التهيئة، واستخداماتها. وهي تحتوي على عنصرين. يستخدم العنصر الأول: وهو عنصر "مصدر بيانات حالة ايثرنيت" etherStatsDataSource لبيان القطاع الشبكي الذي يقوم المجس برصده حالياً. و

العنصر الآخر هو "حالة المالك/المدير" etherStatsOwner، ويبين المدير الذي يقوم بتهيئة العناصر الموجودة في هذا الصف في مجس الرصد.

3.1.3 عناصر مجموعة الإحصاءات الخاصة بإدارة الأداء

يبين الجدول 6.2 قائمة عناصر مجموعة الإحصاءات الخاصة بإدارة الأداء، واستخداماتها.

مثال: نفترض الحالة التي يوجد فيها قنطرة في قطاع الشبكة. يوجد نظام "A" ، في نفس القطاع يقوم بالاتصال بالنظام "B" ، على الجانب الأخر من القنطرة، كما هو موضح في الشكل 6.7. يقوم أحد المستخدمين في النظام "A" بالاتصال ليشتكي من مشكلات بطء الأداء عند الوصول إلى النظام "B".

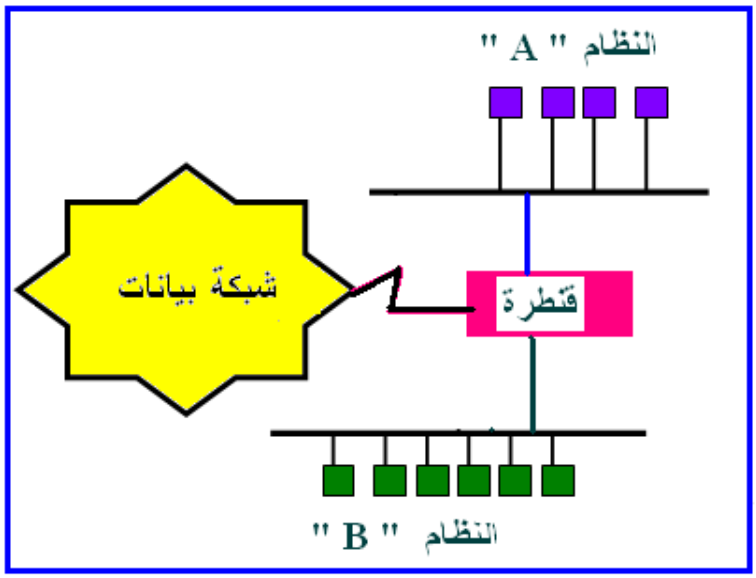
عندما نستخدم مجسات الرصد عن بعد لرصد معدل الاستخدام في كل قطاعات الشبكة، نجد أن معدل الاستخدام يكون 5%، وهو رقم معقول. بعد ذلك نقوم بفحص عدد المستخدمين والعمليات في كل نظام، ونجد أن كلاهما تقريبا في حالة توقف idle. نختبر الحمل Load عند القنطرة، ونجد أن معالجها له معدل استخدام كثيف. نفحص معدل حزم البيانات على كل قطاعات الشبكة، ونجد أنه مرتفع، ويصل تقريبا إلى 500 حزمة / ثانية. بعد ذلك، نستخدم إحصاءات إضافية في مجس الرصد، فنجد أن كل هذه الحزم تظهر في المدى من 65 إلى 127 بايت (حرف).

جدول 6.2

عناصر مجموعة الإحصائيات المستخدمة في إدارة الأداء

رقم	العنصر	الحسابات التي يقوم بها
1	etherstatsOctets	إجمالي معدل حركة المرور
2	etherstatsPkts	إجمالي معدل الحزم
3	etherstatsBroadcastPkts	معدل الحزم الإذاعية
4	etherstatsMulticastPkts	معدل الحزم متعددة الإذاعة
5	etherstatsPkts64Octets	معدل حزم 64 بايت
6	etherstatsPkts65to127Octets	معدل حزم 65-127 بايت
7	etherstatsPkts128to255Octets	معدل حزم 128-255 بايت
8	etherstatsPkts256to511Octets	معدل حزم 256- 511 بايت
9	etherstatsPkts512to1023Octets	معدل حزم 512-1023 بايت
10	etherstatsPkts1024to1518Octets	معدل حزم 1024-1518 بايت
11	etherstatsCRCAlignErrors	معدل أخطاء CRC
12	etherstatsUndersizePkts	معدل الحزم تحت الحجم
13	etherstatsOversizePkts	معدل الحزم فوق الحجم
14	etherstatsFragments	معدل التقسيم الحزمي
15	etherstatsJabbers	معدل وجود جابرز
16	etherstatsCollisions	معدل وجود تصادمات

باستخدام جهاز المحلل البروتوكولي Protocol Analyzer (أو خاصية رصد حزم البيانات عن بعد)، نجد أن حزم البيانات تنشئ شجرة اجتياز Spanning Tree ترسل إلى القنطرة، وتجعل جهاز المحلل البروتوكولي يتم إعادة حسابها لجدول إرسالها. أثناء إعادة هذه الحسابات لا تقوم القنطرة بإرسال حزم بنفس معدل التشغيل المعتاد بل تستمر بإجراء إعادة الحسابات. تنتج حزم البيانات الكثيرة لشجرة الاجتياز عن وصلة التوالي في القنطرة، حيث تنتقل من الحالة النشطة إلى الحالة غير النشطة بطريقة تكرارية. وهذا يؤدي إلى مشكلة الأداء بين النظام "A" والنظام "B". ونلاحظ أن معدل حزم البيانات المرتفع في القطاع ساعدنا في تشخيص أعطال هذه المشكلة.



شكل6.7 تم إعداد الشبكة بواسطة توصيل النظامين A, B عن طريق قنطرة.

- **حساب معدل الاستخدام في القطاع:**

يمكن حساب معدل الاستخدام Utilization للقطاع بين فترات زمنية x, y كما يلي:

Utilization

Totalbytes= ($etherStatsOctets_y$ - $etherStatsOctets_x$)/(y-x)

U = Totalbytes / ifSpeed

- **حساب معدل الأخطاء في القطاع:**

يمكن حساب معدل الأخطاء في القطاع بين فترات زمنية x, y كما يلي:

$$\begin{aligned}Total\text{-}errors = &(etherstatsCRCAlignErrors\ at\ y \\ &- etherstatsCRCAlignErrors\ at\ x) \\ &+ (etherstatsUndersizePkts\ at\ y \\ &- etherstatsUndersizePkts\ at\ x) \\ &+ (etherstatsOversizePkts\ at\ y \\ &- etherstatsOversizePkts\ at\ x) \\ &+ (etherstatsFragments\ at\ y \\ &- etherstatsFragments\ at\ x) \\ &+ (etherstatsJabbers\ at\ y \\ &- etherstatsJabbers\ at\ x)\end{aligned}$$

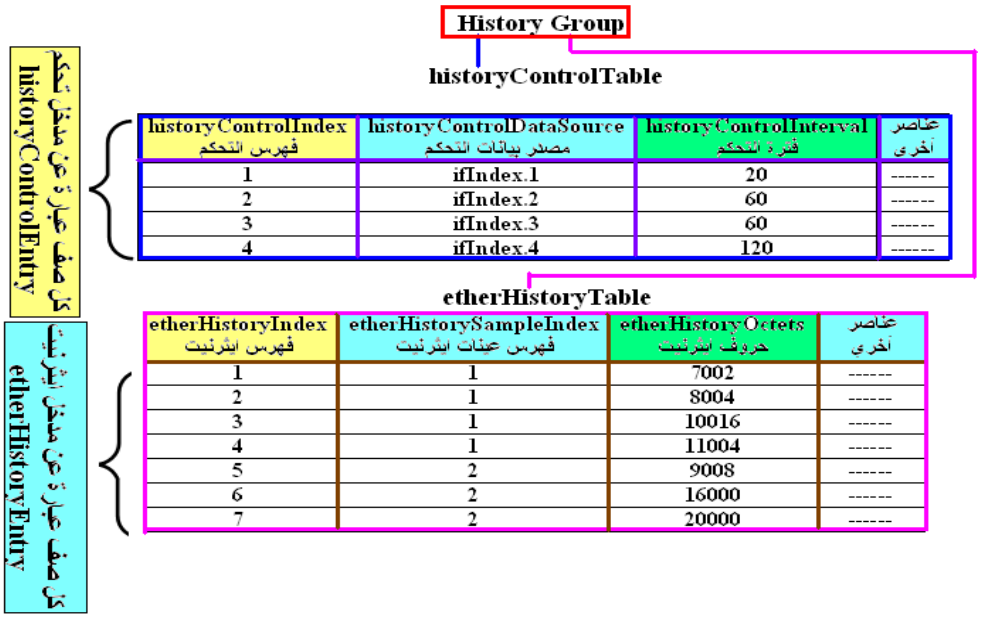
$$Error\ Percentage = Total\text{-}errors \,/\, (etherStatsPkts\ at\ y - etherStatsPkts\ at\ x)$$

- **حساب النسبة المئوية للتصادم Collision :**

$$\begin{aligned}Collision\ Percentage = &(etherstatsCollisions\ at\ y - etherstatsCollisions\ at\ x) \,/ \\ &(etherstatsCollisions\ at\ y - etherstatsCollisions\ at\ x) + \\ &(etherstatsPkts\ at\ y - etherstatsPkts\ at\ x)\end{aligned}$$

2.3 مجموعة التاريخ History Group

تساعد مجموعة التاريخ مهندس الشبكة في أخذ عينات إحصائية دورية من القطاع الشبكي وتخزينها داخل مجس الرصد ، لاستخدامها فيما بعد عند إجراء عمليات التحليل. تتكون عناصر مجموعة التاريخ من جدول التهيئة اللازم لتحديد العينات، وجدول تحديد الوسط الذي يخزن العينات فور الحصول عليها. يوضح الشكل6.8 الهيكل البنائي لمجموعة التاريخ. لاحظ أنه ليست كل العناصر تم ذكرها في الرسم.



الشكل6.8 الهيكل البنائي لمجموعة التاريخ.

يبين الجدول6.3 عناصر مجموعة التاريخ التي تفيد في تطبيقات تحقيق الأداء وفائدة كل عنصر منها.

الجدول6.3 عناصر مجموعة التاريخ

عناصر مجموعة التاريخ المستخدمة في إدارة الأداء

رقم	العنصر	الحسابات التي يقوم بها
1	etherHistoryOctets	إجمالي معدل حركة المرور
2	etherHistoryPkts	إجمالي معدل الحزم
3	etherHistoryBroadcastPkts	معدل الحزم الإذاعية
4	etherHistoryMulticastPkts	معدل الحزم متعددة الإذاعة
5	etherHistoryCRCAlignErrors	معدل أخطاء CRC
6	etherHistoryUndersizePkts	معدل الحزم تحت الحجم
7	etherHistoryOversizePkts	معدل الحزم فوق الحجم
8	etherHistoryFragments	معدل التقسيم الحزمي
9	etherHistoryJabbers	معدل وجود جابرز
10	etherHistoryCollisions	معدل وجود تصادمات
11	etherHistoryUtilization	معدل الاستخدام

3.3 مجموعة الإنذار Alarm Group

تفيد مجموعة الإنذار في إدارة الأداء. حيث تسمح لنا هذه العناصر بتعريف الحدود threshold لقاعدة المعلومات الإدارية خلال مدة زمنية. بعد ذلك، يقوم مجس الرصد بأخذ عينات من هذا العنصر خلال المدة الزمنية التي تم تحديدها، ويقوم بمقارنة هذه القيم مع القيم الحدية threshold. يمكن ضبط القيم الحدية لأي عنصر في قاعدة المعلومات الإدارية التي تقابل قيمة عددية، مثل العداد counter. على سبيل المثال، قد نحتاج ضبط القيم الحدية لمراقبة عدد الأخطاء "X" التي قد تحدث خلال مدة زمنية عشرة دقائق. عندما تزيد القيم الحدية عن الحد المسموح، تقوم مجموعة الإنذار بتخصيص وسيلة لتوليد حدث event.

تعرف القيم الحدية إما بالصعود rising، أو بالهبوط falling. إن القيم الحدية الصاعدة، هي التي تحدث عندما تزيد القيمة التي تم رصدها، بينما القيمة الحدية الهابطة، تحدث عندما تقل القيمة التي تم رصدها. إن ميزة استخدام قيمتين حديتين هو تقليل عدد الإنذارات الخاصة بإدارة الأداء.

1.3.3 عناصر مجموعة الإنذار الخاصة بإدارة الأداء

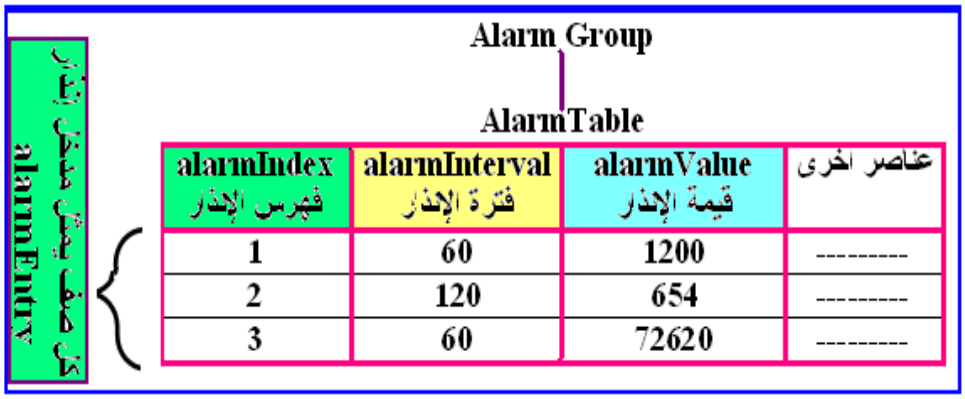
يلخص الجدول6.4 عناصر مجموعة الإنذار التي تفيد في تحقيق إدارة الأداء. تحتوي هذه المجموعة على جدول واحد، يسمى جدول الإنذار alarm-Table. يسمح هذا الجدول لمهندس الشبكة بأن يقوم بضبط الإنذار

الجدول6.4

عناصر مجموعة الإنذار المستخدمة في إدارة الأداء

Serial	object العنصر	Information المعلومات
1	alarmInterval	تحديد فترة رصد عينة العنصر
2	alarmVariable	تحديد قاعدة MIB للعنصر لأجل العينة
3	alarmSampleType	تحديد كيفية تفسير قيم العينة
4	alarmValue	يعطي القيمة الحالية لعينة العنصر
5	alarmStartupAlarm	تحديد كيفية تفسير القيمة عندما يبدأ الإنذار
6	alarmRisingThreshold	تحديد الحد الصاعد
7	alarmFallingThreshold	تحديد الحد الهابط
8	alarmRisingEventIndex	تحديد الحدث عندما يتم تخطي الحد الصاعد
9	alarmFallingEventIndex	تحديد الحدث عندما يتم تخطي الحد الهابط

كل صف في الجدول يسمى مدخل الإنذار alarmEntry. كل مدخل إنذار يحتوي على رقم مميز مصاحب له يسمى فهرس الإنذار alarmIndex ، كما هو موضح في الشكل6.9 .



شكل 6.9 الهيكل البنائي لمجموعة الإنذار – لا يظهر الرسم كافة العناصر.

يتم تحديد الفترة الزمنية بالثانية بواسطة العنصر alarmInterval. وهي المدة التي ينبغي أن يقوم فيها مجس الرصد بمقارنة عينة البيانات بالقيم الحدية. يحتوي العنصر alarmVariable على هوية عنصر ASN.1 للعنصر الذي يتم أخذ عينته.

كما يستطيع الإنذار أن يولد حدثاً an Event، وذلك عندما يتم تخطي القيمة الحدية سواء أكان ذلك في حالة الصعود، أو في حالة الهبوط. بينما يقوم عنصر "تخطي الحد الصاعد" alarmRisingEventIndex، بتحديد العنصر الذي يتم توليده، عندما يتم تخطي القيمة الحدية الصاعدة، يقوم عنصر "تخطي الحد الهابط" alarmFallingEventIndex، بتوليد العنصر المناظر عند تخطي القيمة الحدية الهابطة. يبين الجدول6.4، باقي استخدامات عناصر مجموعة الإنذار الخاصة بإدارة الأداء ووظائفها.

أسئلة تقويم ذاتي

1. قارن بين مجموعات عناصر قواعد المعلومات الإدارية RMON1, RMON2 من حيث الاستخدام.

2. اشرح طريقة استخدام عناصر مجموعة الإحصاءات في كل من:

أ) إدارة أعطال الشبكة. ب) إدارة أداء الشبكة. ج) إدارة تهيئة الشبكة.

اختر الإجابة الصحيحة:

3. يمكن استخدام مجموعة التاريخ History Group لقاعدة رمون-1 في:

أ) أخذ عينات إحصائية دورية من قطاع شبكة محلية.

ب) تخزين العينات التاريخية داخل مجس الرصد.

ج) استخدام العينات التاريخية في عمليات تحليل الشبكة.

د) كل ما سبق.

هـ) لا شيء مما سبق.

4. تفيد مجموعة الإنذار Alarm Group لقاعدة رمون-1 في:

أ) إدارة الأداء في قطاع شبكة محلية.

ب) ضبط القيم الحدية خلال مدة زمنية.

ج) تخصيص وسيلة لتوليد حدث event، عند تخطي القيم الحدية.

د) لا شيء مما سبق.

هـ) أ ، ب ، ج .

5. باستخدام عناصر مجموعة الإحصاءات، اكتب المعادلات اللازمة لحساب ما يلي:

أ) معدل الاستخدام لقطاع شبكة محلية ايثرنيت.

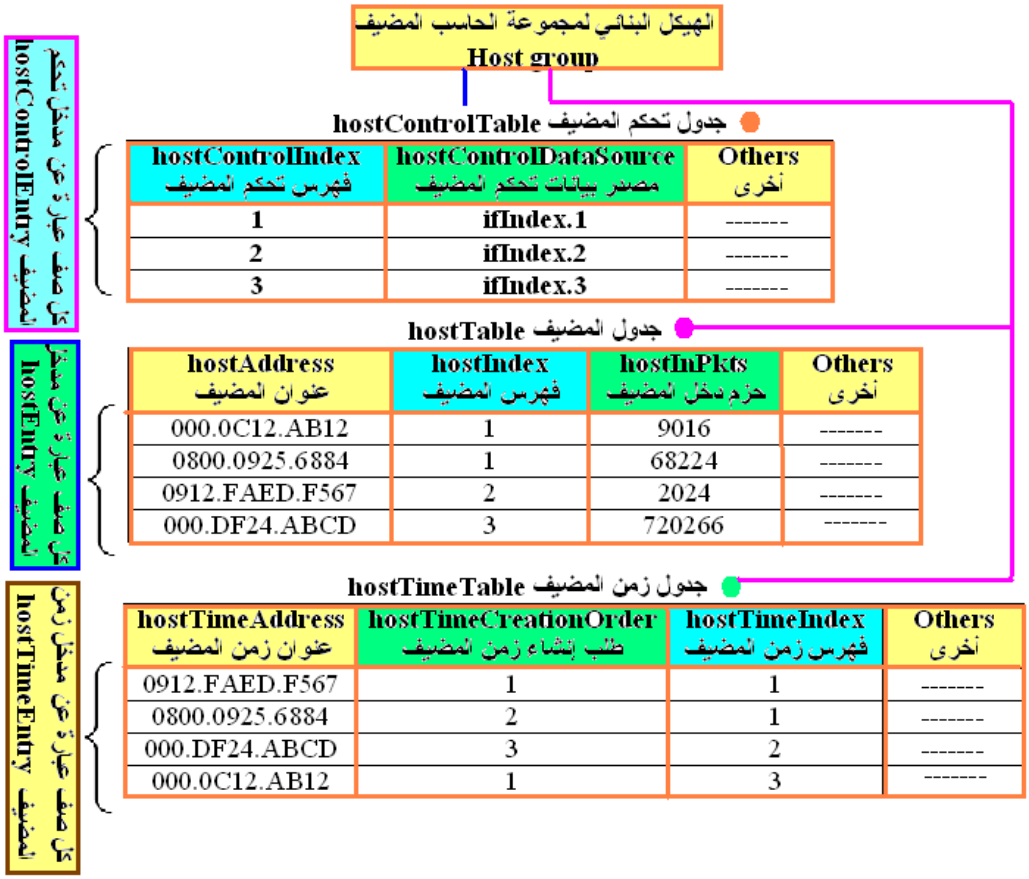
ب) معدل الأخطاء في قطاع شبكة محلية ايثرنيت.

ج) النسبة المئوية لتصادم الرسائل لقطاع شبكة محلية ايثرنيت.

4.3 مجموعة الحاسوب المضيف Host Group

تحتوي مجموعة الحاسوب المضيف على العناصر المصاحبة للحاسوب المضيف لقطاع الشبكة، حيث يتم وضع مجس الرصد. يكتشف مجس الرصد الحواسيب المضيفة في الشبكة، بواسطة تتبع الوسط لكل من المصدر والهدف. من خلال عناوين تحكم الوصول MAC الموجودة في القطاع، يستطيع مجس الرصد رؤية جميع حزم البيانات في قطاع الشبكة، لأن وحداته البينية تعمل في نمط التشغيل المختلط Promiscuous.

تتكون عناصر مجموعة الحاسوب المضيف من جدول تحكم لاكتشاف الحواسيب المضيفة، وجدول الإحصاءات عن كل حاسوب مضيف يتم اكتشافه، وقائمة الطلبات الزمنية time-ordered لإحصاءات الحاسوب المضيف، كما هو موضح في الشكل6.10.يتم تحديد جدول تحكم الوحدات البينية للحاسوب المضيف المكتشف الذي يقوم مجس الرصد بتنفيذه.



الشكل6.10 هيكل بنائي مختصر لمجموعة الحاسوب المضيف

يتم تخزين جدول الإحصاءات بناء على الحواسيب المضيفة (per-hosts)، يتم تخزين جدول الطلبات الزمنية للحاسوب المضيف بناءً على طلبات الإحصاءات، حسب الوقت (per Time). تفيد عناصر مجموعة الحاسوب المضيف، في تطبيقات إدارة التهيئة، والحسابات، والأداء. وفيما يلي سوف نتناول شرح عناصر مجموعة الحاسوب المضيف المستخدمة في تطبيق إدارة الأداء، وإدارة الحسابات.

1.4.3 عناصر مجموعة الحاسوب المضيف الخاصة بإدارة الأداء

يبين الجدول6.5 قائمة عناصر مجموعة الحاسوب المضيف الخاصة بإدارة الأداء، ووظيفة كل عنصر.

جدول6.5

عناصر مجموعة الحاسب المضيف المستخدمة في إدارة الأداء

Serial	object العنصر	Information المعلومات
1	hostInPkts	معدل الحزم الداخلة
2	hostOutPkts	معدل الحزم الخارجة
3	hostInOctets	معدل الحروف الداخلة
4	hostOutOctets	معدل الحروف الخارجة
5	hostOutErrors	معدل الأخطاء المرسلة
6	hostOutBroadcastPkts	معدل الحزم الإذاعية المرسلة
7	hostOutMulticastPkts	معدل الحزم متعددة الإذاعة المرسلة

يمكن حساب النسبة المئوية لحركة مرور حزم البيانات لكل حاسوب مضيف كما يلي:

```
Host Percentage = (hostInOctets at y - hostInOctets at x)
                + (hostOutOctets at y - hostOutOctets at x)
                / (etherStatsOctets at y - etherStatsOctets at x)
```

يمكن بالمثل، حساب النسبة المئوية لمعدل الأخطاء التي تنشأ في قطاع الشبكة، وهذا يساعد مهندس الشبكة بعزل الحواسيب المضيفة التي تقوم بإرسال هذه الأخطاء.

2.4.3 عناصر مجموعة الحاسوب المضيف الخاصة بإدارة الحواسيب

يبين الجدول6.6 قائمة عناصر مجموعة الحاسوب المضيف الخاصة بإدارة الحسابات، ووظيفة كل عنصر.

جدول6.6

عناصر مجموعة الحاسب المضيف المستخدمة في إدارة الحسابات

Serial	object العنصر	Information المعلومات
1	hostInPkts	عدد الحزم الداخلة
2	hostOutPkts	عدد الحزم الخارجة
3	hostInOctets	عدد الحروف الداخلة
4	hostOutOctets	عدد الحروف الخارجة
5	hostOutBroadcastPkts	عدد الحزم الإذاعية المرسلة
6	hostOutMulticastPkts	عدد الحزم متعددة الإذاعة المرسلة

تختص عملية إدارة الحسابات بعدّ الحزم والحروف لكل حاسوب مضيف. عندما تقرر المؤسسة تطبيق إدارة الحسابات بحسب عدد الحزم المرسلة أو المستقبلة، فإن العناصر التالية ستعطي المعلومات اللازمة لكل حاسوب مضيف:

hostInPkts, hostOutPkts, hostOutBroadcastPkts, and hostOutMulticastPkts.

بالمثل، عندما تقرر المؤسسة تطبيق نظام إدارة الحسابات بناء على عدد الحروف المرسلة والمستقبلة، فإن العناصر التالية ستعطي المعلومات اللازمة لكل حاسوب مضيف:

hostInOctets, and hostOutOctets.

عندما يقرر تطبيق إدارة الحسابات أنه يحتاج الاستفسار عن كل حاسوب مضيف في قطاع الشبكة، يمكنه أن يستفسر من مجس الرصد عن بعد، عن جميع الإحصاءات الضرورية.

5.3 مجموعة القمة N للحاسوب المضيف Host-Top N

تستخدم مجموعة القمة N للحاسوب المضيف نفس العناصر الموجودة في مجموعة الحاسوب المضيف، وذلك لتجهيز تقارير لإعداد الحواسيب المضيفة خلال مدة زمنية معلومة. يتم تجهيز هذه التقارير على أساس الإحصاء الذي تم تحديده بواسطة نظام إدارة الشبكة.

يمكن ضبط القاعدة الإحصائية Base Statistic لتقوم بتدوين إحصاءات الحاسوب المضيف لإيجاد القيم العليا للعدد N ؛(top N)؛ لحزم البيانات المرسلة والمستقبلة، أو الحروف المرسلة والمستقبلة، أو الأخطاء، أو الإذاعيات، أو الحزم متعددة الإذاعة المرسلة. يقوم النظام الإداري أيضاً، بإعلام مجس الرصد عن مدة التقرير، وعدد الحواسيب المضيفة في كل تقرير. إن عدد الحواسيب المضيفة المتغير في كل تقرير، يمثل الاسم المصدري لهذه المجموعة، لأن قيمة العدد N للحواسيب المضيفة تنشئ التقرير بناء على الإحصاءات المستخدمة من مجموعة الحاسوب المضيف، وأن كل عناصر هذه المجموعة تطبق في كل من إدارة الأداء، وإدارة الحواسيب.

مثال: نفترض أن مهندس الشبكة يريد تحديد قيمة عشرة حواسيب مضيفة، لتحديد حجم حركة المرور Traffic Volume ، لكامل شبكة البيانات لغرض إدارة الحسابات. يقوم مهندس الشبكة بتجميع الحواسيب المضيفة العشرة التي تستقبل وترسل الحروف لكل قطاع شبكي، مستخدما مجسات الرصد عن بعد، بعد ذلك يقوم المهندس باستخدام بروتوكول إدارة الشبكة لإحضار هذه المعلومات إلى قاعدة البيانات العلاقية SQL في نظام إدارة الشبكة.

باستخدام قاعدة البيانات العلاقية، يتم تصنيف البيانات، وإنشاء تقرير يوضح الحاسب المضيف الذي يستقبل أقصى عدد حروف من الشبكة، وذلك بواسطة الأمر التالي:

```
SELECT   hostname, bytes-sent, bytes-received
FROM rmon-data SORT By bytes-received
```

يفترض تطبيق هذا الأمر، وجود جدول قاعدة بيانات يسمى ***rmon-data***. يحتوي على عمود بأسماء الحواسيب المضيفة ***hostname***. وإجمالي عدد الحروف المرسلة ***bytes-sent*** بواسطة الحاسب المضيف. وإجمالي عدد الحروف المستقبلة ***bytes-received*** بواسطة الحاسب المضيف.

تحتوي مجموعة القمة N للحاسب المضيف على جدولين، الجدول الأول هو hostTopNControlTable، الذي يسمح لنظام إدارة الشبكة بإعداد التقرير.

والجدول الثاني هو hostTopNTable، والذي يتم فيه وضع نتائج التقرير. كما هو موضح في الشكل6.11 .

الهيكل البنائي لمجموعة القمة N للمحاسبات المضيفة
hostTopN group

جدول تحكم القمة N للمضيف
hostTopNControlTable

كل صف عبارة عن مدخل تحكم
hostTopNControlEntry

hostTopNControlIndex فهرس تحكم القمة N	hostTopNHostIndex فهرس مضيف القمة N	hostTopNRateBase قاعدة معدل القمة N	--
1	1	hostTopNOutErrors القمة N لأخطاء الخرج	-
2	1	hostTopNOutOctets القمة N لحروف الخرج	-
3	2	hostTopNOutBroadcastPkts القمة N لخرج الحزم الإذاعية	-

جدول القمة N للمضيف
hostTopNTable

كل صف عبارة عن مدخل
hostTopNEntry

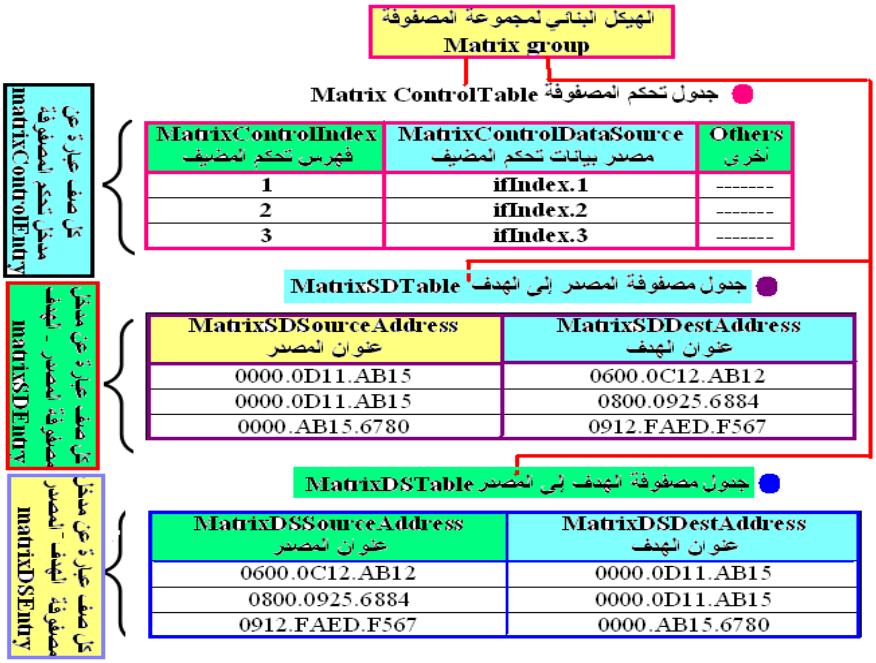
hostTopNReport تقرير القمة N	hostTopNIndex فهرس القمة N	hostTopNAddress عنوان مضيف القمة N	hostTopNRate معدل القمة N
1	1	0800.0925.6884	0
1	2	0912.FAED.F567	50
2	1	000.DF24.ABCD	1100

شكل6.11 هيكل بنائي مختصر لمجموعة القمة N للحاسب المضيف.

6.3 مجموعة المصفوفة Matrix Group

تحتوي مجموعة المصفوفة على جدول العناصر الذي يحفظ الإحصاءات عن عدد الحزم والحروف والأخطاء المرسلة بين عناوين في القطاع الشبكي. يقوم مجس الرصد بتكوين هذه الجداول بواسطة فحص المصدر والهدف لعناوين MAC الموجودة في حزم بيانات القطاع. يقوم المجس بحفظ جدولين، الأول من المصدر إلى الهدف، والثاني من الهدف إلى المصدر. يمكن أن تساعدنا المعلومات الموجودة في المصفوفة في تحديد نماذج حركة مرور البيانات في قطاع الشبكة. وذلك بجعل هذه البيانات مفيدة ومتاحة في إدارة الأداء، وإدارة الحواسيب، وإدارة الأمن.

تنقسم مجموعة المصفوفة إلى ثلاثة جداول، هي: جدول التحكم، وجدول حركة مرور البيانات من المصدر إلى الهدف، وجدول حركة مرور البيانات من الهدف إلى المصدر.، كما هو موضح في الشكل 6.12.



شكل6.12 هيكل بنائي مختصر لمجموعة المصفوفة.

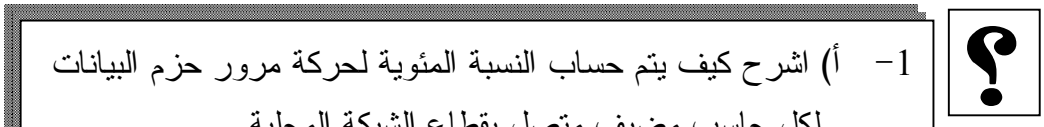
يتحكم الجدول matrixControlTable في عمليات مجموعة المصفوفة. كل صف في هذا الجدول يمثل مدخلاً للجدول matrixControlEntry. يمكن أن يوجد في مجس الرصد مداخل صفوف عديدة في الجدول، بسبب أن المجس قد يوجد به بعض الوحدات البينية الخاصة بتجميع عناصر مجموعة المصفوفة.

مثال: نفترض أن بعض المستخدمين في قطاع الشبكة المحلية يعانون من بطء الأداء في القطاع، ويرغب مستخدموا هذه الشبكة في تركيب جهاز شبكي مثل القنطرة، أو مفتاح، أو موجِّه، لتقسيم القطاع إلى مناطق أصغر بهدف تحسين أداء الشبكة. يقوم مهندس الشبكة بفحص بيانات مجموعة المصفوفة، لتحديد ما إذا كان عملية إضافة الجهاز في قطاع الشبكة سوف يحسن فعلا الأداء أم لا. إنه من المفيد أولاً، تحديد ما إذا كانت

الحواسيب المضيفة في القطاع تتخاطب مبدئيا مع بعضها أو ما إذا كانت حركة مرور البيانات يتجه معظمها إلى قطاع أخر.

يمكن أن يستخدم مهندس الشبكة الجدول matrixSDtable (والجدول المناظر matrixDStable) لإيجاد هذه المعلومات. عندما يوجد جزء كبير من حركة مرور البيانات من الحواسيب المضيفة إلى القطاع لا يتجه إلى قطاع آخر، فإن عملية تقسيم القطاع إلى مناطق أصغر يكون لها أحقية متساوية للدخول إلى جهاز الشبكة الذي يوصل إلى القطاع الآخر، يكون معقولا. عندما يوجد جزء كبير من حركة المرور يظل داخل القطاع ويتجه إلى حاسب مضيف واحد (مثلاً جهاز الخادم)، فإن توفير سعة نطاق إضافية إلى الخادم قد يكون معقولاً. في حالة أخرى، إذا تم توزيع حركة مرور البيانات بشكل عادل بين جميع الحواسيب المضيفة في القطاع وظل الأداء ضعيفا؛ يكون من المعقول استخدام وسط ذي سرعة أعلى، أو توفير مسارات متوازية عديدة بين الحواسيب المضيفة. بغض النظر عن اتخاذ قرار تصميم الشبكة، لتحسين أداء القطاع، فإن البيانات من الجدول matrixSDtable سوف تكون ذات فائدة كبيرة لمهندس الشبكة.

أسئلة تقويم ذاتي



1- أ) اشرح كيف يتم حساب النسبة المئوية لحركة مرور حزم البيانات لكل حاسب مضيف متصل بقطاع الشبكة المحلية.

ب) اذكر مسميات عناصر مجموعة الحاسب المضيف، التي يمكن استخدامها في إدارة الحسابات لشبكة أحد المؤسسات.

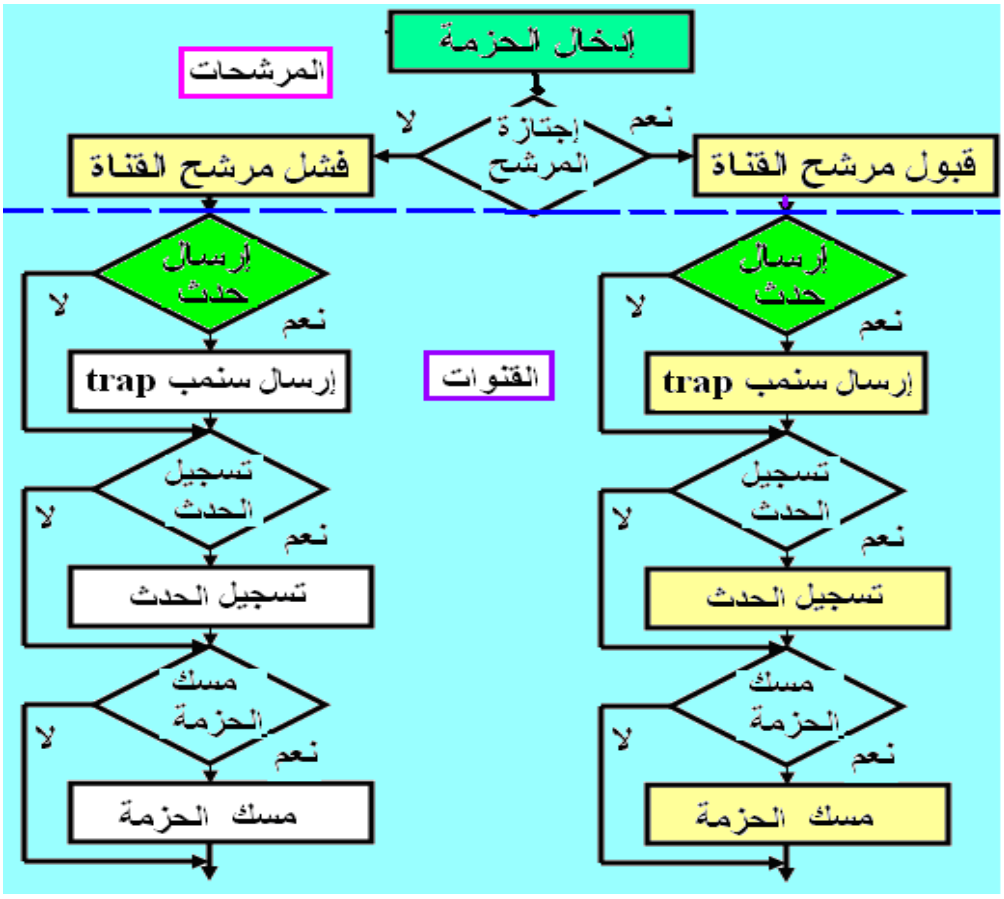
2- اذكر وظيفة ما يلي، مع إعطاء مثال توضيحي مبسط :

أ) مجموعة القمة N للحاسب المضيف.

ب) مجموعة المصفوفة Matrix Group.

7.3 مجموعة المرشح Filter Group

تساعد مجموعة المرشح مهندس الشبكة بأن يستخدم مجس الرصد عن بعد، لفحص حزم بيانات محددة في قطاع الشبكة. يتم تهيئة المجس بواسطة مرشح، الذي يحدد له حزم البيانات المطلوب فحصها في القطاع. عندما يجد المجس حزم البيانات التي تطابق (أو لا تطابق) المرشح؛ فإنه يقوم بإرسال حزم البيانات إلى القناة Channel، كما هو موضح في خريطة سير العمليات في الشكل6.13. تحتفظ القناة بعدد حزم البيانات التي يتم إيجادها، وتستطيع اختيارياً توليد حدث event عندما تجد حزمة البيانات أو تحتفظ بها لأجل تحليلات أخرى.



شكل 6.13 خريطة سير العمليات للمرشحات والقنوات.

تفيد هذه الوظائف في مجالات إدارة الأعطال وإدارة الأمن، حيث يمكن لمجموعة المرشح أن تعين في تطبيق إدارة الأعطال، حيث يستطيع مجس الرصد ملاحظة حزم بيانات محددة، أو أخطاء في القطاع، بعد ذلك يقوم بتوليد حدث ويرسله عبر القناة. يمكن أن تستفيد وظائف إدارة الأمن من مجموعة المرشح، إذ يمكن لمهندس الشبكة تهيئة المرشح للبحث عن نوع معين من حزم البيانات، أو حزم من مستخدم، أو حاسب مضيف محدد. عندما تظهر هذه الحزمة، يقوم بإرسال حدث عبر القناة إلى نظام إدارة الشبكة.

1.7.3 المرشحات Filters

يعرف المرشح بأنه حزمة البيانات التي سوف يقوم مجس الرصد بمراقبتها. يوجد نوعين من المرشحات: هما مرشح البيانات data filter، ومرشح الحالة status filter. يستطيع المجس البحث عن حزم البيانات التي تطابق نموذج معلومة محدد، بواسطة استخدام مرشح البيانات. ومراقبة حزم البيانات بناء على حالتها الحالية (صالحة valid، قزمة runt، عملاقة giant، أو بها خطأ تكراري CRC error)، بواسطة استخدام مرشح الحالة.

<u>على سبيل المثال</u>: يقوم مرشح الحالة بفحص حالة حزمة البيانات، عندما يقوم المجس باستلامها. عندما يوجد بها خطأ، يقوم المرشح بحساب المجموع sum بناء على شفرة الخطأ. وهذا المجموع في البداية يكون صفراً، ثم يتم إضافة كل خطأ يتم اكتشافه إلى هذا المجموع، بدلالة code ***error*** ^ ***2*** .

مثلا: في حالة شبكة ايثرنيت يتم تحديد هذه المعلومات bits والأخطاء المصاحبة لها كما يلي:

Bit0: تحدد حزمة بيانات أطول من 1518 حرفاً (حزمة عملاقة).

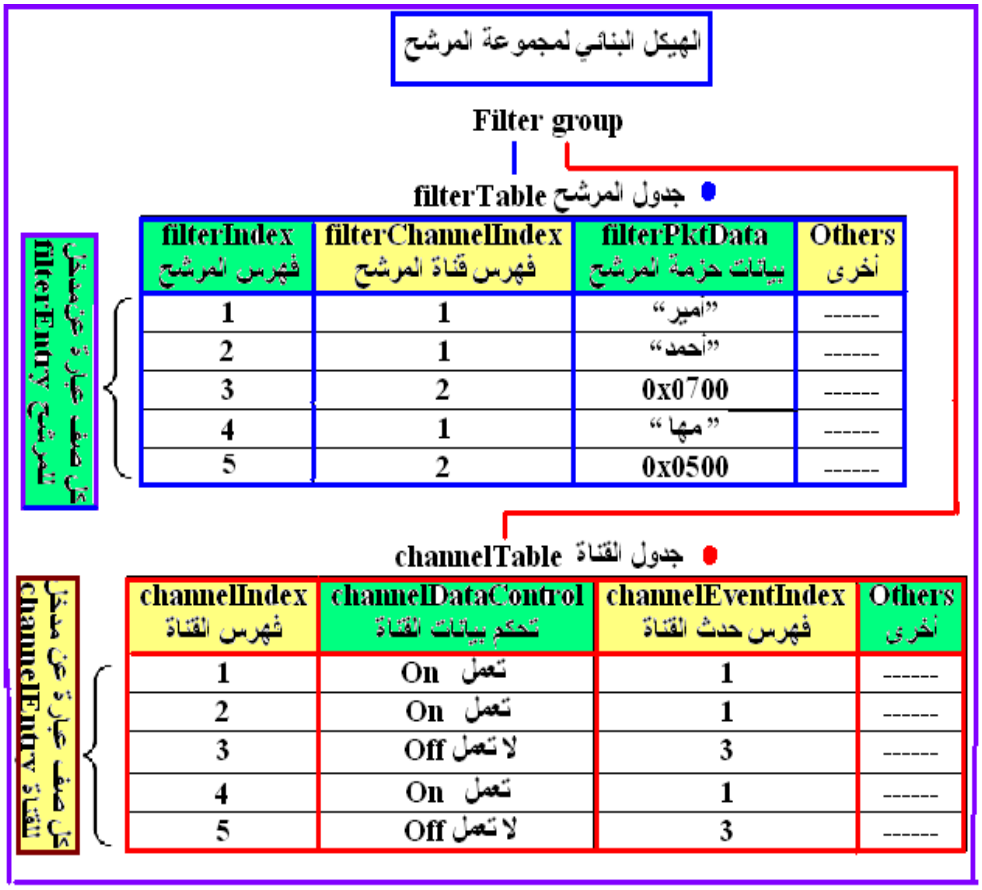
Bit1: تحدد حزمة بيانات أقصر من 64 حرفاً (حزمة قزمة).

Bit2: تحدد حزمة بيانات تعاني من وجود أخطاء أو CRC.

وتكون قيمة عنصر حالة حزمة بيانات المرشح filterPktStatus لها قيمة خطأ CRC تساوي: ***5 = 2^2+2^0***

يمكن إعداد مرشحات مركبة بواسطة استخدام مرشحات متعددة تقوم بالإرسال إلى قناة واحدة. على سبيل المثال، يمكننا البحث عن حزم البيانات التي لها نموذج بيانات محدد (مثلا: اسم الحاسب المضيف)، أو التي يوجد بها خطأ وتأتي من عنوان حاسب مضيف محدد داخل القطاع.

يتم إعداد المرشحات داخل جدول المرشح filterTable، والذي يتكون من العناصر الموضحة في الشكل 6.14.



الشكل 6.14 هيكل بنائي مختصر لعناصر مجموعة المرشح.

مثل الجداول الأخرى لقاعدة المعلومات الإدارية للرصد عن بعد، فإن جدول المرشح، يوجد به عنصر يسمى "مالك المرشح" filterOwner ، يحدد النظام الإداري الذي قام بإعداد هذا المرشح، وكذلك حالة المرشح، التي تبين الحالة الحالية للمرشح.

2.7.3 القنوات Channels

الجدول الثاني في مجموعة المرشح، هو جدول القناة channelTable ، كما هو موضح في الشكل6.14 . يمكن للقناة أن تقبل حزمة البيانات، عندما تطابق المرشح، أو عندما لا تطابق المرشح. نستطيع أن نخصص أحداثاً events في مجموعة الأحداث، كي تقوم بتشغيل on أو إيقاف off القناة. بمعنى أنه عندما يقع حدث معين، فقد يكون من المرغوب فيه أن يتم فتح قناة مع المرشحات للبحث عن بيانات محددة ، أو حالة حزم بيانات في القطاع.

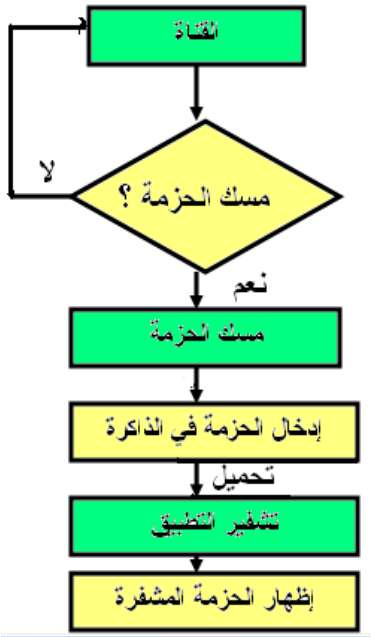
كما يمكن للقناة نفسها أن تقوم بتوليد الحدث. يقوم عنصر "فهرس الحدث" channelEventIndex بتحديد الحدث الذي ينبغي أن تقوم القناة بتوليده، عندما يكون عنصر "تحكم البيانات" channelDataControl في الحالة on ، وتكون القناة قد قبلت حزمة البيانات. ويخبرنا عنصر "حالة الحدث" channelEventStatus أن القناة قد قامت بإرسال هذا الحدث. وأخيراً، فإن عنصر "مالك القناة" channelOwer يخبرنا عن النظام الإداري الذي قام بإعداد هذه القناة، ويقوم عنصر حالة القناة بإعطائنا الحالة الحالية لهذه القناة.

8.3 مجموعة مسك الحزم Packet Capture Group

تستخدم هذه المجموعة لإعداد نظام التخزين المؤقت Buffering Scheme لحزم البيانات التي يتم إرسالها إلى قناة واحدة من مجموعة المرشح. بسبب أن مجموعة مسك الحزم، تعتمد على القنوات channels، فإن مجس الرصد يحتاج أولاً إلى بناء مجموعة المرشح. مثل مجموعة المرشح، فإن مجموعة مسك الحزم يمكن أن توفر الوظائف التي تساعد في تطبيقات إدارة الأداء، وإدارة الأمن. وهذه الوظائف تكون متاحة لا بسبب

المهام التي يدعمها مجس الفحص لمجموعة مسك الحزم (مسح الحزم لاسترجاعها فيما بعد) ، لكن بسبب مقدرة نظام إدارة الشبكة ، والتطبيقات على تحميل حزمة البيانات ، وبعد ذلك يتم فك تشفيرها Decoded.

يوضح الشكل6.15 خريطة سير العمليات لأحد التطبيقات التي تستخدم مجموعة مسك الحزم.



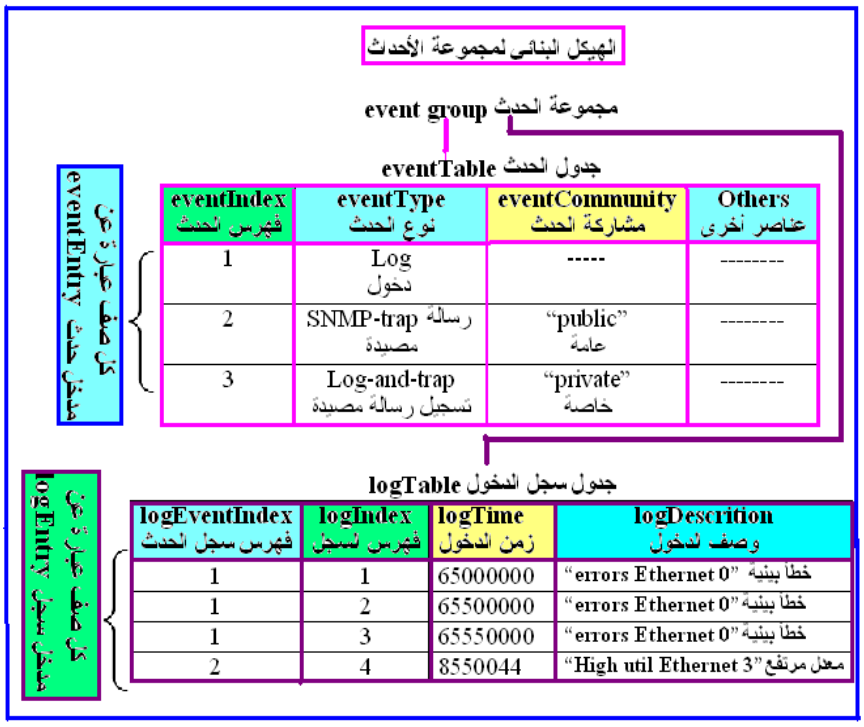
شكل6.15 خريطة العمليات لأحد تطبيقات مجموعة مسك الحزم.

9.3 مجموعة الحدث Event Group

تسمح مجموعة الحدث بتعريف الأحداث. يمكن أن يتم بدء الحدث trigger من الإنذارات alarms، والقنوات channels ، كما شرحنا سابقا. يمكن للحدث أن يولد فعلاً action، مثل فتح أو غلق القناة. يستطيع الحدث أن ينشئ سجل دخول Log Entry أو ربما- اختياريا- يجعل المجس يقوم بإرسال رسالة المصيدة SNMP Trap إلى نظام إدارة الشبكة.

يمكن لمجموعة الأحداث أن تساعد في تطبيقات إدارة الأعطال، والأداء، والأمن. كما يمكن للأحداث التي يتم توليدها بواسطة مجس الرصد عن بعد، أن تساعد في الاستغناء عن نظام إدارة الشبكة للقيام بإجراء عمليات التصويت الدوري للأجهزة من أجل اكتشاف الأعطال. عندما يقوم المجس بتوليد الحدث بناء على الإنذار الذي يراقب عدد الأخطاء، أو حركة المرور في القطاع؛ فإن هذه المبادرة بالرصد، يمكن أن تعاون إدارة الأداء. بالمثل، عندما يتم إعداد الإنذار أو المرشح لمراقبة مخالفة الأمن؛ فإن الحدث يمكن أن يخبر مهندس الشبكة عن وجود مشكلة في إدارة الأمن. ويمكن أيضا، تسجيل الأحداث المساعدة في إنشاء سجلات التدقيق المزيلة Audit Trail، وهى بيانات هامة في تحقيق إدارة الأمن.

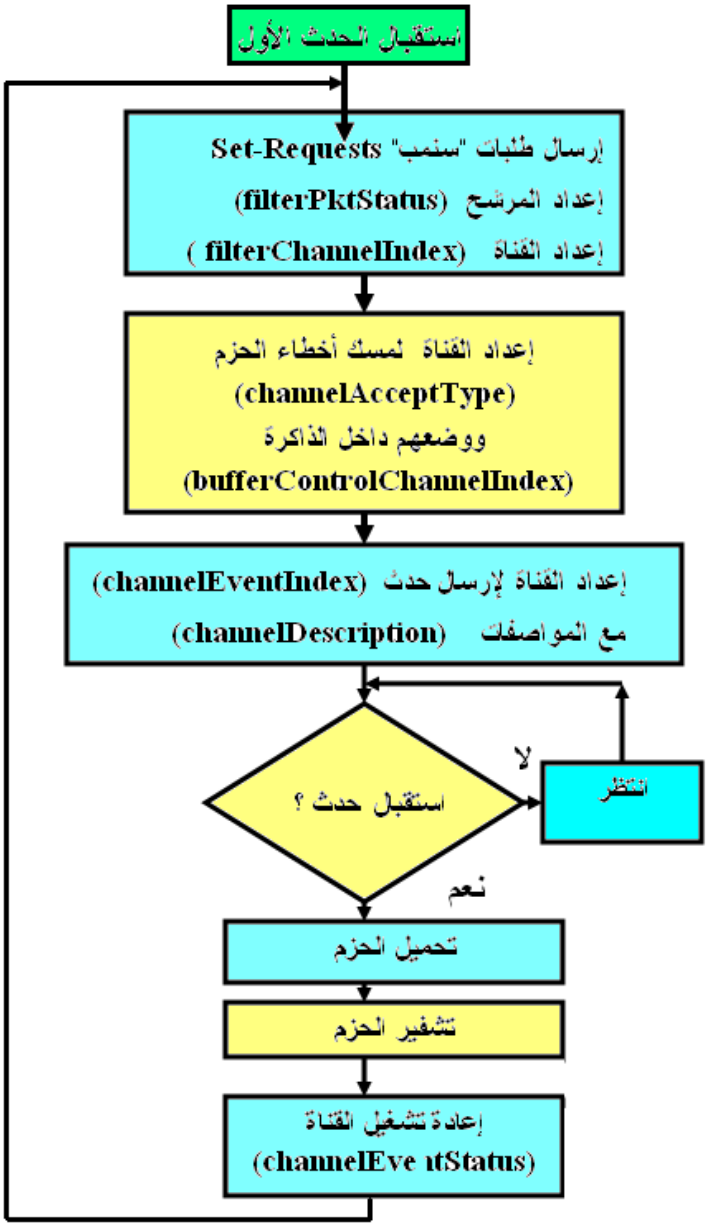
تتكون مجموعة الأحداث من جدولين، الأول للأحداث، والثاني لسجل دخول الأحداث. وتحتوي هذه الجداول على العناصر الموضحة في الشكل 6.16.



شكل6.16 يوضح هيكل بنائي مختصر لمجموعة الأحداث.

<u>على سبيل المثال</u>: نفترض أن تطبيق إدارة الأداء يستخدم مجس الرصد عن بعد لرصد عدد الأخطاء في قطاع شبكة ايثرنيت. يقوم التطبيق بإعداد عناصر مجموعة الإنذار، لبدء تشغيل الإنذار، عندما يزيد عدد الأخطاء في الإطار (زيادة القيمة CRC)، بمعدل أكثر من 50 في زمن دقيقة. بعد ذلك يقوم الإنذار بتوليد حدث يرسل إشارة SNMP Trap إلى نظام إدارة الشبكة، الذي يراه التطبيق في سجل الحدث.

عندما يتم استلام هذا الحدث الأول، يرسل التطبيق رسائل Set-Requests متتابعة إلى مجس الرصد، ويقوم بإعداد مرشح الحالة، والقناة المرافقة له. يتم إعداد القناة الجديدة لمسك حزم البيانات مع الأخطاء وتخزينها في ذاكرة التخزين Capture Buffers لمجس الرصد. بعد ذلك، يقوم التطبيق بإعداد حدث آخر بمواصفات مختلفة، ويجعل القناة الجديدة تقوم ببدء تشغيل هذا الحدث الجديد. عندما يتم رؤية رسالة SNMP Trap مع مواصفات الحدث الجديد، بواسطة نظام إدارة الشبكة والتطبيق؛ يقوم التطبيق بتحميل حزم البيانات الممسوكة، ويفك شفرتها لمهندس الشبكة. يقوم التطبيق بعد ذلك، بإعادة تشغيل reset القناة لمسك حزم بيانات خطأ أكثر في المستقبل. يوضح الشكل 6.17 خريطة سير العمليات لهذا التطبيق. في هذا الشكل، يقوم الحدث الأول بإعلام notify التطبيق بوجود مشكلة في الأداء في القطاع. بعد ذلك، يقوم التطبيق بتخصيص مصادر في مجس الرصد كي تقوم بفحص المشكلة أكثر ومسك حزم البيانات ذات العلاقة للقيام بفحصها بعد ذلك.



شكل6.17 توضيح بعض عناصر RMON MIB لأحد تطبيقات إدارة الأداء.

أسئلة تقويم ذاتي

1- تساعد مجموعة المرشح في رصد الشبكة عن بعد، وفحص حزم بيانات محددة في قطاع الشبكة المحلية.اشرح ذلك.

أ) عرِّف المرشح.

ب) عدد أنواع المرشحات.

ج) ارسم خريطة سير العمليات التي توضح عمل المرشحات والقنوات.

د) كيف يتم حساب قيمة الأخطاء CRC error المصاحبة لحزم البيانات بواسطة مرشح حالة حزم البيانات ؟.

2- يبين الجدول التالي حالة شبكة ايثرنيت بواسطة مرشح حالة حزم البيانات. قم بتوفيق المعلومات Bits ، مع ما يقابلها من الأخطاء المصاحبة.

المعلومة	الأخطاء المصاحبة
Bit0	حزمة بها أخطاء CRC errors
Bit1	حزمة عملاقة Giant
Bit2	حزمة قزمة Runt

3- اذكر وظيفة مجموعة مسك الحزم، مع إعطاء مثال توضيحي.

4- اذكر وظيفة مجموعة الحدث.

5- اذكر مسميات خمس مجموعات مستخدمة في قاعدة المعلومات الإدارية لرصد الشبكة عن بعد RMON2، واكتب نبذة مختصرة عن وظيفة كل مجموعة.

10.3 مجموعات قاعدة المعلومات الإدارية RMON2

تعتبر مجموعات قاعدة المعلومات الإدارية RMON2، امتدادا لقاعدة المعلومات الإدارية RMON1 ، التي تشتمل على مجموعات تمكن البروتوكول من رصد حركة المرور في المستويات العليا فوق مستوى MAC . تمكن هذه القدرات مجس الرصد عن بعد من رصد حركة المرور على أساس مستوى بروتوكولات الشبكة وعناوينها، ويشمل ذلك بروتوكولIP . بذلك يستطيع المجس رؤية حركة المرور القادمة إلى الشبكات المحلية من خلال الموجّهات، وليس فقط من الشبكة المحلية المتصل بها. ثانياً، توفير وسائل لتشفير ورصد حركة المرور في المستوى التطبيقي، مثل البريد الإلكترونيe-Mail، ونقل الملفات file transfer ، وبروتوكولات الويب WWW، ويعني ذلك أن المجس يستطيع تسجيل حركة المرور من و إلى الحواسيب المضيفة لتطبيقات محددة. ويوضح الشكل6.18 هذه المجموعات الإضافية.

الشكل6.18

تشتمل مجموعات قاعدة المعلومات الإدارية RMON2، على تسع مجموعات هي:

- مجموعة دليل البروتوكول protocolDIR group :

إن مجموعة دليل البروتوكول، هي عبارة عن الدليل الرئيسي الذي يحتوي قائمة تفصيلية بالمعلومات عن كل البروتوكولات التي يستطيع المجس تفسيرها. وهي تقوم بتدوين البروتوكولات التي يمكن للمجس أن يشفرها decode ويقوم بعدها. تمثل هذه البروتوكولات المستوى الشبكي، مستوى النقل، والمستويات العليا الأخرى. ينبغي أن يقوم المجس بإجراء عملية التحضير للتشغيل boot up بهذا الجدول، وإجراء عملية التهيئة المسبقة preconfigured بهذه البروتوكولات التي سيتم رصدها.

أ- مجموعة بروتوكول التوزيع protocolDist group

تقوم مجموعة بروتوكول التوزيع، بتجميع إجمالي الإحصاءات عن حركة المرور الموزعة، التي يتم توليدها بواسطة كل بروتوكول لكل قطاع شبكي محلي.

ب- مجموعة ترجمة العنوان addressMap group

تقوم مجموعة ترجمة العنوان بتوفيق matches عناوين المستوى الشبكي مع عناوين مستوى MAC الخاصة بها على منافذ ports الجهاز المتصل والعنوان الفيزيقي لقطاع الشبكة.

ج- مجموعة الحاسب المضيف للمستوى الشبكي:nlHost group:

تقوم مجموعة الحاسب المضيف للمستوى الشبكي، برصد حركة المرور الداخلة والخارجة من الحواسيب المضيفة طبقا لعناوين المستوى الشبكي. ويسمح ذلك للمدير بأن يفحص ما وراء الموجّه للوصول للحاسبات المضيفة المتصلة. وهي تتحكم في جداول كل من المستوى الشبكي والمستوى التطبيقي للحاسبات المضيفة.

د- مجموعة المصفوفة للمستوى الشبكي nlMatrix group

تتعامل مجموعة المصفوفة للمستوى الشبكي، مع مجموعة الإحصاءات بين أزواج pairs الحواسيب المضيفة بواسطة البروتوكول، طبقا لعناوين المستوى الشبكي. تشتمل

جداول بيانات هذه المجموعة، على إحصاءات مشابهة لمجموعات مصفوفة قاعدة المعلومات RMON1، ومجموعة القمة N للحاسبات المضيفة.

هـ- مجموعة الحاسب المضيف للمستوى التطبيقي alHost group

تقوم مجموعة الحاسب المضيف للمستوى التطبيقي، بتجميع الإحصاءات على المستوى التطبيقي للبروتوكول من عناوين شبكة محددة، التي تم تحديدها بواسطة الوحدة البينية لهذا الجهاز.

و- مجموعة المصفوفة للمستوى التطبيقيalMatrix group

تقوم مجموعة المصفوفة للمستوى التطبيقي، بتجميع الإحصاءات من أزواج الحواسيب المضيفة، طبقا لبروتوكول المستوى التطبيقي.

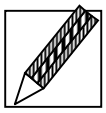
ز- مجموعة تاريخ المستخدم usrHistory group

تقوم مجموعة تاريخ المستخدم بدمج أساليب الإنذار والمجموعات التاريخية، وتقوم بأخذ عينات دورية لمتغيرات محددة خاصة بالمستخدم، وتسجل هذه البيانات طبقاً لمعاملات تحديد المستخدم.

ح- مجموعة تهيئة المجس probeConfig group

تحدد مجموعة تهيئة المجس، معاملات التهيئة القياسية عن بعد، المدعمة للوكلاء، ومراجعة البرمجيات، وتحكم إعادة التشغيل، وكذلك جدول أهداف المصيدة trap (قائمة رسائل المصيدة، التي تقوم الحواسيب المضيفة لبروتوكول IP باستلامها).

تدريب (1)



قدِّم مقارنة بين سنمبSNMP و رمون RMON ومن خلال عناصر المقارنة قم بإنشاء جدول مقارنة من حيث:
درجة تعقيد الوكيل، المدير، بينية برنامج التطبيق API ، وكذلك من حيث استخدام العمارة الموزعة، ودرجة تحقيق الأمن، وسعة الانتشار.

الخلاصة

عزيزي الدارس،

تناولت الوحدة في قسمها الأول أجهزة رصد الشبكة عن بعد. وأوضح القسم أن الغرض من جهاز رصد الشبكة عن بعد، هو المساعدة في إجراء عمليات إدارة الشبكة على قطاع شبكي Network Segment محدد. وتناول القسم المكونات الأساسية لرصد الشبكة عن بعد، وتشمل نظام إدارة الشبكة، جهاز الرصد (المجس)، وقاعدة المعلومات الخاصة بالرصد، و القطاع الشبكي لإيثرنيت، الذي يتم رصد بياناته. يكون جهاز رصد الشبكة عن بعد مسؤولاً عن تجميع الإحصاءات المعرفة في قاعدة المعلومات الإدارية RMON MIB. وأوضح القسم أن قاعدة المعلومات "رمون–ميب RMON-MIB" ، تمت معايرتها standardized من أجل العمل على قطاعات الشبكات المحلية ايثرنيت، لكن هذا لا يمنع تقنيات الشبكات الأخرى من استخدامها. فقد تم توسعتها لتشمل إدارة شبكات مثل Token Ring، وشبكات FDDI ،كما أوضح القسم أنه :

– يمكن للمؤسسة أن تضع جهاز رصد الشبكة عن بعد في كل قطاع شبكي، وعند تطبيق هذه الطريقة، يستطيع مدير الشبكة المركزي تجميع الإحصاءات الخاصة بقاعدة معلومات "رمون–ميب" من كل قطاع شبكي.

– شراء برنامج يستطيع إجراء رصد الشبكة عن بعد، بواسطة جهاز غير محجوز Nondedicated، حيث نستطيع شراء البرنامج للعديد من محطات العمل التي تستطيع إضافة رصد الشبكة عن بعد ، ضمن وظيفة محطة العمل .

– بوضع المجس الوظيفي داخل مجمع سلكي ذكيIntelligent Wiring Hub (مثل هذا المجمع متوفر في الأسواق) يوصل المجمع السلكي في نهاية النظم، ويتم وضع المجس في مكان مناسب.

القسم الثاني تناول أهداف قاعدة المعلومات الإدارية للرصد عن بعد وهي :

– أخذ المبادرة بإجراء عملية الرصد Preemptive Monitoring.

- الكشف عن المشاكل وتدوينها Problem Detection and Reporting
- إتاحة بيانات القيمة المضافة Value-Added Data.
- توفير الدعم لمدرين متعددين Multiple Managers .

القسم الثالث تناول مجموعات عناصر قواعد المعلومات الإدارية ,RMON1 RMON2 ، حيث تختص قاعة المعلومات الإدارية "رمون–1 " بإدارة الشبكات المحلية، التي تتعامل فقط مع المستويين الأول والثاني في النظام المرجعي OSI، أمّا قاعدة المعلومات الإدارية "رمون–2 RMON2 " فتختص بالتعامل مع إدارة المستويات العليا.

وقد تناول القسم قائمة مجموعة "رمون–1" ، و "رمون–2" ، وهما تحتويان على تسع عشرة مجموعة، تم شرحها بالتفصيل تباعا في هذا القسم من الوحدة الدراسية ، وهي كالتالي :

- مجموعة الإحصاءات Statistics Group ، وتحتوي مجموعة الإحصاءات على العناصر Objects التي يتم قياسها لكل وحدة بينية ايثرنيت في جهاز الرصد عن بعد. يتم حفظ الإحصاءات الخاصة ببينية ايثرنيت منفصلة عن البينيات Interfaces الأخرى. تسمح هذه الخاصية بأن يستطيع مجس الرصد توفير بيانات عن قطاعات عديدة في نفس الوقت، تفيد هذه الإحصاءات في إجراء عمليات إدارة الأعطال، والتهيئة، والأداء.
- مجموعة التاريخ History Group ، وتساعد مجموعة التاريخ مهندس الشبكة في أخذ عينات إحصائية دورية من القطاع الشبكي وتخزينها داخل مجس الرصد ، لاستخدامها فيما بعد عند إجراء عمليات التحليل. تتكون عناصر مجموعة التاريخ من جدول التهيئة اللازم لتحديد العينات، وجدول تحديد الوسط الذي يخزن العينات فور الحصول عليها.
- مجموعة الإنذار Alarm Group ، التي في إدارة الأداء.

– مجموعة الحاسب المضيف Host Group ، التي تحتوي على العناصر المصاحبة للحاسب المضيف لقطاع الشبكة، وتفيد عناصر مجموعة الحاسب المضيف، في تطبيقات إدارة التهيئة، والحسابات، والأداء.

– مجموعة القمة N للحاسب المضيف Host-Top N ، وتستخدم نفس العناصر الموجودة في مجموعة الحاسب المضيف، لتجهيز تقارير لإعداد الحواسيب المضيفة، خلال مدة زمنية معلومة. يتم تجهيز هذه التقارير على أساس الإحصاء الذي تم تحديده بواسطة نظام إدارة الشبكة.

– مجموعة المصفوفة Matrix Group ، وتحتوي على جدول العناصر الذي يحفظ الإحصاءات عن عدد الحزم والحروف والأخطاء المرسلة بين عناوين في القطاع الشبكي.

– مجموعة المرشح Filter Group ، وتساعد مهندس الشبكة بأن يستخدم مجس الرصد عن بعد لفحص حزم بيانات محددة في قطاع الشبكة.

– مجموعة مسك الحزم Packet Capture Group

تستخدم هذه المجموعة لإعداد نظام التخزين المؤقت Buffering Scheme لحزم البيانات التي يتم إرسالها إلى قناة واحدة من مجموعة المرشح.

– مجموعة الحدث Event Group ، وتسمح بتعريف الأحداث.

يمكن لمجموعة الأحداث أن تساعد في تطبيقات إدارة الأعطال، والأداء، والأمن.

– مجموعات قاعدة المعلومات الإدارية RMON2 وتعتبر هي امتدادا لقاعدة المعلومات الإدارية RMON1 ، التي تشتمل على مجموعات تمكن البروتوكول من رصد حركة المرور في المستويات العليا فوق مستوى MAC . تمكن هذه القدرات مجس الرصد عن بعد، من رصد حركة المرور على أساس مستوى بروتوكولات الشبكة وعناوينها، ويشمل ذلك بروتوكولIP وتشتمل مجموعات قاعدة المعلومات الإدارية RMON2، على تسع مجموعات هي:

- مجموعة دليل البروتوكول protocolDIR group.

- مجموعة بروتوكول التوزيع protocolDist group.
- مجموعة ترجمة العنوان addressMap group.
- مجموعة الحاسب المضيف للمستوى الشبكي nlHost group.
- مجموعة المصفوفة للمستوى الشبكي nlMatrix group.
- مجموعة الحاسب المضيف للمستوى التطبيقي alHost group.
- مجموعة المصفوفة للمستوى التطبيقيalMatrix group .
- مجموعة تاريخ المستخدم usrHistory group.
- مجموعة تهيئة المجس probeConfig group.

لمحة مسبقة عن الوحدة التالية

عزيزي الدارس،

تبحث الوحدة التالية في الأدوات البرمجية المعاونة في إدارة الشبكات، حيث تتناول الوحدة أدوات قاعدة المعلومات الإدارية MIB-Tools. وتشمل هذه الأدوات مترجم ميب، ومتصفح ميب، وأداة ميب للاسم المستعار، وأداة استفسار ميب. كما تجد في هذه الوحدة أدوات العرض والتي تتضمن السجل المركزي، وكاتب التقرير، والحزم الرسوم وأيضا ً تجد في الوحدة تناولاً لأدوات حل المشاكل، وهي: نظم تتبع المشكلة، أدوات تصميم الشبكة، النظم الخبيرة .

إجابات التدريبات

تدريب (1)

إن الفرق بين "سنمب" SNMP ، و"رمون" RMONهو أن "سنمب" يدير ويرصد أجهزة الشبكة مثل المجمعات Hubs، والقناطر Bridges، أمّا "رمون" فيرصد حركة مرور Traffic الشبكات المحلية LAN. عند تطبيق "رمون" فإن بعض الذكاء الإداري Management Intelligence يتم نقله إلى الشبكة. حيث يقوم مجس رمون للرصد عن بعد بإعلام الكونصل المركزي، عند حدوث تجاوز الحد Threshold ، مثلاً: عندما يزيد عدد حزم البيانات.

(جدول مقارنة بين "سنمب–ف1" ، "سنمب–ف3"، وثميب CMIP، و"رمون" .)

FACTOR المعامل	CMIP ثميب	SNMP-V1 سنمب–ف1	SNMP-V1 سنمب–ف1	RMON رمون
Agent Complexity تعقيد الوكيل	مرتفع	منخفض	منخفض	مرتفع
Manager Complexity تعقيد المدير	متوسط	عالٍ	عالٍ	متوسط
Security الأمن	عالٍ	منخفض	حسب الطلب (قد يصل لمرتفع)	منخفض
Distributed Architecture العمارة الموزعة	توجد	لا توجد	توجد	لا توجد
API Complexity بينية برامج التطبيق	عالٍ	منخفض	منخفض	متوسط
Dissemination سعة الانتشار	منخفض	انخفاض (متزايد)	عالٍ	متوسط

نجد من الجدول أن بروتوكول "ثميب" ، وكذلك سنمب–1 قَلِيْلَيْ الانتشار ، أمّا "رمون" فمتوسط الانتشار، ويفوقه بروتوكول "سنمب–ف3" في سعة الانتشار.

وبخصوص استخدام إدارة الشبكات في نظم العمارة الموزعة، فإنه بحسب نتائج الجدول فإن أنسب البروتوكولات هو بروتوكول "سنمب–ف3"، كما أنه يفوق "رمون" من حيث تحقيق الأمن.

مسرد المصطلحات

جهاز رصد الشبكة عن بعد

هو جهاز (أو مجس Probe) يوضع على قطاعات الشبكة. ويقوم برصد هذه القطاعات الشبكية وتجميع الإحصاءات. الغرض من جهاز رصد الشبكة عن بعد، هو المساعدة في إجراء عمليات إدارة الشبكة على قطاع شبكي Network Segment محدد.

مجس الرصد الغير محجوز NonDedicated

هو عبارة عن برنامج يستطيع إجراء رصد الشبكة عن بعد، ويمكن تشغيله على جهاز الحاسب بالشبكة، أو جهاز الوكيل بالشبكة.

مجموعات قاعدة المعلومات الإدارية RMON1

تختص مجموعات قاعدة المعلومات الإدارية **RMON1** بإدارة الشبكات المحلية، التي تتعامل فقط مع المستويين الأول والثاني في النظام المرجعي OSI. وتشتمل على عشر مجموعات.

مجموعات قاعدة المعلومات الإدارية RMON2

تعتبر مجموعات قاعدة المعلومات الإدارية RMON2، امتدادا لقاعدة المعلومات الإدارية RMON1، التي تشتمل على مجموعات تمكن البروتوكول من رصد حركة المرور في المستويات العليا فوق مستوى MAC.

فهرس الإنذار alarmIndex

عبارة عن رقم مميز مصاحب لكل مدخل إنذار alarmEntry .

المرشحات Filters

يعرف المرشح بأنه حزمة البيانات التي سوف يقوم مجس الرصد بمراقبتها، و يوجد نوعان من المرشحات هما : مرشح البيانات data filter، ومرشح الحالة status filter.

مالك المرشح filterOwner

هو عنصر يوجد في جدول المرشح يحدد النظام الإداري الذي قام بإعداد هذا المرشح، وكذلك حالة المرشح، التي تبين الحالة الحالية للمرشح.

المصطلح بالإنجليزية	معناه بالعربية
Alarms	إنذارات
Alarm Group	مجموعة الإنذار
Audit Trail	سجلات التدقيق المزيلة
Boot up	التحضير للتشغيل
Buffering Scheme	نظام التخزين المؤقت
Broadcast Traffic	حركة الرسائل الإذاعية
Capture Buffers	ذاكرة المسك
Channels	القنوات
Collision	تصادم
CRC error	خطأ تكراري
Data Filter	مرشح البيانات
Dedicated	يتم حجزه
Decoded	يتم فك تشفيرها
e-Mail	البريد الإلكتروني
Event Group	مجموعة الحدث
Falling	الهبوط
Filter Group	مجموعة المرشح
File Transfer	نقل الملفات
Host Group	مجموعة المضيف
Host-Top N	مجموعة القمة N للمضيف
History Group	مجموعة التاريخ
Intelligent Wiring Hub	المجمع السلكي الذكي
Giant	عملاقة

Log Entry	سجل دخول
Management Intelligence	الذكاء الإداري
Matrix Group	مجموعة المصفوفة
Multiple Managers	مديرون متعددون
Network Segment	قطاع شبكي
NonDedicated	غير محجوز
Offline	بدون اتصال
Outage	انقطاع اتصال الشبكة
Off-Line Operation	إجراء العمليات دون الاتصال بالشبكة
Packet Capture Group	مجموعة مسك الحزم
Preemptive Monitoring	مبادرة إجراء عملية الرصد
Preconfigured	التهيئة المسبقة
Protocol Analyzer	المحلل البروتوكولي
Promiscuous	نمط الاختلاط
Problem Detection and Reporting	كشف المشاكل وتدوينها
Remote Monitoring (RMON)	الرصد عن بعد
Rising	الصعود
Routing	تحديد المسار
Runt	قزمة
Standardized	معايرتها
Status Filter	مرشح الحالة
Statistics Group	مجموعة الإحصاءات
Spanning Tree	شجرة الاجتياز
Threshold	القيم الحدية

Time-Ordered	قائمة الطلبات الزمنية
Traffic Volume	حجم حركة المرور
Trigger	بدء الحدث
Utilization	معدل الاستخدام
Valid	صالحة
Value-Added Data	بيانات القيمة المضافة

قائمة المراجع

1- SNMP, SNMPv2c, SNMPv3, and RMON 1 and 2, 3rd Edition, by William Stallings, Published by Addison-Wesley Pub Co Publication 1999, ISBN: 0201485346

2- RMON: Remote Monitoring of SNMP-Managed LANs, by David T. Perkins, Published by Prentice Hall Professional Technical Reference, 1999., ISBN: 0130961639.

3- LAN Management With SNMP and RMON, by Gilbert Held, Published by John Wiley & Sons, 1996, ISBN: 0471147362.

4- Network Management: A Practical Perspective, by Allan Leinwand, Karen Fang-Conroy. Info at Addison-Wesley, 1997.

5- Web Sites:

http://www.javvin.com/protocol/rfc2819.pd

http://www.javvin.com/protocol/rfc2021.pdf
http://www.javvin.com/protocol/rfc1157.pdf


الوحدة السابعة
الأدوات البرمجية المعاونة
في إدارة الشبكات

محتويات الوحدة

المقدمة

تمهيد

عزيزي الدارس،

مرحباً بك في الوحدة السابعة من مقرر "استخدام و إدارة الشبكات 2". تبحث هذه الوحدة في الأدوات البرمجية المعاونة في إدارة الشبكات.

يتناول القسم الأول من الوحدة أدوات قاعدة المعلومات الإدارية، وتشمل هذه الأدوات: مترجم ميب، ومتصفح ميب، وأداة ميب للاسم المستعار، وأداة استفسار ميب.

القسم الثاني من الوحدة يتناول أدوات العرض وتتضمن هذه الأدوات: السجل المركزي، وكاتب التقرير، والحزم الرسوم.

القسم الثالث من الوحدة يتناول أدوات حل المشاكل، وهي: نظم تتبع المشكلة، وأدوات تصميم الشبكة، والنظم الخبيرة.

أهداف الوحدة

بنهاية دراسة هذه الوحدة ينبغي – عزيزي الدارس– أن تكون الدارس قادراً على أن:

- **تعدد** وظائف واستخدامات أدوات قاعدة المعلومات الإدارية.
- **تشرح** عمل المترجم والمتصفح، وأداة الاستفسار، وأداة الأسماء المستعارة.
- **تعدد** وظائف واستخدامات أدوات العرض وأهميتها في إدارة الشبكة.
- **تشرح** عمل السجل المركزي، وبرنامج كاتب التقرير، والحزم الرسومية.
- **تعدد** وظائف واستخدامات أدوات حل المشاكل في تحسين الشبكات.
- **تصف** نظام تتبع المشكلة، وأدوات تصميم الشبكة، والنظم الخبيرة.
- **تطبق** بعض التدريبات والتطبيقات العملية على قواعد معلومات إدارة شبكة البيانات مستخدما بعض البرمجيات المتاحة على شبكة الإنترنيت.

توطئة

عزيزي الدارس،

يحتوى نظام إدارة الشبكات على عدة أدوات برمجية لمعاونة مهندس الشبكة في إدارة شبكة البيانات بكفاءة عالية. حيث يمكن أن يحتوي نظام إدارة الشبكة على خصائص أخرى مفيدة لا تنتمي مباشرة لأداء مجال إدارة شبكة معينة. وأن إضافة هذه الأدوات تعين مهندس الشبكة في تحسين أداء كفاءة إنتاجية النظام بدرجة عالية. على سبيل المثال، يمكن أن يحتاج مهندس الشبكة إلى وسيلة معاونة لكي يفحص عناصر قاعدة المعلومات الإدارية "ميب" MIB. وقد تشتمل هذه الوسائل على مترجم Compiler، ومتصفح Browser، وأداة استفسار Query، وأداة لتفسير الأسماء المستعارة Alias.

وقد يحتاج مهندس الشبكة، بعد أن يتم تجميع عناصر"ميب " من أجهزة الشبكة، أن يستخدم أدوات عرض Presentation Tools لإنشاء سجلات دخول Logs، ورسومات بيانية Graphs، وكتابة بعض التقارير. إضافة إلى ذلك، يمكن لمهندس الشبكة، أن يستعين بأدوات حل المشكلة Problem Solving Tools، لتحليل البيانات التي تم تجميعها من أجهزة الشبكة، وعرض بعض الحلول الممكنة. قد تحتوي هذه الأدوات على نظام تتبع المشكلة Trouble Tracking System، وأدوات تصميم الشبكة، والنظم الخبيرة Expert Systems. تعين هذه الأدوات مهندس الشبكة في تحسين إنتاجية إدارة الشبكة.

يمكن أن يحتوى النظام الإداري لشبكة البيانات، على كل هذه المجموعة من الأدوات مجتمعة، ويمكن أن توجد كل أداة في النظام بشكل مستقل. ويوجد بالأسواق أدوات عديدة الخصائص نتناول شرحها في هذه الوحدة الدراسة، كما نناقش بعض الأدوات البرمجية الأخرى التي يمكن تطويرها للأوساط المحيطة بشبكه معينة. ونوصي المؤسسات ومهندسي الشبكات– عند شراء أو تطوير نظام إدارة الشبكة– أن تأخذ بعض هذه الأدوات في الاعتبار، أو ربما جميعها، ويعتمد ذلك على كيفية المعاونة التي تريد

المؤسسة ومهندس الشبكة، تحقيقها في نظام إدارة الشبكة، من أجل تطبيق إدارة الشبكة بفاعلية وكفاءة وإنتاجية متميزة.

1. أدوات قاعدة المعلومات الإدارية MIB-Tools

عزيزي الدارس،

تفيد هذه الأدوات في التعامل مع معلومات "ميب MIB"، في نظام إدارة الشبكة وتشمل هذه الأدوات: مترجم ميب، متصفح ميب، أداة ميب للاسم المستعار، أداة استفسار ميب.

1.1 مترجم ميب MIB Compiler

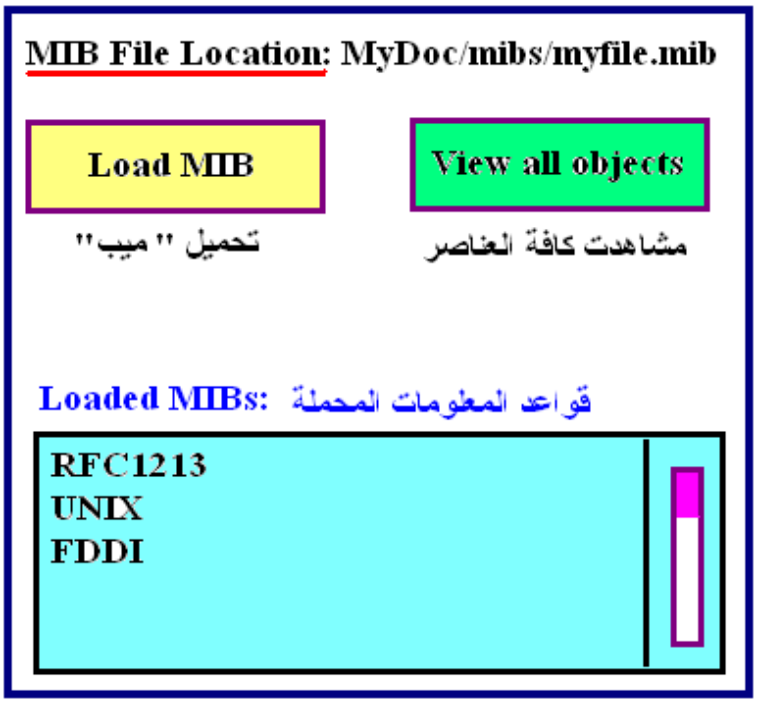
يقوم مترجم ميب بأخذ ملف على شكل الشكل ASN.1 ويحوله للاستعمالات المناسبة لنظام إدارة الشبكة. إن الإصدارات المهيأة للمستخدمين Customized Versions من قاعدة ميب تُفضَّلُ عادةً لأنها تقوم بإجراء عمليات البحث أسرع من استخدام ملف مكتوب بشفرة أسكي. قد نحتاج استخدام مترجم ميب لإنشاء قاعدة معلومات إدارية جديدة خاصة بمورد، أو تحديث ملف ميب موجود. وينبغي أن تكون هذه العملية سهلة الاستخدام. كما ينبغي أن يقوم النظام أيضا بتوليد قاعدة معلومات إدارية خاصة بالإصدار المهيأ للمستخدم، لتسمح لنظام إدارة الشبكة بالاستفسار عن الجهاز، بواسطة استعمال بروتوكول سنمب.

قد يوجد بالنظام حقل للإدخال an input field يسمح للمستخدم بتحديد اسم ملف مكتوب بشفرة أسكي لقاعدة المعلومات الإدارية. في هذه الحالة، يستطيع المترجم آلياُ قراءة هذا الملف، ويسمح لنا برؤية عناصر محددة. يوضح الشكل 7.1 مثالاً لهذه الأداة. ويمكن تطبيق هذه العناصر على أي من مجالات الوظائف الخمسة لإدارة الشبكة. غالباً، فإن كل نظم إدارة الشبكات المتاحة في الأسواق يوجد بها مترجم ميب. من أمثلة هذه النظم:

- نظام شركة أنسي بي HP Open View.

- نظام شركة أي بي إم IBM Net View / AIX.

تستخدم هذه النظم نافذة رسومية صغيرة ، مشابهة للشكل 7.1، حيث تسمح لنا بترجمة ميب على شاشة العرض. كما يحتوي برنامج مدير شبكة Sun Connect، على أداة تسمى mib2scheme لبروتوكول سنمب–ف1، وأداة أخرى تسمى v2mib2scheme لبروتوكول سنمب–ف2، وهذه الأدوات تترجم ملفات MIB إلى ملفات مدير SunNet.



شكل7.1 أداة ترجمة MIBs إلى نظام إدارة الشبكة.

على سبيل المثال: نفترض أننا نريد معرفة عدد المحطات النشطة الحالية المتصلة بالمجمع السلكي Wiring Hub، وهذه المعلومات تكون هامة في مسائل الحسابات والأداء. وأن هذه المعلومات غير متاحة في قاعدة المعلومات الإدارية القياسية. لكن يمكننا إضافة قاعدة معلومات إدارية خاصة بالمورد إلى المجمع السلكي لنظام إدارة الشبكة، وبذلك يكون النظام قادرا، بعد ذلك، على استرجاع هذه البيانات.

في حالة أخرى، يمكن أن يسمح المجمع السلكي تنشيط أو إخماد منفذ Port بواسطة إجراء طلب إعداد Set-Request لبروتوكول سنمب–ف1 للعنصر الخاص بقاعدة المعلومات الإدارية الخاصة بالمورد. كما درسنا سابقاً في الجزء الأول من كتاب إدارة الشبكات، فإن أداة إدارة الأعطال يمكن أن تستخدم هذا العنصر لإغلاق shut off المنفذ المعطل faulty port، كما تستطيع أداة إدارة التهيئة استخدامه لتهيئة وإعداد هذا المجمع.

- **ربط عناصر مترجم ميب مع خريطة الشبكة:**

يقوم مترجم ميب بتحميل قواعد المعلومات الإدارية إلى النظام. ويساعدنا في الحصول على البيانات الضرورية من أجهزة مختلفة كثيرة في الشبكة. كما يمكن إلحاق معاملات "ميب" إلى عناصر رسومية على خريطة رسم الشبكة.

على الرغم من أن الوصول إلى معلومات "ميب" الخاصة بالمورد تكون مهمة، يكون من المفيد عادة، أن يتم إحالة وربط هذه العناصر مع خريطة رسم الشبكة. **مثال1 "رصد معدل الخطأ":** بفرض أن أحد العناصر في قاعدة المعلومات الإدارية نفسها والخاصة بالمجمع السلكي قد أظهرت معدل خطأ دخول في كل منفذ. يمكننا إعداد عملية تجميع بيانات معدل خطأ الدخول هذا، وتخزينه في قاعدة البيانات العلاقية Relational Database لإدارة الشبكة، ثم إظهار وعرض إشارة رسومية على خريطة الشبكة، عندما يحدث معدل خطأ دخل مرتفع. إن تطبيق إدارة الأداء ربما لا يستطيع إجراء هذه العملية، بسبب أنه لا يفهم عنصر "ميب" الخاص بالمورد. إن بناء علاقة بين عنصر "ميب" محدد، وعنصر رسومي يكون وسيلة معقدة Sophisticated لاستخدام معلومات "ميب".

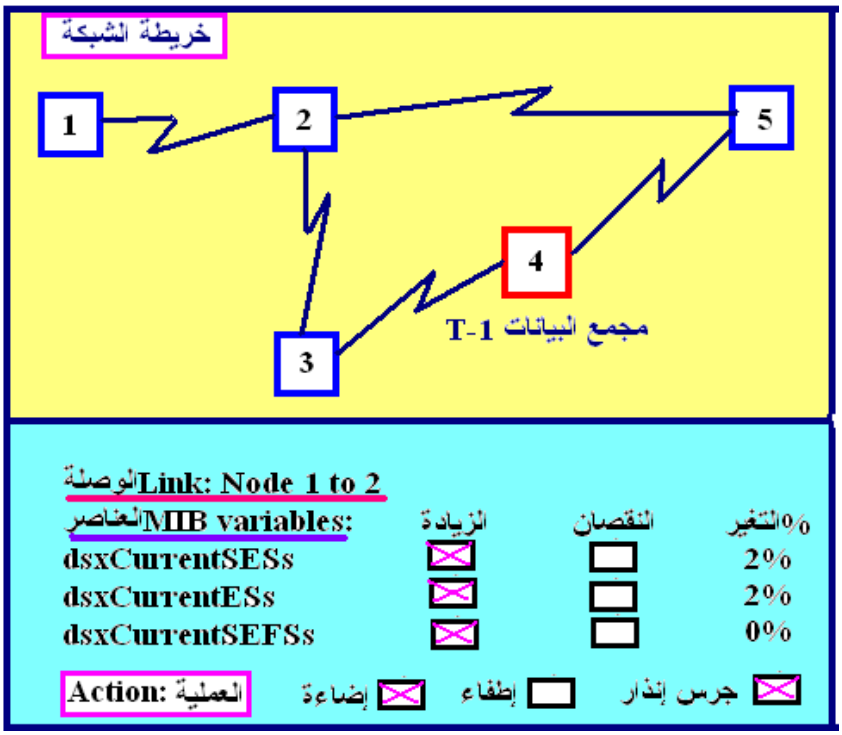
مثال2 "رصد تجاوز معدل الخطأ": نفترض أننا نريد تنصيب نظام إدارة شبكة لرصد معدل خطأ الدخل للوحدة البينية للموزع البصريFDDI ، المتصلة بخادم الملف File Server، وقررنا أنه عندما يزيد معدل خطأ الدخول عن 5% ، تضئ (تومض) أيقونة

الجهاز الموجودة على خريطة الشبكة الخاصة بخادم الملف. بذلك يمكن لهذه العلاقة الاختيارية بين عناصر "ميب"، وخريطة الشبكة، أن تساعدنا بفاعلية في فحص أداء الشبكة.

مثال3 "رصد معدل ثواني الخطأ الشديد": نفترض أننا نريد مصاحبة عناصر "ميب" متعددة بواسطة عنصر رسومي، لمعرفة زيادتها، نقصانها، أو تغير حالتها. نفترض شبكة بيانات تحتوي على مجمع بيانات Multiplexer من نوع T-1 ، يقوم بتوصيل العديد من الشبكات المحلية معاً من مواقع متعددة. باستخدام العناصر القياسية لقاعدة المعلومات الإدارية "ميب"، مثل جدول الوحدة البينية Interface Table، يستطيع تطبيق إدارة الأعطال أن يجعل الوصلات Links التي بها أخطاء تضئ Flash على خريطة رسم الشبكة.

يوجد مقياس معياري هام في وصلات T-1 الخاصة بمجمعات البيانات تسمى "ثواني الخطأ الشديد Severely Error Seconds "، وأن هذه المعلومات غير متاحة في قاعدة "ميب" القياسية، لكنها متاحة في قاعدة المعلومات الخاصة بمجمع البيانات، وتسمى T-1 MIB. ويرمز لهذا العنصر بالرمز dsx1CurrentSESs، وتعرف قيمته بأنها فترة زمنية مدتها ثانية واحدة، يحدث خلالها خطأ أكبر 30%. وهو يبين عدد الأخطاء الشديدة الحالية التي حدثت خلال مدة ثواني، في الوحدة البينية DS1. ونحن نرغب في إضاءة الوصلة على خريطة الشبكة ، عندما تصل قيمة عنصر "ثواني الخطأ الشديد" إلى الحد المعروف (أكبر من 30%).

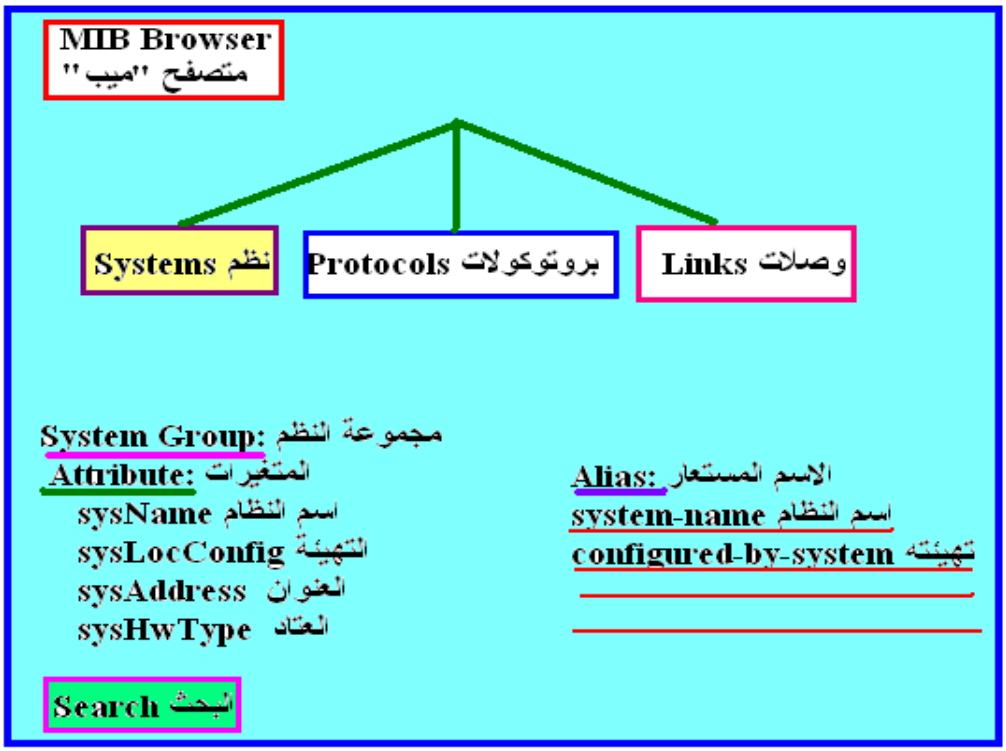
لتوفير هذه الوظيفة، فإن نظام إدارة الشبكة، يجب أولاً أن يتعلم قاعدة المعلومات الإدارية الخاصة بالوحدة البينية T-1 ، والموجودة في قاعدة المعلومات T1 MIB. كما أننا نحتاج إلى وجود وسيلة لإخبار النظام أنْ يضئ الوصلة المناسبة على خريطة الشبكة، عندما يزيد معدل خطأ مجمعات البيانات T-1. يوضح الشكل 7.2 ، مثالاً على تطبيق الوحدة البينية المصاحبة لعناصر "ميب" مع عناصر خريطة رسم الشبكة.



شكل7.2 خريطة الشبكة، والتطبيق المصاحب عناصر T-1 لعناصر رسومية.

2.1 متصفح ميب MIB Browser

متصفح "ميب" هو وسيلة إلكترونية لمشاهدة وعرض عناصر MIB، بعد تحميلها من أجل إيجاد معلومات معينة. يعرض متصفح "ميب" المجموعات المختلفة في قاعدة المعلومات الإدارية MIB بطريقة رسومية، مثل شجرة مستعرضة، كما يمكننا من إجراء البحث عن وظيفة محددة في معلومات "ميب"، حيث يمكن استخدام جهاز الماوس المتصل بالحاسوب واستعراض شجرة "ميب"، وفحص عناصرها على حدة، أو معرفة مجال معلومات معينة خاصة بمعدلات الخطأ في قاعدة "ميب". في هذه الحالة، على سبيل المثال، نستطيع كتابة كلمة "errors" على الشاشة، ويقوم المتصفح بإظهار جميع العناصر الخاصة بهذا الموضوع. وتشبه هذه الخاصية في المتصفح عملية وجود فهرس لقاعدة المعلومات "ميب". يوضح الشكل 7.3 مثالاً لشاشة عرض لمتصفح بسيط.



شكل7.3 متصفح MIB بسيط.

توفر العديد من برامج نظم إدارة الشبكات وجود متصفح لقاعدة المعلومات الإدارية بها. بعض هذه النظم تمكننا من إجراء الاستفسار من "ميب" بواسطة استخدام جهاز الماوس، وعرض شرح رسومي لقاعدة "ميب" (مثل منتجات شركتي HP Open View, Cabletron Spectrum). تتيح بعض الشركات الأخرى وسائل لنظام قوائم حسب احتياج المستخدم، كي تبين هيكل "ميب"، مثل برنامج نظام شركة (Sun Connect Sun-Net Manager).

أسئلة تقويم ذاتي

اذكر أنواع ثلاث أدوات يمكن أن تستخدم للمعاونة في فحص عناصر قاعدة المعلومات الإدارية في الشبكة.

أكمل ما يلي:

أ) يستخدم مترجم ميب في .....

ب) يستخدم متصفح ميب في : .....

3.1 أداة الأسماء المستعارة MIB Aliases

أداة ميب للاسم المستعار، هي أداة تساعدنا في فهم أسماء عناصر "ميب" شديدة الإرباك، وذلك بتحديد صلة أسماء هذه العناصر بأسماء أكثر ألفة لنا نستطيع فهمها بسهولة.

عندما يتم إيجاد العناصر المهمة من قاعدة المعلومات الإدارية MIB الجديدة، يكون من المفيد أن يصاحب اسم العنصر حروف أكثر ألفة لنا يسهل فهمها. تقوم أداة تحديد الأسماء المستعارة MIB Aliases بتوفير هذه المهمة. على سبيل المثال، يحتوي جدول الوحدات البينية Interface Table على عنصر يسمى ifInOctets، الذي يعدُّ عدد الحروف Octets المستقبلة من الوحدة البينية. وبما أن الحرف Octet هو عبارة عن Byte، فإن هذا العنصر يقوم بعدِّ عدد Bytes في الدخل لهذه الوحدة البينية. لكن بسبب أن الحروف Octets لا تكون مألوفة للبعض، فإن النظام يسمح لنا بأن يصاحب هذا الاسم مسميات توضح معناه. مثلا يمكن تخصيص بند يرافق كلمة octet، مثل عبارة Total-Input-Bytes، وتعني "إجمالي حروف الدخل"، تكون أكثر وضوحا وسهلة الفهم للقارئ المتوسط.

تمتاز أداة الأسماء المستعارة MIB Aliases بأنها مقيدة ، وتجعل أسماء عناصر "ميب" أكثر وضوحا وفهما للمستخدمين، لذلك فإنها توجد في العديد من برامج نظم إدارة

الشبكة. لكن بسبب وجود أعداد ضخمة للغاية من عناصر "ميب"، فإنه – يصعب غالباً– القيام بتوفير أسماء مستعارة لكامل مجموعة العناصر التي يمكن أن يستعملها المستخدم.

4.1 أداة الاستفسار MIB Query

تقوم أداة استفسار ميب بتصويت poll الوكلاء في أجهزة الشبكة، كي تفحص القيم العائدة التي يمكن أن تعاون مهندس الشبكة في تحديد ما إذا كانت عملية التصويت على العنصر ستكون مفيدة.

بعد تصفح قاعدة المعلومات "ميب" ، وتهيئة الأسماء المستعارة aliases، فقد نحتاج بعد ذلك لإجراء عملية البحث عن القيم العائدة بواسطة وكيل جهاز الشبكة. إذ يمكن أن يكون وصف عنصر "ميب" غامضا ويحتاج إلى توضيح. أحد الوسائل لإجراء ذلك هو الاستفسار من جهاز الوكيل عن العناصر من قاعدة المعلومات MIB الجديدة، وبعد ذلك نفحص النتيجة. لذلك ينبغي أن تسمح لنا أدوات "ميب" بإجراء الاستفسار مرة كل فترة one-time عن عنصر محدد في قاعدة "ميب". وبذلك نتمكن من معرفة ما إذا كانت المعلومات العائدة من الوكيل لها علاقة بحالة التشغيل الحالية، أم لا.

يمكن أن تمتد هذه الأداة لتسمح لنا بإنشاء استفسارات "ميب" بحسب احتياجات كل المستخدمين. إن الاستفسار المهيأ للمستخدم Custom Query هو عبارة عن مجموعة من عناصر MIB محددة توجد في أي قاعدة معلومات إدارية، يمكن أن يفهمها النظام. إن الهدف من الاستفسار المهيأ للمستخدم هو استرجاع معلومات محددة من الجهاز، وهذه المعلومات لا يستطيع نظام إدارة الشبكة إظهارها، أو عرضها في شكلِ شكلٍ نود تغييره. باستخدام الاستفسار المهيأ للمستخدم، نستطيع إنشاء رؤيتنا الخاصة لعناصر MIB. يوجد طريقتان شائعتان لبناء الاستفسار المهيأ للمستخدم، هما: طريقة الشفرة الزائفة Pseudo Code، وطريقة النوافذ.

أولا: طريقة الشفرة الزائفة :

تسمح طريقة الشفرة الزائفة بإنشاء ملف يحتوي على أوامر لبناء الاستفسار المهيأ للمستخدم. تمتاز هذه الطريقة بأنها سهلة الاستخدام عند إجراء استفسار منفرد مهيأ للمستخدم، وبعد ذلك يمكن نسخه لإجراء استفسارات أخرى عديدة بسرعة. من عيوب هذه الطريقة أنه ينبغي على مهندس الشبكة أن يتعلم لغة هذه الشفرة الزائفة وقواعدها.

ثانيا: طريقة النوافذ

في هذه الطريقة يتم عرض نافذة فارغة، يتم من خلالها إجراء توليد الاستفسار بواسطة التجول خلال قوائم Menus باستخدام الماوس، وتحديد أين سيكون الخرج على النافذة. على سبيل المثال، يمكن أن نختار عناصر "ميب" بواسطة متصفح "ميب"، وبعد ذلك نحدد أين يظهر خرجها على النافذة الفارغة الخاصة بالاستفسار المهيأ للمستخدم.

تمتاز طريقة النوافذ في إنشاء الاستفسار المهيأ للمستخدم بأنها لا تحتاج من مهندس الشبكة بأن يتعلم لغة الشفرة الزائفة، كما أنها تمكن المهندس من معرفة تغذية راجعة فورية عن كيفية ظهور خرج الاستفسار. لكن العيب الأساسي لهذه الطريقة، هو أنه ينبغي على مهندس الشبكة أن يقوم بعرض و تصفح العديد من القوائم من أجل إنشاء الاستفسار المهيأ للمستخدم.

على سبيل المثال

نفترض قاعدة "ميب" لمحطة عمل خاصة بمورد محطة عمل تسمى Station4Me، تسمح لنا بالاستفسار من الوكيل عن عدد المستخدمين داخل النظام، وكذلك زمن المعالجة المخصص لجلساتهم الحالية. بسبب أن قاعدة هذه المعلومات "ميب" خاصة بالمورد ، فإن نظام إدارة الشبكة لا يوجد به نافذة قياسية لعرض ورؤية هذه المعلومات. لحل هذه المشكلة، يمكن أن يتم بناء "استفسار مهيأ للمستخدم" لعرض المعلومات الضرورية. بعد ذلك، يستخدم الاستفسار المهيأ للمستخدم لمعرفة عدد المستخدمين، وزمن المعالجة الخاص بجلساتهم الحالية على أي محطة عمل من نوع Station4Me.

يوجد في الأسواق العديد من برامج إدارة الشبكات توفر وسيلة الاستفسار عن عناصر "ميب" محددة، وكذلك إنشاء استفسارات مهيأة للمستخدم. وأن معظم هذه البرامج تستخدم طرقاً رسوميةً لبناء الاستفسار، وبعد ذلك إنشاء هذا الاستفسار داخل قوائم النظام البرمجي. في حالات كثيرة، عندما يتم إنشاء الاستفسار المهيأ للمستخدم على هذه البرامج، فإن المستخدم العادي الذي لا يعرف هذا البرنامج، يظن أن هذا الاستفسار المهيأ للمستخدم (والذي قد تم إنشاءه) من ضمن خواص البرنامج القياسية.

أسئلة تقويم ذاتي

أكمل ما يلي:

أ) تستخدم أداة استفسار ميب في : .....

ب) تستخدم الشفرة الزائفة ملف يحتوي على : .....

بيِّنْ استخدام أداة الأسماء المستعارة Aliases .

اذكر طريقتين لبناء الاستفسار المهيأ للمستخدم ، وقارن بينهما من حيث المميزات والعيوب.

أسئلة تقويم ذاتي

يبين الجدول التالي بعض الأدوات المعاونة في إدارة الشبكة واستخداماتها قم بتوفيق الإجابات الصحيحة.

رقم الأداة	مسمى الأداة	استخدامها	رقم الإجابة
1	مترجم ميب	إنشاء تقارير مهيأة للمستخدم.	.....
2	متصفح ميب	عرض الرسائل التي يتم توليدها بواسطة التطبيق.	.....
3	استفسار ميب	عرض معلومات ميب بطريقة رسومية.	.....
4	الاسم المستعار	ترجمة ملف ASN.1 ليناسب إدارة الشبكة.	.....
5	السجل المركزي	تفسير عناصر ميب شديدة الإرباك.	.....
6	كاتب التقرير	الاستفسار من الوكيل عن عناصر ميب الجديدة.	.....

2. أدوات العرض Presentation Tools

عزيزي الدارس،

إن عرض المعلومات على مهندس الشبكة هي وظيفة عصيبة وحاسمة Crucial لنظام إدارة الشبكة. حيث إن العديد من التطبيقات تحاول التعبير عن معلوماتهم بطريقة سهلة الفهم. لكن، يمكن أن يستخدم مهندس الشبكة أدوات العرض التالية في جميع التطبيقات، حيث إنها بوجه عام تساعد في زيادة إنتاجية النظام. وتتضمن هذه الأدوات السجل المركزي، كاتب التقرير والحزم الرسومية.

1.2 السجل المركزي Centralized Log

يوفر السجل المركزي لمهندس الشبكة وسائل لتتبع نشاط الشبكة كما يراها النظام، ويشمل رسائل النظام وأحداث الشبكة.

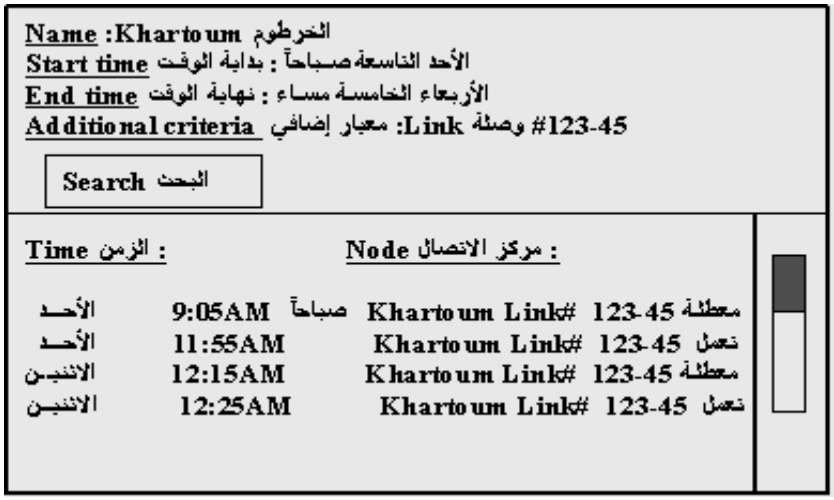
تعرض أداة السجل المركزي الرسائل التي يتم توليدها بواسطة تطبيقات مختلفة، وتتيح لنا مكاناً واحداً لنظام رصد الحالة. يأتي دخل هذه الأداة من التطبيقات التي تعمل في نظام إدارة الشبكة. عندما يجد التطبيق حدثاً هاماً، يستطيع إدخاله في السجل، إما آليا أو بواسطة مهندس الشبكة. إن تحديد أهمية الحدث تعتمد على نوع التطبيق. على سبيل المثال، إن تطبيق إدارة الأعطال الذي يقوم بإجراء عملية التصويت للأجهزة لتحديد توصيلها الحالي، سوف يعتبر أن فقد الاتصال بالجهاز يعتبر حدثاً هاماً ويقوم آليا بإدخال هذا الحدث إلى السجل المركزي. من ناحية أخرى، إن أداة إدارة الأداء التي ترصد الإحصاءات والحدود المسموحة، يمكن أن تهيأ بحيث تحدد لنا ما إذا كان تخطي الحدود المسموحة يعتبر حدثاً مهماً يمكن إدخاله إلى السجل المركزي أم لا.

يمكن أن يعرض السجل المركزي أحداث الشبكة، مثل استقبال رسالة التطوع (رسالة مصيدة سنمب- ف1)، أو فقد عملية الاتصالية بجهاز محدد قد تم معرفته من خلال إجراء عملية التصويت. كما ينبغي أن تتيح أداة السجل المركزي وسيلة لإجراء عملية البحث عن أحداث محددة خلال فترات زمنية، كما هو موضح في الشكل 7.4.

يستخدم نظام إدارة الشبكة ملف أسكي أو قاعدة بيانات علاقية، لتخزين السجل المركزي. إن اختيار هاتين الطريقتين أو إحداهما يعتمد على التهيئة الاختيارية لأداة السجل المركزي.

تستخدم معظم تطبيقات برمجيات إدارة الشبكة أدوات لإجراء عمليات السجل. وتستخدم شركتا HP Open View, IBM Net View/AIX سجلات متتابعة تعرض في سجل منفصل، يحتوي كل سجل رسائل عن مجموعة أحداث محددة. كما تستخدم شركة Sun Connect برنامج Sun Net Manager يوجد به نافذة تسجيل رئيسية لعرض جميع

أحداث الشبكة. تدعم جميع هذه البرمجيات وجود وسيلة للاستفسار من السجلات بواسطة اسم المضيف Host Name . كما أن معظم هذه النظم تخزن معلومات السجل في ملف أسكي. لذلك فإن بعض تطبيقات إدارة الشبكة تختار أن تأخذ المدخلات من السجل الموجود بالبرنامج، وتضعه داخل قاعدة بيانات علائقية، حيث يمكن أن يخزن ويتم إجراء عمليات البحث به، كما يمكن ربطها بالأحداث الأخرى التي تقع في الشبكة.

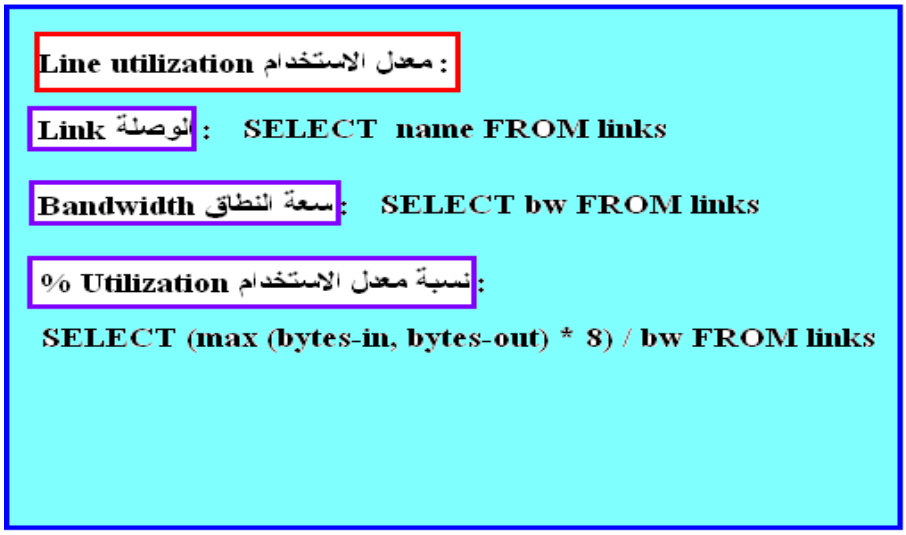


شكل7.4 عينة من أداة السجل المركزي ، مع عملية تحديد البحث.

2.2 كاتب التقرير Report Writer

تسمح أداة كاتب التقرير لمهندس الشبكة بإنشاء تقارير مهيأة للمستخدم. على الرغم من إمكانية وجود أدوات أخرى في النظام يمكن أن تنشئ تقاريرها الخاصة؛ فقد نحتاج إنشاء تقرير خاص غير متاح إنشاؤه بواسطة النظام الافتراضي Default System. إن الأداة المفيدة هي التي تتيح وسيلة عامة لاستخلاص البيانات من قاعدة البيانات خلال SQL، وبعد ذلك يتم توليد التقارير بناء على هذه البيانات. وبذلك يكون شكل التقرير الذي نحدده يمكن أن يحتوي أي جمل SQL صالحة، متضمنة معادلات حسابية. يمكن أن تسمح الأداة أيضا بإنشاء تقارير عند فترات زمنية: يومية، أسبوعية، شهرية، أو سنوية.

ينبغي أن يتم تحديد المعلومات المطلوب استخلاصها من قاعدة البيانات لأداة كاتب التقرير، وكيفية عرضها داخل التقرير. ويمكن أن تستقبل الأداة بيانات الدخل من خلال وحدة واجهة رسومية. على سبيل المثال، يمكن توفير قالب فارغ Blank Template، ونستخدم الماوس ووحدة المفاتيح لتحديد النص والمعلومات المسترجعة من قاعدة البيانات، كما هو موضح في الشكل 7.5. تسمح لنا هذه الطريقة برؤية شكل التقرير قبل أن يتم توليده. وتشبه هذه الطريقة، الطريقة السابقة المستخدمة في إنشاء نافذة استفسارات MIB المهيأة للمستخدم.



شكل7.5 عينة تقرير معدل الاستخدام وأسماء الوصلات وسعة النطاق.

<u>على سبيل المثال</u>: يمكن إنشاء تقرير إدارة الأداء؛ لتوضيح معدل استخدام الوصلة الموجودة داخل أحد الشبكات أثناء فترات ذروة استخدام الشبكة. حيث يمكن تهيئة كاتب التقرير لإنشاء تقرير يعرض أسماء الدوائر، وسعة النطاق، ونسبة معدل الاستخدام. يمكن أن يقوم النظام بإنشاء هذا التقرير مبكراً كل صباح، وذلك لعرض معدل الاستخدام عن اليوم السابق.

ويوجد العديد من برامج كاتب التقرير متاحة في الأسواق، وتعمل مع نظم قواعد البيانات العلائقية. عندما يستخدم برنامج إدارة الشبكة، قاعدة بيانات علائقية شائعة مثل:

أوراكل Oracle، أو سيباس Sybase، أو إنجريس Ingres، أو إنفورمكس Informix، فإن المؤسسة غالبا ما توصي بوجود برنامج كاتب التقرير. إن البرامج المختلفة لكاتب التقرير، تحتوي عادةً على حزم رسومية، تسمح لمهندس الشبكة ببناء تقارير مهيأة للمستخدم بطريقة سهلة.

3.2 الحزم الرسومية Graphic Packages

توفر الحزم الرسومية لمهندس الشبكة وسيلة لرؤية البيانات على شكل رسومات بيانية. يمكن أن يتم توفير هذه الحزم الرسومية بواسطة النظام أو من خلال وحدات بينية لهذه الحزم ، وتكون قادرة على عرض المعلومات على شكل رسومات خطية، أو قضبان، أو فطيرة Pie.

إن الحزم الرسومية العامة يمكن أن توفر وسيلة أخرى لتمثيل المعلومات. إن أدوات عديدة في معظم مجالات أداة إدارة الشبكة، تستفيد من امتلاكها حزماً رسوميةً لعرض البيانات. مثل برنامج كاتب التقرير، فإن الحزم الرسومية، يمكن أن تستخرج المعلومات المخزنة في قاعدة البيانات، وتسمح لنا بإنشاء الرسومات التي نحتاجها. يمكن لهذه الحزم البرمجية أن تنشئ: رسومات خطية ، قضبانية ، أو على شكل فطيرة. بسبب أن التعبير عن البيانات بطريقة رسومية يكون شديد الأهمية في إدارة الشبكات؛ فإن معظم برامج إدارة الشبكات تدعم وجود هذه الحزم الرسومية.

أسئلة تقويم ذاتي

اشرح وظائف اثنتين فقط من أدوات العرض التالية، مع إعطاء مثال توضيحي:

أ) السجل المركزي. ب) كاتب التقرير. ج) الحزم الرسومية.

3. أدوات حل المشاكلProblem Solving Tools

عزيزي الدارس،

تعين الأدوات الذكية المستخدمة في نظم إدارة الشبكة، مهندس الشبكة في تتبع المشاكل وحلها. تختص أولى هذه الأدوات بنظم تتبع المشكلة، وتسمح بتتبع المشكلة منذ لحظة اكتشافها إلى لحظة عزلها. المجموعة الثانية من هذه الأدوات، تساعد مهندس الشبكة في إجراء عمليات تحليل تصميم الشبكة لمحاولة تجنب المشاكل قبل حدوثها. الأداة الثالثة هي النظم الخبيرة. وهى تستخدم مجموعة من القواعد مع بيانات الشبكة، لتقييم الشبكة وعرض مقترحات تعاون مهندس الشبكة في حل المشاكل الخاصة بالشبكة. حيث يستطيع النظام الخبير أن يتعلم من المشاكل السابقة، ويقوم بإجراء تغيير قواعده حسب الاحتياج. ونناقش تباعاً هذه الأدوات بالتفصيل.

1.3 نظم تتبع المشكلات Trouble Tracking Systems

يقوم نظام تتبع المشكلة برصد الشبكة، وعرض المشاكل الخاصة بإدارة الأعطال وجميع المفاهيم الأخرى الخاصة بإدارة الشبكة. على سبيل المثال، يمكن للنظام تتبع تغيرات التهيئة، تعديلات الأمن، وطلبات الأداء وتحسينها، وكذلك مصادر الحسابات. يمكن أن يشمل نظام تتبع المشكلة الخطوات التالية:

أولا: إصدار بطاقة لوصف المشكلة:

يمكن أن يقوم النظام بإنشاء بطاقة جديدة New Ticket لكل مشكلة محددة. تحتوي كل بطاقة على تسجيل بيانات عن المشكلة، والإجراءات اللازمة للتعامل معها من البداية حتى النهاية. يمكن لمهندس الشبكة أو فني الشبكة أن يحرر هذه البطاقة يدويا بواسطة

إدخال كل المعلومات المعروفة عن المشكلة. على سبيل المثال، قد تحتوي هذه المعلومات على اسم الجهاز، المناطق المتأثرة في الشبكة، الشخص الذي يدير الجهاز.

ثانيا: تعبئة بيانات البطاقة آليا:

يمكن لنظام إدارة الشبكة أن يقوم بتعبئة معلومات البطاقة آلياً. حيث يتم بدء هذا العمل عندما يتم تدوين حدث بالشبكة بواسطة الأداة الإدارية. على سبيل المثال، إن أدوات إدارة الأعطال يمكن أن تتبع خطوات لحل المشكلات. كما يمكن للنظم الخبيرة أيضا أن تساعد النظام آلياً نحو حل المشكلة. عندما لا يستطيع النظام عزل المشكلة، يتم إنشاء بطاقة المشكلة التي تحتوي على المعلومات اللازمة (اسم الجهاز، الشخص المسئول، الخ)، ويتم الحصول عليها من قاعدة المعلومات العلاقية.

ثالثا: إحالة البطاقة:

بعد أن يقوم النظام بإنشاء البطاقة، يتم إحالتها إلى مهندس الشبكة. إن عملية إحالة البطاقة يساعد ضمان أن المشكلة يتم توزيعها بشكل عادل على المهندسين العاملين بالشبكة. على الرغم من أن النظام يقوم بإحالة المشاكل آلياً؛ فإن معظم المؤسسات يمكن أن تفضل إحالة هذه البطاقات يدويا، حيث أن بعض المهندسين ربما يكون لديهم معرفة مسبقة لمشاكل محددة، أو يكون لديهم دراية وظيفية بهذه المشاكل.

رابعا: تصنيف المشكلة:

عندما يتم إحالة المشكلة إلى مهندس الشبكة، ينبغي أن يتم تصنيفها آلياً بواسطة النظام، أو يدوياً بواسطة المهندس. يعين هذا التصنيف مهندس الشبكة في المستقبل، عندما يقوم بمحاولة تحديد مشاكل متكررة الحدوث. يمكن أن تتضمن بعض التطبيقات الشائعة: أعطال الوصلة، أعطال جهاز الشبكة، خرق الأمن Security Breach، أخطاء التهيئة، مشاكل الأداء، مشاكل الحسابات. يوضح الشكل 7.6 عينة لبطاقة تدوين مشكلة.

شكل 7.6 عينة لبطاقة تدوين مشكلة.

خامساً: تخزين المعلومات:

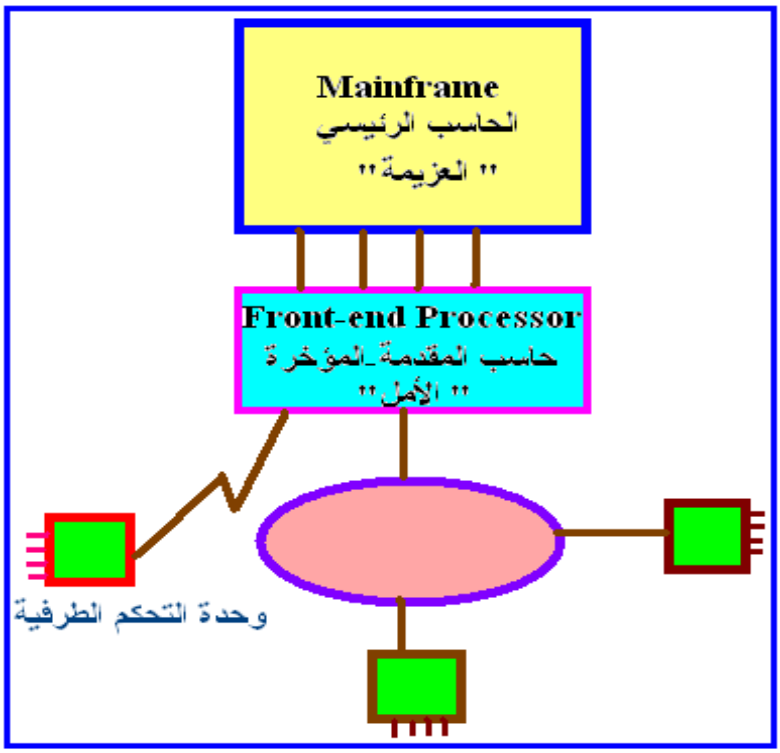
يقوم نظام تتبع المشكلة بتخزين جميع المعلومات عن البطاقات في قاعدة البيانات العلاقية، لذلك نستطيع تصفح قاعدة المعلومات لمعرفة المشاكل السابقة التي قد يكون لها علاقة بالمشكلة الحالية. ينبغي أن تكون وسيلة التصفح سهلة الاستخدام، وأن تسمح لنا بإجراء عملية البحث SQL. على سبيل المثال، يمكن أن نقوم بإدخال بعض الكلمات من وحدة المفاتيح إلى النظام مثل "الخرطوم: ، "أم درمان" ، ودائرة الاتصال رقم "123-456-7755" للبحث عن الخبرات السابقة عن هذه الدائرة. يقوم النظام بعد ذلك بإجراء عملية البحث اللازمة باستخدام SQL وإنشاء قائمة بجميع البطاقات السابقة التي تتوافق مع رقم هذه الدائرة.

سادساً: عملية البحث:

يمكننا في نظام التوليد الآلي للبطاقات إجراء عملية البحث في قاعدة بيانات النظام للإطلاع على مشاكل مشابهة. بذلك يمكننا استقبال البطاقات وكذلك قائمة المشاكل السابقة المشابهة للمشكلة الحالية، وتفيد هذه المعلومات في حل المشكلة. يمكن استخدام قاعدة بيانات نظام تتبع المشكلة لإجراء عمليات البحث وتجميع بيانات عن نوع المشاكل السابقة، ومعدل تكرارها. يمكن إدخال هذه المعلومات إلى برنامج كاتب التقرير، وإنشاء قائمة بالتقارير المتاحة عن عدد المشاكل السابقة الخاصة بعطل معين، مثل: عطل الوصلة، اختراق الأمن، أجهزة من مورد معين، وهكذا.

سابعاً: إنشاء تقرير:

يمكن إنشاء تقرير يوضح المشاكل التي تستغرق وقتا ومصادر من مهندس الشبكة. كما يمكن استخدام الحزم الرسومية لإنشاء رسومات بيانية توضح هذه المعلومات. على سبيل المثال، نفترض أننا قمنا بتحديث العتاد الخاص بجهاز حاسوب المقدمة والمؤخرة Front-End المسمى "الأمل"، المتصل بجهاز الحاسب الرئيسي Mainframe المسمى "العزيمة" في الشبكة، كما هو موضح في الشكل 7.7. يتطلب تحديث هذا العتاد أيضا، أن يتم إعادة تهيئة الحاسوب الرئيسي. لذلك نحتاج إصدار بطاقتين لتحديد هاتين المشكلتين، ليتم إدخالهما إلى النظام. البطاقة الأولى خاصة بتغيير تهيئة العتاد الخاص بحاسوب "الأمل"، والبطاقة الثانية خاصة بعمل التغيرات اللازمة لتهيئة برنامج حاسوب "العزيمة". يتم تصنيف البطاقة الأولى تحت مسمى :تحديث عتاد"، والثانية تحت عنوان "تعديل التهيئة". يقوم المهندسون القائمون بحل هاتين المشكلتين بتسجيل الخطوات التي تم اتخاذها على هاتين البطاقتين. بعد ذلك يتم إتاحة هذه البيانات كي تساعد في حل مشاكل مستقبلية مشابهة.



شكل 7.7 يخدم حاسب المقدمة والمؤخرة "الأمل"، محكمات الوحدات الطرفية لجلسات المستخدمين المتصلين بالحاسوب الرئيسي "العزيمة".

إن نظم تتبع المشكلة عموماً ليست جزءاً من النظم البرمجية لإدارة الشبكات، لكنها عادةً تكون ضمن التطبيقات المتصلة بهذه النظم. من أمثلة ذلك، نظام Action Request الصادر من شركة ريميدي كوربوراشن Remedy Corporation، والذي يعمل مع العديد من البرمجيات المشهورة لنظم إدارة الشبكات.

2.3 أدوات تصميم الشبكة

يمكن أن تساعدنا أدوات تصميم الشبكة في إجراء بعض المهام التي تجنبنا مشاكل مستقبلية في شبكة البيانات. تتعلم أداة تصميم الشبكة تهيئة الشبكة، بعد ذلك تسمح لنا بإجراء التعديلات ورؤية كيفية تأثير تدفق حركة المرور والأداء.

لكي تتعلم أدوات التصميم عن تهيئة الشبكة؛ فإنها تحتاج إدخال معلومات التهيئة عن كل جهاز في الشبكة. يمكن أن يتم الحصول على هذه المعلومات من ملفات نصية تصف تهيئة الجهاز، أو من بروتوكول إدارة الشبكة. على سبيل المثال، تستطيع الأداة قراءة ملف تهيئة النظام CONFIG.SYS من كل حاسوب شخصي يعمل بنظام التشغيل DOS، أو يستعلم عن معلومات الأجهزة من قاعدة المعلومات الإدارية MIB-II من مجموعة النظام.

إن عملية جعل الأداة تقوم بتفسير ملف التهيئة النصي لكل جهاز موجود بالشبكة تستغرق وقتاً. بالإضافة إلى أن العديد من الأجهزة لا تدعم بروتوكول إدارة الشبكة، كما أن المعلومات المتاحة في قاعدة المعلومات الإدارية MIB-II تكون غير كافية لتعلم التهيئة الكاملة عن كل جهاز، ويعني ذلك أنه ينبغي على الأداة أن تتعلم كيفية استخدام جميع قواعد المعلومات الإدارية الممكنة للموردين، وهذا ليس حلاً عملياً.

لهذه الأسباب، فإن العديد من نظم تصميم الشبكات تستخدم طرقاً مركبةً، وتحصل على معلومات حزم البيانات من الشبكة الحالية، بالإضافة إلى المعاونة في تحديد تهيئة الشبكة. بعض الأدوات تستخدم مجسات الرصد عن بعد RMON Probes لإجراء هذه المهمة، وذلك عند إتاحة هذه الإمكانية بالشبكة.

عندما نحاول استخدام أدوات تصميم الشبكة قبل بنائها، فإن الطرق التي تم شرحها لتحديد التهيئة الحالية للشبكة لا يكون لها معنى. لذلك بعض أدوات تصميم الشبكات يوجد بها عينات من الأجهزة تمثل أنواعاً مختلفةً من مكونات الشبكة. يمكن أن نستخدم عينات هذه الأجهزة وتطويعها لتوافق أجهزة الشبكة التي سوف يتم بناؤها وتوظيفها. إن هذه الطريقة لا ينتج عنها تمثيل حقيقي للشبكة، لكنها تكون غالباً قريبةً بدرجةٍ كافيةٍ من أجل عمل تحليل مبدئي لتصميم الشبكة.

يكون خرج تعليم التهيئة من الشبكة الحالية، أو من الشبكة المستقبلية عبارة عن خريطة رسومية للشبكة. يمكن أن يتم إضافة أو حذف أجهزة من خريطة الشبكة، أو نقل أجهزة إلى أماكن جديدة. يمكن بعد ذلك استخدام أداة تصميم الشبكة لإجراء عملية تحليل نماذج

حركة المرور في الشبكة الجديدة التي تم تصميمها، وإيجاد الثغرات الأمنية، وإنشاء رسومات وتقارير عن أداء الشبكة. يعتمد تحليل الأداء على الأداة التي نستخدمها، ويمكن تحسين هذه التحليلات باستخدام النظم الخبيرة. تساعد هذه التحليلات في إنشاء شبكة بيانات ذات أعطال أقل، ومشاكل تهيئة أقل، وكذلك بأقل مشاكل في الأداء.

يوجد بعض الشركات التي تقوم بتوفير أدوات تصميم الشبكة، مثل شركات:
Make Systems, Comdisco Systems, Optimal Networks, and Net-Sys Technology.

يحتاج مهندس الشبكة أن يحدد بالضبط أجهزة الشبكة المطلوبة في إجراء عملية التحليل، حيث أن معظم أدوات تصميم الشبكة لا تعمل مع كل جهاز محتمل يوجد في الشبكة.

3.3 النظم الخبيرة Expert Systems

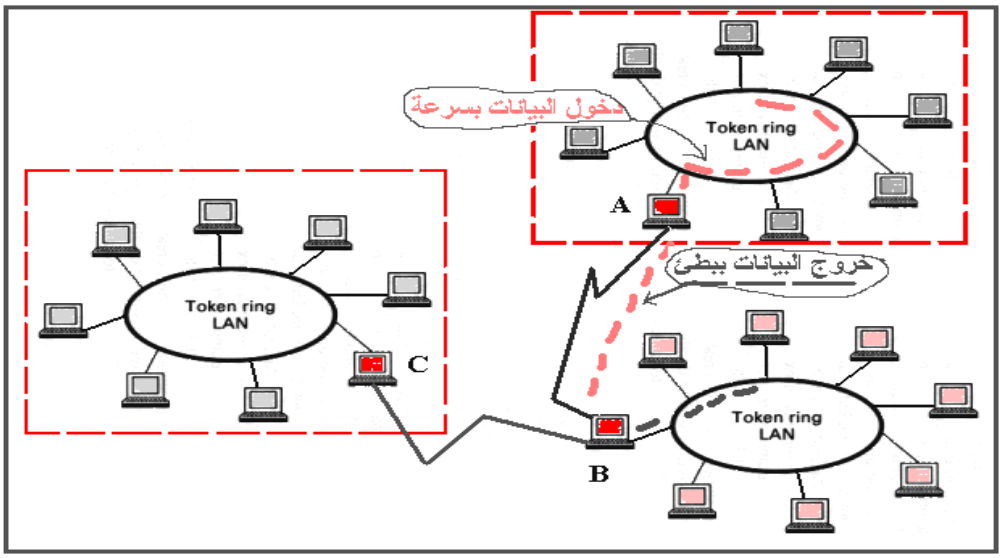
يمكن أن يتم إدخال الوضع الحالي للشبكة إلى نظام خبير، وتقييم البيانات، وحساب مصدر المشكلة، ويتم اقتراح العمل اللازم لإجراء حل المشكلة. يمكن أن يقوم النظام الخبير بإجراء هذه الخطوات كجزء من تحليل تصميم الشبكة، أو للمعاونة في تشخيص أعطال مشكلة، حيث يستخدم النظام الخبير مجموعة من القواعد، ومجموعة من الشروط if-then-else المتتابعة. تقوم الأداة باتباع هذه القواعد للوصول إلى مقترحات. بناءً على هذه النتائج، يستطيع النظام الخبير بعد ذلك، اختبار بعض هذه المقترحات، دون الاحتياج إلى مهندس الشبكة لإجراء كل خطوة يتم تنفيذها نحو حل المشكلة.

عموماً، إن إتاحة مجموعة عامة من القواعد يمكن أن تكون بداية جديدة نحو حل المشكلة. من الناحية العملية، فإن القواعد العامة غالباً ينشأ عنها اقتراحات عامة، مثلاً: افحص جهاز المودم، بدلاً من ذكر حلول صريحة للمشكلة. على الرغم من أن هذه المقترحات ربما تساعد مهندس الشبكة المبتدئ (قليل الخبرة)، لكنها لا تعاون كثيراً مهندس الشبكة الذي يعرف فعلاً ما هو العمل المطلوب اتخاذه نحو حل المشكلة.

على سبيل المثال، عندما تعطل وصلة الربط، فإن النظام الخبير قد يقترح لنا الحلول العامة التالية: افحص أجهزة المودم عند كل نهاية، افحص التهيئة وإمكانية الوصول

Reachability لأجهزة الشبكة عند كل طرف، وقم باستدعاء مورد الشبكة. بناءً على نتائج الاختبارات، يمكن أن يصدر النظام الخبير بطاقة تحديد المشكلة ويدون الخطوات التي تم إجراؤها.

إن أساس النظام الخبير هو مقدرته على استخدام الخبرات السابقة أو البيانات الماضية لتعديل قواعده، وبذلك يمكن أن يصل إلى مقترحات الحل سريعاً. على سبيل المثال، نفترض أن شبكة حلقية من نوع Token Ring، تعاني مشكلة في الأداء، كما هو موضح في الشكل 7.8. حيث يسبب الجهاز "A" معدل إرسال بطئ، مسبباً مشكلة في الأداء، عندما يحدث حمل مكثف Heavy Load.



شكل7.8 يسبب الجهاز "A" معدل إرسال بطئ، مسببا مشكلة في الأداء،

عندما يحدث حمل مكثف Heavy Load.

يمكن أن يقترح النظام الخبير قائمة بالحلول الممكنة، كما يلي:

- الحلقة الفيزيقية مفتوحة.
- يوجد محطة عمل في الحلقة لا تعمل بشكل صحيح.
- وحدة الوسط الملحقة بالشبكة بها عطل.
- كابل الحلقة غير مطابق للمواصفات.

يبدأ النظام الخبير بتقييم كل إمكانية على الشبكة، وبعد ذلك يفحص كل حل ممكن على التتابع. عندما يجد أن الحلول الثلاثة الأولى غير حقيقية، فإنه يقترح لنا أن الحل الرابع هو الممكن، وهو أن طول كابل الحلقة مخالف للمواصفات، وقد يكون هو سبب المشكلة. بالتالي سوف يقوم بإصدار بطاقة وتدوين هذه المشكلة. لكننا نكتشف في الحقيقة أن مشكلة الأداء ناتجة عن أن جهاز الشبكة يقوم بتوصيل حزم البيانات بين الحلقة المتصلة محلياً، ووصلة التوالي قد أصبحت مزدحمة بحركة المرور في الحلقة. حيث إن جهاز الشبكة لا يستطيع إرسال الأطر frames بالسرعة التي تسمح بها الحلقة، بذلك تنتج مشكلة الأداء. يمكننا بعد ذلك إدخال هذا الحل، وهو تحديث جهاز الشبكة، إلى بطاقة تدوين المشكلة. يمكن أيضا، إدخال هذه المعلومات إلى النظام الخبير، بالشكل الذي يسمح له بتعديل مجموعة قواعده. وبالتالي فإنه في المرة التالية، عندما تحدث مشكلة في أداء هذه الحلقة، يستطيع النظام الخبير الالتفاف حول أول ثلاثة فحوص، وبعد ذلك يحاول اختبار أداء جهاز الشبكة قبل إصدار بطاقة تحديد المشكلة. إذا كان جهاز الشبكة هو سبب مشكلة الأداء، فإن النظام الخبير سوف يكون لديه الحل الصحيح ويستطيع أن يشير لنا مباشرة إلى هذا الحل.

على الرغم من أن النظم الخبيرة يمكن أن تقدم لنا حلولاً معقولة للمشاكل الروتينية لمهندس الشبكة، فإنها تحتاج وقتا كي يتم تطورها. عندما تسمح التقنيات المتطورة بناء نظم خبيرة مركبة سريعة وفعالة، فإنها سوف تؤثر بشكل جيد جداً على الأداء الوظيفي في كل مراحل إدارة الشبكة.

أسئلة تقويم ذاتي

اختر الإجابة الصحيحة:

– من أدوات حل مشاكل وتحليل بيانات أجهزة الشبكة ما يلي:

أ) نظام تتبع المشكلة.

ب) أدوات تصميم الشبكة.

ج) النظم الخبيرة.

د) لا شيء مما سبق.

هـ) أ، ب ، ج .

– اشرح طريقةً لنظام تتبع مشكلات الشبكة، وارسم شكلاً يوضح محتويات بطاقة تدوين المشكلة، موضحاً عناصرها على الرسم.

– اشرح كيف تحصل أدوات تصميم الشبكة على معلومات تهيئة الشبكة، وكيف تعاون هذه المعلومات في تصميم الشبكة.

– اكتب نبذة مختصرة عن كيفية استخدام النظام الخبير في تشخيص أعطال شبكة البيانات، وحل بعض مشاكلها. اذكر بعض الأمثلة التوضيحية.

نشاط

تدريبات وتطبيقات عملية

يبين الجدول7.1 بعض الأدوات المعاونة في إدارة الشبكة. يمكن للدارس أن يقوم بتحميلها مجاناً من شبكة الإنترنيت. معظم هذه البرامج مبسطة ويمكن التعامل معها بواسطة تشغيلها على جهاز الحاسب الشخصي .

جدول7.1 بعض الأدوات المعاونة في إدارة الشبكة.

مسمى الأداة	عنوان الموقع على شبكة الانترنيت
متصفح MIB	www.oidview.com/mibbrowser.html www.ireasoning.com/mibbrowser.shtml
مترجمMIB	www.logisoftar.com/MibCompiler.htm www.ndt-inc.com/SNMP/MIBCompiler.html
الاستفسار Query	www.freedownloadmanager.org/downloads/snmp_monitor_software/ www.bluechillies.com/list/free-snmp-monitor.html
الرسم Graph	www.manageengine.adventnet.com/products/oputils/snmp-tools.html www.crypton.co.uk/freetools.html

الخلاصة

عزيزي الدارس،

عرضت الوحدة أدوات قاعدة المعلومات الإدارية التي يمكن أن يحتاج لها مهندس الشبكة بوصفها وسيلة معاونة في فحص عناصر قاعدة المعلومات الإدارية "ميب" MIB.

ــ مترجم ميب : يقوم بأخذ ملف على شكل الشكل ASN.1 ويحوله لاستعمالات المناسبة لنظام إدارة الشبكة.كذلك يقوم مترجم ميب بتحميل قواعد المعلومات الإدارية إلى النظام. ويساعد ذلك في الحصول على البيانات الضرورية من أجهزة مختلفة كثيرة في الشبكة.

ــ متصفح ميب : هو وسيلة الكترونية لمشاهدة وعرض عناصر MIB، بعد تحميلها من أجل إيجاد معلومات معينة. يعرض متصفح "ميب" المجموعات المختلفة في قاعدة المعلومات الإدارية MIB بطريقة رسومية.

ــ **أداة الأسماء المستعارة:** هي أداة تساعدنا في فهم أسماء عناصر "ميب" شديدة الإرباك، وذلك بتحديد صلة أسماء هذه العناصر بأسماء أكثر ألفة لنا نستطيع فهمها بسهولة.

أداة الاستفسار:تقوم هذه الأداة بتصويت poll الوكلاء في أجهزة الشبكة، كي تفحص القيم العائدة، التي يمكن أن تعاون مهندس الشبكة في تحديد ما إذا كانت عملية التصويت على العنصر ستكون مفيدة.وتمتد هذه الأداة لتسمح لنا بإنشاء استفسارات "ميب" بحسب احتياجات كل المستخدمين.

قدمت الوحدة أدوات العرض. ويعتبر عرض المعلومات على مهندس الشبكة وظيفة عصيبة وحاسمة لنظام إدارة الشبكة. وتضمنت هذه الأدوات:

ــ السجل المركزي: يوفر السجل المركزي لمهندس الشبكة وسائل لتتبع نشاط الشبكة كما يراها النظام، ويشمل رسائل النظام وأحداث الشبكة.

تعرض أداة السجل المركزي الرسائل التي يتم توليدها بواسطة تطبيقات مختلفة، وتتيح لنا مكاناً واحداً لنظام رصد الحالة.

ــ كاتب التقرير، **و**يسمح لمهندس الشبكة بإنشاء تقارير مهيأة للمستخدم.

ــ الحزم الرسومية: وتوفر الحزم الرسومية لمهندس الشبكة وسيلة لرؤية البيانات على شكل رسومات بيانية.

ناقشت الوحدة أدوات حل المشاكل:

نظام تتبع المشكلات: يقوم نظام تتبع المشكلة برصد الشبكة، وعرض المشاكل الخاصة بإدارة الأعطال وجميع المفاهيم الأخرى الخاصة بإدارة الشبكة.يشمل نظام تتبع المشكلة الخطوات التالية: إصدار بطاقة لوصف المشكلة ــ تعبئة بيانات البطاقة آليا ــ إحالة البطاقة ــ تصنيف المشكلة ــ تخزين المعلومات ــ عملية البحث ــ إنشاء تقرير.

أدوات تصميم الشبكة: تساعدنا أدوات تصميم الشبكة في إجراء بعض المهام التي تجنبنا من مشاكل مستقبلية في شبكة البيانات.

النظم الخبيرة:يمكن أن يتم إدخال الوضع الحالي للشبكة إلى نظام خبير، وتقييم البيانات، وحساب مصدر المشكلة، ويتم اقتراح العمل اللازم لإجراء حل المشكلة. يمكن أن يقوم النظام الخبير بإجراء هذه الخطوات كجزء من تحليل تصميم الشبكة، أو للمعاونة في تشخيص أعطال مشكلة.

لمحة مسبقة عن الوحدة التالية

عزيزي الدارس،

الوحدة التالية تشرح المتطلبات اللازمة لكيفية تطبيق بروتوكول SNMP لإدارة أجهزة هذه الشبكات. كما تشير الوحدة إلى بعض الاتجاهات الحديثة لإدارة بعض الشبكات الأخرى مثل شبكات ATM، وشبكات الويب .

مسرد المصطلحات

مترجم ميب MIB Compiler

يقوم هذا المترجم بأخذ ملف على شكل الشكل ASN.1 ويحوله للاستعمالات المناسبة لنظام إدارة الشبكة.

متصفح ميب MIB Browser

هو وسيلة إلكترونية لمشاهدة وعرض عناصر MIB، بعد تحميلها من أجل إيجاد معلومات معينة.

أداة الأسماء المستعارة MIB Aliases

هي أداة تساعدنا في فهم أسماء عناصر "ميب" شديدة الإرباك، وذلك بتحديد صلة أسماء هذه العناصر بأسماءٍ أكثر ألفة لنا نستطيع فهمها بسهولة.

أداة الاستفسار MIB Query

تقوم أداة استفسار ميب بتصويت poll الوكلاء في أجهزة الشبكة، كي تفحص القيم العائدة التي يمكن أن تعاون مهندس الشبكة في تحديد ما إذا كانت عملية التصويت على العنصر ستكون مفيدة.

الاستفسار المهيأ للمستخدم Custom Query

هو عبارة عن مجموعة من عناصر MIB محددة توجد في أي قاعدة معلومات إدارية، يمكن أن يفهمها النظام. إن الهدف من الاستفسار المهيأ للمستخدم هو استرجاع معلومات محددة من الجهاز، وهذه المعلومات لا يستطيع نظام إدارة الشبكة إظهارها، أو عرضها في شكلِ شكلٍ نودٌ تغييره. باستخدام الاستفسار المهيأ للمستخدم، نستطيع إنشاء رؤيتنا الخاصة لعناصر MIB.

المصطلح بالإنجليزية	معناه بالعربية
Alias	أسماء مستعارة
Blank Template	قالب فارغ
Browser	المتصفح
Centralized Log	السجل المركزي
CONFIG.SYS	ملف تهيئة النظام
Compiler	المترجم
Custom Query	الاستفسار المهيأ للمستخدم
Customized Versions	الإصدارات المهيئة للمستخدمين
Crucial	حاسمة
Default System	النظام القياسي الفرضي
Expert Systems	النظم الخبيرة
Faulty Port	المنفذ المعطل
Front-End	حاسب المقدمة والمؤخرة
File Server	خادم الملف
Graphs	رسومات بيانية
Graphic Packages	الحزم الرسومية
Heavy Load	حمل مكثف
Input Field	حقل الإدخال
Logs	سجلات دخول
Mainframe	حاسب كبير
Menus	قوائم
Multiplexer	مجمع بيانات
Octets	حروف

One-Time	مرة كل فترة
Problem Solving Tools	أدوات حل المشكلة
Pseudo Code	الشفرة الزائفة
presentation tools	أدوات عرض
Query	الاستفسار
Severely Error Seconds	ثواني الخطأ الشديد
Security Breach	خرق الأمن
Set-Request	طلب إعداد
Shut Off	إغلاق
Sophisticated	محنكة
Ticket	بطاقة
Trouble Tracking System	نظام تتبع المشكلة
Relational Database	قاعدة البيانات العلاقية
Report Writer	كاتب التقرير
Reachability	إمكانية الوصول
RMON Probes	مجسات الرصد عن بعد
Wiring Hub	المجمع السلكي

قائمة المراجع

1-SNMP MIB Tools. A MIB compiler; A MIB browser; A MIB alias tool; A MIB query tool. © Copyright 1997, The University of New Mexico. www.unm.edu/~network /presentations/course/

2- MIB Tools Overview**,** www.secure.enterasys.com/support/ manuals/ Atlas_Console_1.5-web/atlas/docs/c_mibt_overview.html

3- Network Management: Principles and Practice SNMP MIB Tools : www.bookpool.com/ sm/0201357429

4- Network Management SNMP MIB Tools:. MIB compiler, MIB browser. MIB alias tool .www.marscenter.it/tutorial/reti/appendix_h-NetMan.pdf

5- Leinwand A., and K. Conroy, K. Fang, Network Management: A Practical Perspective, 2nd ed., Addison-Wesley, 1996. ISBN 0-201-60999-1

6 www.oidview.com/mibbrowser.html

7- www.ireasoning.com/mibbrowser.shtml

8- www.manageengine.adventnet.com/products/oputils/snmp-tools.html

9- www.logisoftar.com/MibCompiler.htm

10- www.ndt-inc.com/SNMP/MIBCompiler.html

11- MPLS Network Management: MIBs, Tools and Techniques, Thomas D. Nadeau,2003. www.mpls.jp/2003/presentations/Implementation_3.pdf


الوحدة الثامنة
تطبيقات في إدارة الشبكات

محتويات الوحدة

المقدمة

تمهيد

عزيزي الدارس،

نرحب بك إلى الوحدة الثامنة والأخيرة من مقرر " استخدام وإدارة الشبكات2"، وموضوعها تطبيقات في إدارة الشبكات.

على الرغم من أن بروتوكول سنمب تم تصميمه للعمل في بيئة شبكات TCP/IP، إلا أنه يمكن توظيفه لإدارة الشبكات الأخرى مثل الشبكات التي تعمل بنظام تشغيل النوافذ، والشبكات التي تعمل بنظام تشغيل يونيكس. حيث إن هذه الشبكات قد تم تهيئتها للعمل مع بروتوكولات OSI, DECNET, IPX. نشرح في هذه الوحدة المتطلبات اللازمة لكيفية تطبيق بروتوكول SNMP لإدارة أجهزة هذه الشبكات. كما نشير إلى بعض الاتجاهات الحديثة لإدارة بعض الشبكات الأخرى مثل شبكات ATM، وشبكات الويب، حيث تشتمل هذه الوحدة على خمسة أقسام: القسم الأول يأتي متناولاً كيفية تهيئة وتنصيب الخدمات الأساسية لبروتوكول سنمب على شبكة النوافذ NT، كما يتم شرح العلاقات بين الوحدات البرمجية لأداء تطبيقات سنمب مع نظام النوافذ NT. وكذلك خدمات سنمب في نظام النوافذ، وأنواع الخدمة. كما يتناول القسم قواعد المعلومات الإدارية MIBs لنوافذ NT. أما القسم الثاني فيتناول إدارة شبكات يونيكس Unix، وأيضاً يتناول القسم الوكيل التابع بروكسي Proxy في نظم يونيكس Unix، وكذلك يتناول القسم قاعدة المعلومات الإدارية MIB لمحطة عمل يونيكس. أما القسم الثالث من الوحدة فيتناول إدارة شبكات MIB، كما يتناول هذا القسم أيضاً إدارة شبكات نمط النقل غير المتزامن Asynchronous Transfer Mode (ATM) من خلال استخدام منتجات IBM.

القسم الرابع يتناول نظام CORBA لإدارة الشبكات ، أما القسم الخامس من الوحدة فيتناول إدارة شبكات الويب Web .

أهداف الوحدة

عزيزي الدارس، بعد فراغك من دراسة هذه الوحدة ينبغي أن تكون قادراً على أن:

- **تشرح** كيفية إدارة شبكات ويندوز باستخدام بروتوكول SNMP.
- **تحدد** المتطلبات اللازمة لتشغيل بروتوكول SNMP على نظام النوافذ.
- **توضح** كيف يتم تنفيذ خدمات SNMP في نظام النوافذ.
- **تشرح** قواعد المعلومات الإدارية MIBs لنظام النوافذ.
- **تبين** كيفية إدارة شبكات يونيكس باستخدام بروتوكول SNMP.
- **تصف** بالرسم الوكيل التابع Proxy في نظم يونيكس.
- **تعدد** مكونات قاعدة المعلومات الإدارية MIB لمحطة عمل يونيكس.
- **تشرح** كيفية إدارة شبكات IBM .
- **تشرح** بالرسم كيفية إدارة شبكات ATM بواسطة استخدام بروتوكول CMIP,SNMP .
- **تذكر** مميزات وعيوب نظام COBRA لإدارة الشبكات غير المتجانسة.
- **توضح** طريقة إدارة شبكات الويب Web ، وتحدد مميزاتها.

1 . إدارة شبكات ويندوز

عزيزي الدارس،

نشرح هنا كيفية إدارة شبكات النوافذ NT باستخدام بروتوكول سنمب. وبنفس الطريقة يمكن تحميل برامج سنمب المهيأة لإدارة نظم شبكات ويندوز الأخرى، التي تعمل بنظم تشغيل مختلفة مثل ويندوز 2000، و ويندوزXP ، ويندوز Vista.

إن حاسبات النوافذ NT تدعم استخدام بروتوكول سنمب، وتحدد عناصر قاعدة المعلومات الإدارية MIB الخاصة بها. ونتناول هنا كيفية تهيئة وتنصيب الخدمات الأساسية لبروتوكول سنمب على شبكة النوافذ NT، ونشرح العلاقات بين الوحدات البرمجية لأداء تطبيقات سنمب مع نظام نوافذ NT. وخدمات سنمب في نظام النوافذ، وأنواع هذه الخدمة، إضافة إلى قواعد المعلومات الإدارية MIBs لنوافذ NT.

1.1 تنصيب بروتوكول سنمب على نظام تشغيل النوافذ NT

تتم عملية تنصيب وكيل سنمب SNMP Agent على حاسبات NT ، آلياً أثناء تنصيب وتهيئة بروتوكول TCP/IP. وتتم هذه العملية عندما نستخدم خادم Server يعمل بنظام تشغيل النوافذ NT. وذلك عندما نستخدم خادم يعمل بنظام تشغيل النوافذ ويستخدم الإصدار البرمجي الخامس أو الذي يليه. أما الخادمات التي تعمل بنظام الإصدار الرابع أو الذي قبله يمكن أن تتم عملية إضافة وكيل سنمب إلى خادم النوافذ NT في خطوة منفصلة. بعد تنصيب وتهيئة وكيل سنمب، يمكن لمحطة النوافذ إدارة وإعداد المتغيرات التي تمكن الوصول إليها من خلال محطة إدارة شبكة سنمب المركزية.

2.1 خدمات سنمب في نظام النوافذ

يتم تنفيذ سنمب لخدمة نظام نوافذ Win32، وتنقسم الخدمات التي يقدمها بروتوكول سنمب إلى اثنتين هما: "خدمة الوكيل سنمب" (التي يتم تنفيذها بواسطة

برنامج SNMP.EXE)، وخدمة رسائل المصيدة SNMP Trap والتي يتم تنفيذها بواسطة البرنامج (SNMPTRAP.EXE).

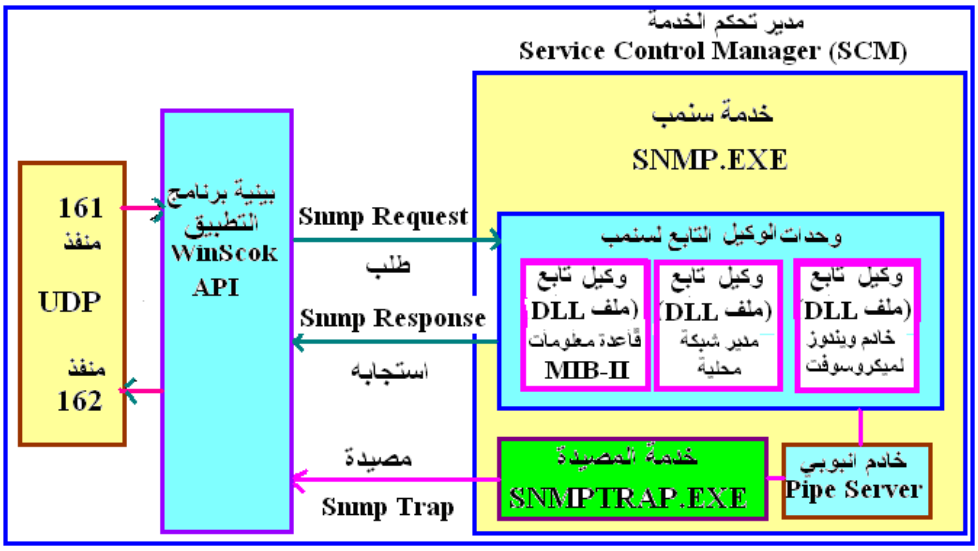
تشمل خدمة الوكيل سنمب: مسؤولية معالجة رسائل SNMP Request التي يتم استقبالها من نظم إدارة سنمب، ويرسل رسائل الاستجابة Get-Response. كما يتعامل الوكيل مع الوحدة البينية الخاصة بسوكيت النوافذ (WinSock)، والوحدة البينية لبرامج التطبيق API، ومفسر Parsing رسائل سنمب، وكذلك التعامل مع رموز القواعد المجردة Abstract Syntax Notation One (ASN.1) ،وقواعد التشفير الأساسية Basic Encoding Rules(BER). يكون الوكيل أيضاً، مسئولاً عن إرسال رسائل المصيدة Trap إلى نظام إدارة الشبكة.

يقوم برنامج "خدمة المصيدة" بالإصغاء إلى رسائل المصيدة التي ترسل إلي حاسب مضيف NT، وبعد ذلك يقوم بتمرير البيانات إلى وحدة API الخاصة بإدارة سنمب لميكروسوفت. تستقبل "خدمة المصيدة" رسائل المصيدة من وحدة برنامج التطبيق WinSock API وتمرر البيانات مستخدمةً خادماً أنبوبياً Pipe Server.

يطلق على وكيل سنمب في نظام تشغيل النوافذ مسمى "الوكيل الممتد أو التابع Extendable SNMP Agent" ويسمح الوكيل التابع بإضافة قواعد معلومات إدارية MIB جديدة، لتدعيم قواعد المعلومات الأساسية بطريقة ديناميكية، حسب احتياج النظام. ويعني ذلك أن مبرمج النظام يستطيع إضافة عناصر MIB جديدة من خلال إضافة وكيل تابع sub-agent يتم تعديله ليستخدم بواسطة الوكيل لمعالجة جميع طلبات الإدارة التي يستقبلها، وينشئ جميع رسائل المصيدة traps التي يرسلها.

يوضح الشكل 8.1 العلاقة بين خدمات سنمب، وتشمل مدير تحكم الخدمة Service Control Manager (SCM)، والوكيل التابع، اللذين يعملان في نظام النوافذ NT. يتم التحكم في هذه الخدمات بواسطة مدير تحكم الخدمة SCM. يتم تسكين الوكيل التابع داخل خدمة سنمب. وهو يستقبل رسائل سنمب عبر الشبكة، باستخدام بينية برنامج

التطبيق WinSock API، ويمرر رسالة البيانات لواحد أو أكثر من الوكلاء التابعين ليتم تحميلهم من أجل إجراء عمليات المعالجة.



الشكل 8.1 إدارة شبكات ويندوز باستخدام بروتوكول SNMP.

إن الوكيل التابع هو عبارة عن ملف برنامج من نوع "مكتبة الربط الديناميكية" Dynamic Link Library (DLL)، يكون مسؤولاً عن تنفيذ عمليات رسائل بروتوكول سنمب: Get-Request, GetNextRequest, and Set Request باستخدام متغيرات قواعد المعلومات الإدارية MIB المحددة في الرسالة. يمكن أن يضم النظام وكيلاً تابعاً "لخادم نوافذ ميكروسوفت"، ووكيلاً تابعاً خاص "لمدير شبكة محلية"، ووكيلاً تابعاً آخراً "لقاعدة المعلومات الإدارية MIB-II".

كما يوضح الشكل8.1 تفاصيل عمليات التفاعل التي تتم بين خدمة وكيل سنمب، ومجموعة الوكلاء التابعين. يتم استقبال رسائل سنمب من "بيئية برنامج التطبيق" WinSock API عن طريق خدمات بروتوكول UDP/IP. يقوم وكيل سنمب بتشفير وتوثيق الرسائل التي يستقبلها، ويمرر البيانات إلى الوكلاء التابعين المسؤولين عن معالجة عناصر MIB المحددة في الرسالة. يتم ترجيع البيانات الناتجة بعد ذلك إلى الوكيل التابع، ويتم وضعها على شكل الفورمات الخاصة ببروتوكول سنمب لرسالة

الاستجابة GetResponse، ويتم إعادة إرسالها إلى نظام إدارة الشبكة. عندما يتم تحديد عناصر MIB غير معرفةٍ في الرسالة، أو غير مدعومةٍ من الوكلاء التابعين، فإن خدمة الوكيل سنمب تقوم بإعادة إرسال رسالة تبين وجود خطأ (NoSuchName).

تقوم "خدمة المصيدة" ؛ كما هو موضح بالشكل 8.1؛ بالإصغاء إلى رسائل المصيدة المرسلة بواسطة وكلاء سنمب الآخرين، ثم توجه البيانات إلى وحدة "إدارة بينية برنامج التطبيق" API لإدارة ميكروسوفت سنمب، عن طريق الخادم الأنبوبي Pipe Server. بعد ذلك، ترسل بيانات رسالة المصيدة إلى التطبيقات التي تستخدم" تطبيق إدارة سنمب"، لتصغي إلى رسائل المصيدة. تقوم وحدة "تطبيق إدارة سنمب" بإرسال واستقبال رسائل سنمب، مستخدمة " إدارة بينية برنامج التطبيق"، التي تقوم بمخاطبة calls "بينية برنامج تطبيق سنمب" لتخصيص ذاكرة و أداء المهام الخاصة بتحويل البيانات" Data Conversion Functions".

3.1 أنواع الخدمة

يقوم مدير تحكم خدمة سنمب لنوافذ NT، بإدارة مجموعة من الخدمات. تعرف الخدمة بأنها نوع محدد من تطبيق Win32 له وحدة بينية مع "مدير تحكم الخدمة SCM". تستخدم الخدمة بينية برنامج التطبيق Win32 API. تكون مهام هذه الخدمات: رصد و مراقبة أجهزة العتاد، وعمليات المعالجات الأخرى للنظام. ومن الضروري أن يتم معالجة هذه الخدمات في خلفية النظام System Background.

يوجد نوعان من الخدمات: هما خدمات الأجهزة Device Services، وخدمات النظام System Services. تكون مهام خدمات النظام بمراقبة وصيانة عمليات محددة مثل: أحداث سجل الدخول Even Log، متصفح الحاسوب Computer Browser، والمراسل Messenger، وهكذا.

أما خدمات الأجهزة (تسمى المشغلات Drivers)، تستخدم للتحكم في عتاد الطرفيات المتصلة بمحطة العمل Workstation، مثل (مشغلات الأقراص، أو بطاقات الشبكة)،

وتعمل كوحدة بينية للتطبيقات البرمجية لعتاد الأجهزة. يتم تشغيل أو إيقاف الخدمة بواسطة مدير تحكم الخدمة SCM، عندما يقوم المستخدم بالدخول أو الخروج، أو طلب استمرار تشغيل الخدمة في حالة عدم وجود مستخدم.

يتم تنصيب خدمة بروتوكول سنمب في نظام النوافذ NT، مثل خدمات الشبكة الأخرى. المطلب الوحيد هو أن يتم تنصيب المركم البروتوكولي TCP/IP أولاً قبل تنصيب خدمة سنمب. إن المركم البروتوكولي TCP/IP-32 يوجد ضمن برنامج النوافذ NT .

4.1 قواعد المعلومات الإدارية MIBs لنوافذ NT

يوجد منتجات شبكية عديدة لميكروسوفت يوجد بها وكلاء تابعون لتدعيم الوحدة البينية لإدارة بروتوكول سنمب و قواعد المعلومات الإدارية MIBs التي توجد مع نوافذ NT.

يتم تنصيب ملفات الوكلاء التابعيين DLLs لقاعدة المعلومات MIB-II، ومدير الشبكة المحلية LAN Manager وهما LMMIB2.DLL, INETMIB1.DLL مع خدمة بروتوكول سنمب. أما الملفات الأخرى DLLs الخاصة بالوكلاء التابعيين يتم تنصيبها عندما يتم تنصيب الخدمات الخاصة بها.

أسئلة تقويم ذاتي

اذكر بعض المهام التي تقوم بها خدمة الوكيل سنمب في نظام شبكات النوافذ.

اذكر بعض الوظائف التي تقوم بها خدمة المصيدة Trap في نظام شبكات النوافذ.

ما وظيفة الوكيل التابع، الذي يستخدم في إدارة شبكات ويندوز التي تعمل ببروتوكول SNMP ؟.

اذكر أمثلة لثلاثة أنواع من الوكلاء التابعين، موضحاً وظيفة كل منهم في إدارة الشبكة.

اختر الإجابة الصحيحة:

عندما يستخدم بروتوكول سنمب لإدارة شبكات النوافذ فإن خدمة المصيدة SNMP-Trap Service تقوم بالمهام التالية:

أ) تصغي إلى رسائل المصيدة.

ب) تستخدم الخادم الأنبوبي لتوجيه البيانات إلى بينية API للتطبيق.

ج) تؤدي الوظيفتين أ، ب معاً.

د) ترسل رسائل استجابة إلى بينية برنامج التطبيق WinSock-API.

هـ) لا شيء مما سبق.

أسئلة تقويم ذاتي

اختر الإجابة الصحيحة:

يمكن إضافة وكيلٍ تابعٍ لبروتوكول سنمب لتدعيم قاعدة المعلومات الإدارية MIB. عندما يتم تحديد عناصر MIB غير معرفة في الرسالة أو غير مدعومة، فإن خدمة الوكيل سنمب تقوم بعمل الآتي:

أ) ترسل رسالة مصيدة جديدة.

ب) ترسل طلب Request جديد.

ج) ترسل طلب إعداد .

د) تعيد إرسال رسالة تبين وجود خطأ (No Such Name) .

هـ) كل ما سبق.

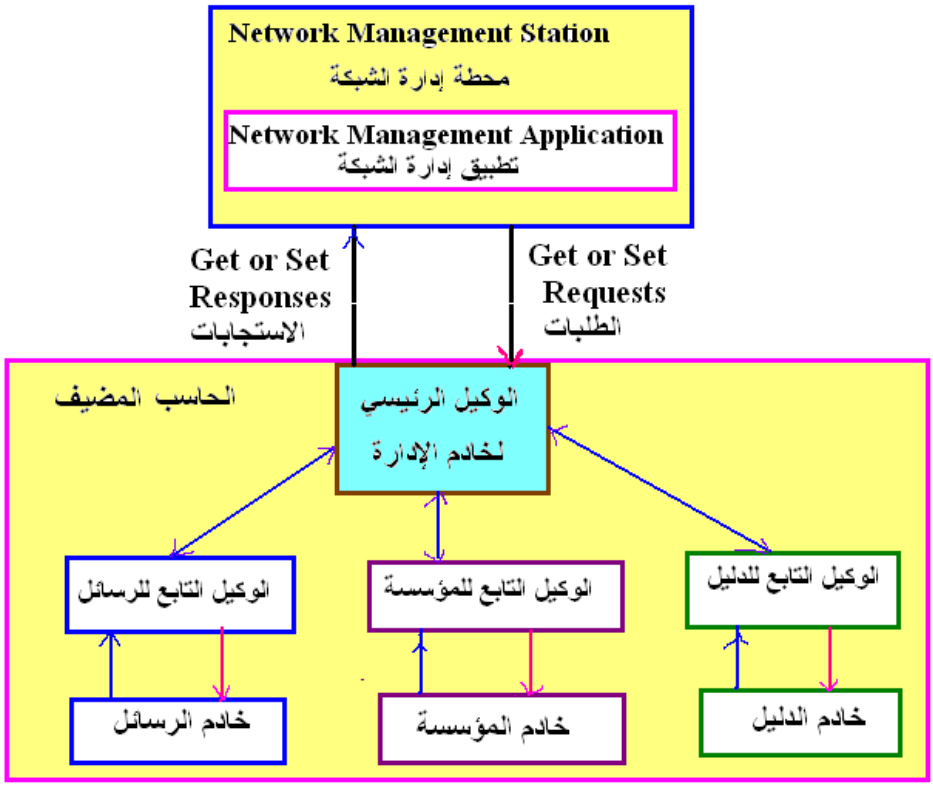
2. إدارة شبكات يونيكس Unix

عزيزي الدارس،

لاستخدام بروتوكول سنمب على نظم يونيكس، ينبغي أن يوجد وكيل رئيسي Master agent، وعلى الأقل وكيل تابع Sub-agent يتم تنصيبه وتشغيله على النظام. يوجد بعض نظم يونيكس بها وكيل رئيسي لبروتوكول سنمب، يسمي "الوكيل القومي Native Agent" . عندما يوجد هذا الوكيل في النظام ينبغي عدم تشغيله Disable أو تغيير رقم المنفذ Port الذي يستعمله. عندما يتم إخماد الوكيل القومي نكون قادرين على استخدام الوكيل الرئيسي مع خادم المدير Administration Server . عندما يتم تغيير رقم المنفذ الذي يستخدم الوكيل القومي نستطيع أن نستخدمه بجانب خادم إدارة الوكيل الرئيسي.

يمكن أن يحتوي الحاسوب المضيف على العديد من الوكلاء التابعيين، لكنه يحتوي فقط على وكيل رئيسي واحد. يوضح الشكل 8.2 – على سبيل المثال– حاسب مضيف

يحتوي على خادم للمؤسسة، وخادم الدليل، وخادم الرسائل. كل منها يوجد له وكيل تابع خاص، بينما يوجد وكيل رئيسي واحد يقوم بخدمتهم. كما يوضح الشكل العمليات التفاعلية التي تتم بين محطة إدارة الشبكة والحاسوب المضيف. نلاحظ أنه في نظام تشغيل النوافذ NT يوجد وكيل رئيسي لبروتوكول سنمب، بينما في نظام يونيكس فإن الوكيل الرئيسي يتم تنصيبه مع خادم الإدارة Administration Server.

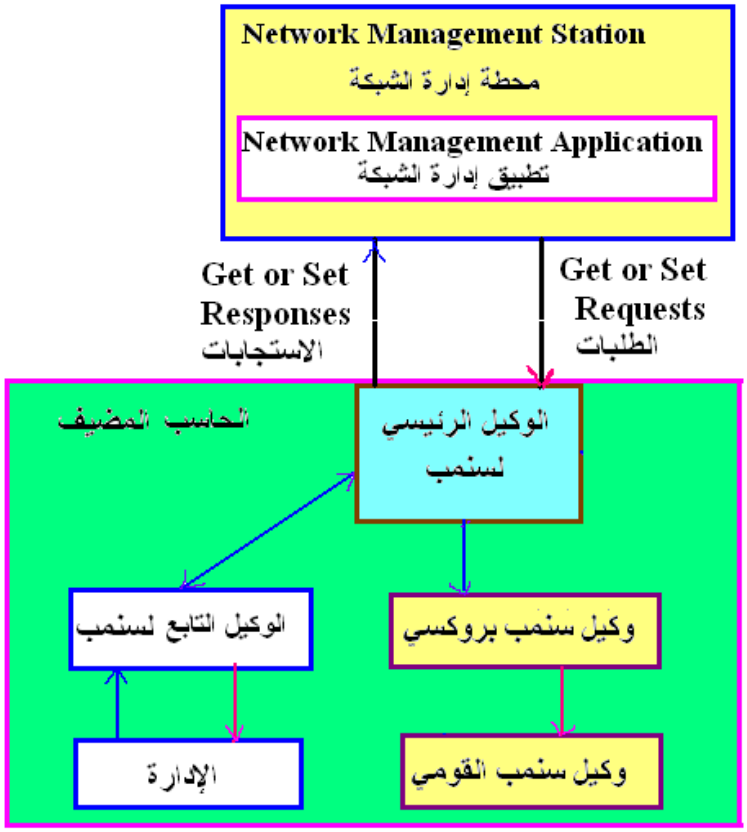


الشكل 8.2 إدارة شبكات يونيكس باستخدام بروتوكول SNMP.

يوجد بعض نظم تشغيل يونيكس تدعم إصدار سنمب، وتستخدم بروتوكول مجمع سنمب SNMP Multiplexer Protocol الذي يعرف باسم SMUX. وتسمح هذه النظم بالعمل دون الاحتياج لوجود وكيل رئيسي. ولكن ينبغي عموماً وجود وكيل رئيسي لبروتوكول سنمب في نظام يونيكس، وكذلك وكيل تابع.

1.2 استخدام الوكيل التابع بروكسي Proxy في نظم يونيكس

عندما نرغب في استخدام الوكيل القومي والوكيل الرئيسي في نفس الوقت concurrently، سوف نحتاج تنصيب set up، الوكيل بروكسي. يقوم الوكيل بروكسي بإصدار الطلبات Requests من الوكيل الرئيسي، وبعد ذلك يمررها إلى الوكيل القومي. يوضح الشكل 8.3 العمليات التفاعلية بين الوكيل بروكسي والوكيل القومي لبروتوكول سنمب.



الشكل 8.3 استخدام الوكيل بروكسي والوكيل القومي مع بروتوكول سنمب.

2.2 قاعدة المعلومات الإدارية MIB لمحطة عمل يونيكس

يمكن تحديث قاعدة المعلومات الإدارية MIB لمحطة عمل يونيكس لتنفيذ وكيل إدارة النظم كي تعمل على نظم برمجية مختلفة مثل (HP-UX, IBM AIX, Sun Solaris, SunOS) . وقد تشمل المكونات التالية:

الذاكرة: الذاكرة الرئيسية، وذاكرة التبديل swap.

الأجهزة: المعالج، الطابعات، أقراص التخزين، نظم الملفات، وهكذا.

العمليات Processes: وتشمل عمليات المستخدم، وعمليات النواة processes Kernel.

المستخدمين Users: وتشمل كلمات السر Passwords، والمجموعات Groups، والحصص Quota.

في كل مرة يتم فيها الوصول إلى متغيرات MIB يتم تمثيلها بواسطة دوال مختلفة. ويعني ذلك أنه يتم تنفيذ دالة أجزاء منفصلة Separate Module لكل متغير. يتم قراءة أو كتابة القيم من خلال الوصول إليها بواسطة الدوال get, set.

أسئلة تقويم ذاتي

اذكر وظيفة كل مما يلي:

أ) الوكيل بروكسي في إدارة شبكات يونيكس.

ب) قاعدة المعلومات الإدارية MIB لمحطة عمل يونيكس.

اختر الإجابة الصحيحة:

1- عند إدارة شبكات يونيكس باستخدام بروتوكول SNMP، ينبغي وجود:

أ) وكيلين تابعين على الأقل.

ب) وكيلين رئيسيين على الأقل.

ج) وكيلاً قومياً Native Agent فقط.

د) وكيل رئيسي واحد، وعلى الأقل وكيلاً تابعاً يتم تنصيبهما على النظام.

هـ) كل ما سبق.

2- يسمح استخدام الوكيل التابع بروكسي Proxy في نظم إدارة شبكات يونيكس:

أ) بالاستغناء عن استخدام الوكيل القومي في النظام.

ب) بتشغيل الوكيل القومي والوكيل الرئيسي في نفس الوقت Concurrently.

ج) بالاستغناء عن الوكيل الرئيسي في النظام.

د) كل ما سبق.

هـ) لاشيء مما سبق.

3. إدارة شبكات IBM

عزيزي الدارس،

إن شركة أي–بي–إم من الشركات الرائدة في تدعيم نظم إدارة الشبكات. وهي المقترحة لنظام عمارة الشبكة المفتوح Open Network Architecture (ONA) الذي هو عبارة عن إطار عام لوصف عمارة إدارة الشبكة. كما أن برنامج NetView يعتبر من البرامج الرائدة في إدارة شبكات IBM للحاسبات من نوع Mainframe. وهو يستخدم في خدمات إدارة الشبكة المركزية التي تسمح بمراقبة ، والتحكم وتهيئة عمارة شبكات نظم SNA (Systems Network Architecture) . وتحقق إدارة نظم IBM إدارة الأعطال، والأداء، والحسابات، والتهيئة، وإدارة الأمن.

يمكن تحقيق إدارة شبكات IBM باستخدام نظم متعددة منها:

أ– استخدام بروتوكول SNMP الذي تم شرحه سابقا.

ب– استخدام برنامج مدير الشبكة المحلية LAN Manager (LMN)، وهو يتحكم في الشبكات المحلية من نوع Token Ring من موقع مركزي. وهو منتج لتطوير نظام التشغيل OS/2، ويعمل مع نظام NetView لإجراء عمليات الإنذارات Alarms.

ج– استخدام برنامج NetView يقوم بتوفير خدمات الإدارة المركزية لشبكات SNA. ويستخدم على الحاسوب الرئيسي IBM وهو جزء من نظام ONA. ويتكون من أوامر للتحكم، ومراقبة العتاد، ومراقبة الجلسات، ومهام المساعدة، ورصد حالة أجهزة الشبكة، ورصد الأداء ومراقبة التوزيعات الإدارية الخاصة بالبرامج وتتبع المهام. نتناول في الفقرات التالية، كيفية تهيئة نظم شبكات IBM لإدارة شبكات ATM.

1.3 إدارة شبكات ATM

نستطيع إدارة شبكات نمط النقل غير المتزامن Asynchronous Transfer Mode (ATM) من خلال استخدام منتجات IBM. يوضح الشكل8.4 كيفية استخدام منتجات

IBM لتلائم الشبكة المرجعية ATM. وتتم عمليات إدارة الشبكة بواسطة استخدام برنامج NetView الخاص بشركة AIX وهو عبارة عن مدير شبكة خاص. ويوضح الشكل8.4 نموذجاً هيكلياً لإدارة شبكة ATM بواسطة بروتوكول سنمب، يتم فيه استخدام ما يلي:

M(1): وحدة بينية للشبكة الحلقية Token Ring.

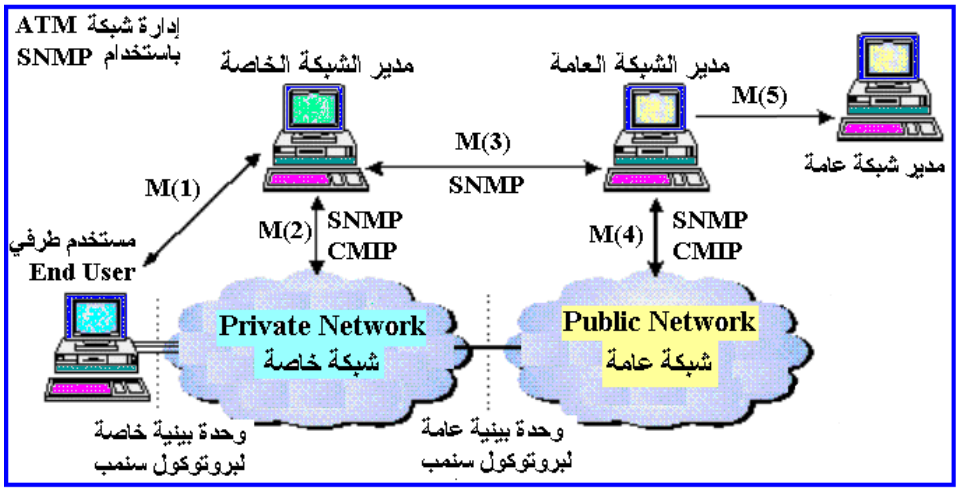
M(2): هو عبارة عن بروتوكول سنمب محمل فوق IP.

M(3): هو عبارة عن بروتوكول سنمب أو CMIP محمل فوق IP.

M(4): هو عبارة عن بروتوكول سنمب أو CMIP محمل فوق IP، أو فوق بروتوكول X.25.

M(5) : عبارة عن وحدة بينية بين الشبكات العامة وبروتوكول النقل.

كما تستخدم وحدة بينية خاصة تربط المستخدم الطرفي مع الشبكة الخاصة. وتستخدم وحدة بينية عامة، تربط الشبكة الخاصة بالشبكة العامة مستخدمة بروتوكول SNMP. ويستخدم كلا الوحدتين نفس قواعد المعلومات الإدارية MIBs على كلا الجانبين، لتحقيق العمليات الإدارية.



الشكل 8.4 إدارة شبكة ATM باستخدام بروتوكول SNMP.

أسئلة تقويم ذاتي

اذكر وظيفة نظام ONA في إدارة شبكات IBM .

4. نظام COBRA لإدارة الشبكات

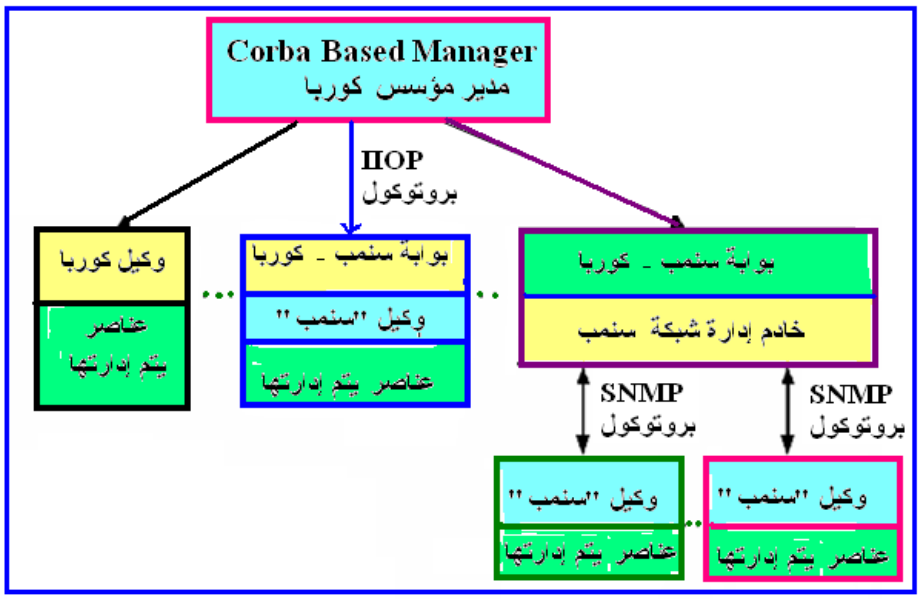
عزيزي الدارس،

يوجد احتياج إلى نظام يمكن توظيفه لتكامل النظم التي تعمل في وسط موزع غير متجانس. قد يشمل هذا الوسط نظم تشغيل مختلفة مثل (OS, Unix, Windows, MacOS, etc). وكذلك وجود نظم لشبكات متنوعة مثل:(TCP/IP, Ethernet, ATM, etc). وكذلك لغات برمجة وتطبيقات مختلفة مثل: C++, Java, Cobol, etc) وكذلك الاحتياج لوجود عتاد مختلف لتشغيل هذه التطبيقات.

إن الهدف من نظام كوربا CORBA، هو تطوير وتوظيف معايير قياسية لتطبيقات الوسط غير المتجانس الموزع، لحل جميع المشاكل المذكورة السابقة. وتعني كلمة CORBA "عمارة الوسيط المطلوب للعناصر الشائعة" وتعني باللغة الانجليزية " Common Object Request Broker Architecture " وهي عبارة عن طبقة وسطية Middleware توفر إطار العمل اللازم، ووحدة بينية برمجية تطبيقية API لتطوير التطبيقات الموزعة.

يوضح الشكل 8.5، على سبيل المثال، إدارة نظام شبكة موزعة باستخدام كوربا. تستخدم كوربا نموذجاً معلوماتياً مبنياً باستخدام النظم الشيئية Object Oriented . يتم تحديد بينيات Interfaces العناصر من خلال وحدة لغة تعريف البينية Interface Definition Language (IDL)، وتستخدم بروتوكول تشغيل العمليات الداخلية لانترنيت يسمى Internet Interoperability Protocol (IIOP)، الذي يتيح عمليات نقل معتمدة reliable فوق بروتوكول النقل TCP/IP. كما يوضح الشكل8.5 أن مدير كوربا، يتعامل مع عدة وكلاء لا تجانس بينهما هي: وكيل سنمب–كوربا، وكيل كوربا،

ووكيل سنمب من خلال خادم سنمب. يؤخذ على نظم كوربا أنها، تحتاج إضافات لبعض خدمات إدارة الشبكة– غير المتاحة حالياً – من أجل إدارة الشبكات غير المتجانسة بكفاءة.



الشكل 8.5 إدارة نظام شبكة موزعة غير متجانسة باستخدام كوربا.

أسئلة تقويم ذاتي

اذكر مزايا وعيوب استخدام CORBA في إدارة الشبكات الموزعة غير المتجانسة.

ارسم شكلاً مبسطاً يوضح المكونات اللازم استخدامها لإدارة نظام شبكة موزعة غير متجانسة باستخدام CORBA.

5. إدارة شبكات الويب Web

عزيزي الدارس،

تم تصميم نظام إدارة شبكات ويب لتوفير ودعم إمكانات إدارة الشبكات لتحقيق ما يلي:

أ- تدعيم إدارة بروتوكولات متعددة.

ب- توظيف اختيارات متنوعة باستخدام نفس النظام الإداري.

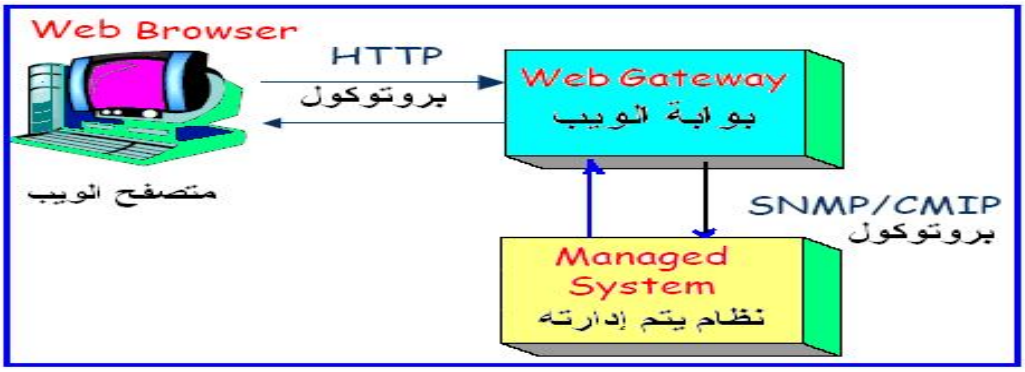
ج- تكامل التطبيقات دون الاعتماد على برنامج الإدارة.

د- الارتقاء بالنظام مع نمو الأعمال Business.

هـ- سهولة إدارة النظام من خلال توفير العديد من الأدوات الإدارية.

و- سهولة صيانة وتحديث النظام ، بسرعة وبأقل المخاطر.

يوضح الشكل 8.6، على سبيل المثال، نظاماً مبسطاً لإدارة شبكات ويب مستخدماً بوابة ويب Web Gateway. يتم الاتصال بين بوابة الويب ومتصفح الويب باستخدام البروتوكول HTTP. بعد ذلك، يتم تحويل طلبات HTTP إلى طلبات بروتوكول SNMP/CMIP. كل نظام يتم إدارته يمثل خادم ويب مصغر. يمكن الوصول إلى النظام الذي يتم إدارته من أي مكان عن طريق متصفح الويب. يؤخذ على هذه النظم أنها تستخدم بروتوكولات (HTTP / XML) التي تعبر عن البيانات بطرق كلامية "Wordy". كما أنها لا تسمح بتوزيع الإدارة الذكية.



الشكل 8.6 إدارة شبكات ويب باستخدام بوابة ويب وبروتوكول HTTP.

أسئلة تقويم ذاتي

اختر الإجابة الصحيحة

يؤخذ على نظام إدارة شبكات الويب أنها:

أ) تستعين ببروتوكول HTTP/XML الذي يتعامل بطرق كلامية Wordy.

ب) لا تسمح بتوزيع الإدارة الذكية على مكونات إدارة الشبكة.

ج) تعاني من نفس المشاكل الموجودة في بروتوكول CMIP.

د) تعاني من نفس المشاكل الموجودة في بروتوكول SNMP.

هـ) كل من أ، ب .

اذكر ثلاثة أهداف من إدارة شبكات الويب .

ارسم شكلا مبسطا يوضح مكونات إدارة شبكات الويب باستخدام بروتوكول HTTP.

اذكر اثنين من المشاكل التي تؤخذ على نظم إدارة شبكات الويب التي تستخدم بروتوكول HTTP.

الخلاصة

عزيزي الدارس،

ذكرت الوحدة في قسمها الأول أن عملية تنصيب وكيل سنمب SNMP Agent على حاسبات NT تتم آلياً أثناء تنصيب وتهيئة بروتوكول TCP/IP. وذلك عندما نستخدم خادم Server يعمل بنظام تشغيل النوافذ ويستخدم الإصدار البرمجي الخامس أو الذي يليه. أما الخادمات التي تعمل بنظام الإصدار الرابع أو الذي قبله يمكن أن تتم عملية إضافة وكيل سنمب إلى خادم النوافذ NT في خطوة منفصلة.

كما بينت الوحدة في هذا القسم أن الخدمات التي يقدمها بروتوكول سنمب لنظام نوافذ Win32تنقسم إلى اثنتين هما: "خدمة الوكيل سنمب" (التي يتم تنفيذها بواسطة برنامج SNMP.EXE)، وخدمة رسائل المصيدة SNMP Trap والتي يتم تنفيذها بواسطة البرنامج (SNMPTRAP.EXE).

وأوضحت الوحدة أنه يطلق على وكيل سنمب في نظام تشغيل النوافذ مُسَمَّى "الوكيل الممتد أو التابع Extendable SNMP Agent " إذ أن مبرمج النظام يستطيع إضافة عناصر MIB جديدة من خلال إضافة وكيل تابع sub-agent يتم تعديله ليستخدم بواسطة الوكيل لمعالجة جميع طلبات الإدارة التي يستقبلها، وينشئ جميع رسائل المصيدة traps التي يرسلها. كما بينت الوحدة أن الوكيل التابع هو عبارة عن ملف برنامج من نوع "مكتبة الربط الديناميكية" Dynamic Link Library (DLL) ، يكون مسؤولا عن تنفيذ عمليات رسائل بروتوكول سنمب: Get-Request, GetNextRequest, and Set Request باستخدام متغيرات قواعد المعلومات الإدارية MIB المحددة في الرسالة.وذكرت الوحدة أنه يمكن أن يضم النظام وكيلاً تابعاً "لخادم نوافذ ميكروسوفت"، ووكيلا تابعا خاص "لمدير شبكة محلية" ، ووكيلاً تابعاً آخراً "لقاعدة المعلومات الإدارية MIB-II" .

كما بينت الوحدة أن مدير تحكم خدمة سنمب لنوافذ NT، يقوم بإدارة مجموعة من الخدمات.كما عرَّفت الوحدة الخدمة بأنها نوع محدد من تطبيق Win32 له وحدة بينية مع "مدير تحكم الخدمة SCM". تستخدم الخدمة بينية برنامج التطبيق Win32 API. تكون مهام هذه الخدمات: رصد و مراقبة أجهزة العتاد، وعمليات المعالجات الأخرى للنظام.

ويوجد نوعان من الخدمات: هما خدمات الأجهزة Device Services، وخدمات النظام System Services

القسم الثاني بينت فيه الوحدة أنه لاستخدام بروتوكول سنمب على نظم يونيكس؛ ينبغي أن يوجد وكيل رئيسي Master agent ، وعلى الأقل وكيل تابع Sub-agent يتم تنصيبهما وتشغيلهما على النظام. كما يوجد بعض نظم يونيكس بها وكيل رئيسي لبروتوكول سنمب، يسمى "الوكيل القومي Native Agent" .

وفي نظام يونيكس يتم تنصيب الوكيل الرئيسي مع خادم الإدارة Administration Server.

كما توجد بعض نظم تشغيل يونيكس تدعم إصدار سنمب، وتستخدم بروتوكول مجمع سنمب SNMP Multiplexer Protocol الذي يعرف باسم SMUX . وتسمح هذه النظم بالعمل دون الاحتياج لوجود وكيل رئيسي. ولكن ينبغي عموماً وجود وكيلٍ رئيسي لبروتوكول سنمب في نظام يونيكس، وكذلك وكيل تابع.

كما أوضحت الوحدة أنه يمكن تحديث قاعدة المعلومات الإدارية MIB لمحطة عمل يونيكس لتنفيذ وكيل إدارة النظم كي تعمل على نظم برمجية مختلفة مثل (HP-UX, IBM AIX, Sun Solaris, SunOS) .

ذكرت الوحدة في القسم الثالث أنه يمكن تحقيق إدارة شبكات IBM باستخدام نظم متعددة منها:

أ – استخدام بروتوكول SNMP .

ب- استخدام برنامج مدير الشبكة المحلية LAN Manager (LMN)، وهو يتحكم في الشبكات المحلية من نوع Token Ring من موقع مركزي. وهو منتج لتطوير نظام التشغيل OS/2، ويعمل مع نظام NetView لإجراء عمليات الإنذارات Alarms.

ج - استخدام برنامج NetView يقوم بتوفير خدمات الإدارة المركزية لشبكات SNA. ويستخدم على الحاسوب الرئيسي IBM وهو جزء من نظام ONA.

كما تناول القسم أيضاً إدرة شبكات ATM حيث يمكن إدارة شبكات نمط النقل غير المتزامن Asynchronous Transfer Mode (ATM) من خلال استخدام منتجات IBM.

أوضحت الوحدة في القسم الرابع أن الهدف من نظام كوربا CORBA، هو تطوير وتوظيف معايير قياسية لتطبيقات الوسط غير المتجانس الموزع، وهي عبارة عن طبقةٍ وسطية Middleware توفر إطار العمل اللازم، ووحدةٍ بينية برمجية تطبيقية API لتطوير التطبيقات الموزعة.

في القسم الخامس بينت الوحدة أن نظام إدارة شبكات ويب تم تصميمه لتوفير ودعم إمكانات إدارة الشبكات لتحقيق ما يلي:

_ تدعيم إدارة بروتوكولات متعددة.

_ توظيف اختيارات متنوعة باستخدام نفس النظام الإداري.

_ تكامل التطبيقات دون الاعتماد على برنامج الإدارة.

_ الارتقاء بالنظام مع نمو الأعمال Business.

_ سهولة إدارة النظام من خلال توفير العديد من الأدوات الإدارية.

_ سهولة صيانة وتحديث النظام ، بسرعة وبأقل المخاطر.

مسرد المصطلحات

الوكيل التابع Extendable SNMP Agent

هو عبارة عن ملف برنامج من نوع "مكتبة الربط الديناميكية" Dynamic Link Library (DLL) ، يكون مسؤولا عن تنفيذ عمليات رسائل بروتوكول سنمب: Get-Request, GetNextRequest, and Set Request باستخدام متغيرات قواعد المعلومات الإدارية MIB المحددة في الرسالة.

الوكيل بروكسي Proxy في نظم يونيكس.

يقوم الوكيل بروكسي بإصدار الطلبات Requests من الوكيل الرئيسي، وبعد ذلك يمررها إلى الوكيل القومي.

نظام عمارة الشبكة المفتوح Open Network Architecture (ONA)

هو عبارة عن إطار عام لوصف عمارة إدارة الشبكة.

برنامج NetView

يعتبر من البرامج الرائدة في إدارة شبكات IBM للحاسبات من نوع Mainframe. وهو يستخدم في خدمات إدارة الشبكة المركزية التي تسمح بمراقبة ، والتحكم وتهيئة عمارة شبكات نظم SNA (Systems Network Architecture) .

نظام كوربا CORBA

تعني كلمة CORBA "عمارة الوسيط المطلوب للعناصر الشائعة" وتعني باللغة الإنجليزية " Common Object Request Broker Architecture " وهي عبارة عن طبقة وسطية Middleware توفر إطار العمل اللازم ، ووحدة بينية برمجية تطبيقية API لتطوير التطبيقات الموزعة. و الهدف من نظام كوربا CORBA، هو تطوير وتوظيف معايير قياسية لتطبيقات الوسط غير المتجانس الموزع .

المصطلح بالإنجليزية	معناه بالعربية
Abstract Syntax Notation One(ASN.1)	رموز القواعد المجردة
Applications	تطبيقات
Application Program Interface	بينية برنامج التطبيق
Administration Server	خادم المدير
Asynchronous Transfer Mode (ATM)	نمط النقل غير المتزامن
Basic Encoding Rules (BER)	قواعد التشفير الأساسية
Browser	متصفح
Common Object Request Broker Architecture(CORBA)	عمارة الوسيط المطلوب للعناصر الشائعة
Concurrently	في نفس الوقت
Data Conversion Functions	المهام الخاصة بتحويل البيانات
Device Services	خدمات الأجهزة
Drivers	مشغلات
Dynamic Link Library (DLL)	مكتبة الربط الديناميكية
Even Log	أحداث سجل الدخول
Extendable Agent	الوكيل الممتد أو التابع
Hyper Text Transfer Protocol (HTTP)	بروتوكول نقل النصوص المختلطة
Interface Definition Language(IDL)	بينية تعريف اللغة
Internet Interoperability Protocol (IIOP)	بروتوكول العمليات داخل إنترنيت
Messenger	المراسل
Middleware	مجمع

Multiplexer	طبقة وسطية
Native Agent	الوكيل القومي
Open Network Architecture(ONA)	عمارة الشبكة المفتوحة
Passwords	كلمات السر
Pipe Server	الخادم الأنبوبي
Parsing	تفسير
Quota	الحصص
Service Control Manager (SCM)	مدير تحكم الخدمة
Sub-Agent	وكيل فرعي
Separate Module	دالة منفصلة
System Services	خدمات النظام
Systems Network Architecture (SNA)	عمارة شبكات النظم
System Background	خلفية النظام
Swap	التبديل
XML Extensible Markup Language.	لغة العلامة الممتدة
Web Gateway	بوابة ويب
Workstation	محطة العمل

قائمة المراجع

1-Telecommunications Network Management, by Haojin Wang ,Publisher: McGraw-Hill Professional, 1999, ,Updated on /2004. ISBN-13: 978-0070681705

2- Security for Telecommunications Network Management ,by Moshe Rozenblit ,Publisher: Wiley-IEEE Press; 1999,ISBN-13: 978-0780334908.

3- Network Management Systems Essentials,Publisher: McGraw-Hill, 1996. ISBN 0-07-065766-1

4- INTEGRATED MANAGEMENT OF NETWORKED SYSTEMS By Heinz-Gerd Hegering ,Sebastian Abeck ,Bernhard Neumair, 2007.

5- Web-Based Systems and Network Management, 1999, ISBN:0849395984

6- Windows NT SNMP, By James D. Murray,1st Edition January 1998, 1-56592-338-3.

7- Network Management for Microsoft Networks Using SNMP, By Karanjit S. Siyan,

8- Network Management Protocols, Article Written by Oren Chapo , August 1999.

9- Network Management Fundamentals, By Alexander Clemm ,Published, 2006 by Cisco Press.

10- The XHTML 1.0 Web Development Sourcebook:, Building Better Sites and Applications, Site URL: http://www.iangraham.org/books/xhtml2/, by Ian S. Graham.

11- Web Services for Network Management - A Universal Architecture and Its Application to MPLS Networks ,B. Thurm ,
27th Annual IEEE International Conference on Local Computer Networks (LCN'02) p. 463.

12- Web-Based Network-Management Solutions,John Edwards on December 12, 2007.

13- Multiprotocol Network Management: A Practical Guide to Netview for Aix ,by Larry Bennett ,Publisher: Mcgraw-Hill (Tx) (February 1996) ISBN-13: 978-0077091224

14- Enterprise network management: a guide to IBM's NetViewDavid M. Peterson McGraw-Hill, 1994 ISBN:0-07-049654-4

15- SNMP-Based ATM Network Management by Heng Pan Publisher: Artech House Publishers; 1st edition (September 15, 1998) ISBN-13: 978-0890069837

16- Planning and Managing ATM Networks, Daniel Minoli, Thomas W. Golway, and Norris P. Smith, 1996 , ISBN: 132621894.