جامعة دمشق

كلية الهندسة المعلوماتية

قسم النظم و الشبكات الحاسوبية

تصميم و تنفيذ نظام إدارة و مراقبة منظومة شبكية

مشروع أعد لنيل درجة الإجازة في الهندسة المعلوماتية

قسم النظم و الشبكات الحاسوبية

إشراف

د . محمد نوّار العوا م . عرفان أبو الشامات

تقديم

مصطفى محمد نجم محمد يوسف محمد

2008-2009

بسم الله الرحمن الرحيم

قالوا سبحانك لا علم لنا إلا ما علمتنا إنك

أنت العليم الحكيم

صدق الله العظيم

سورة البقرة

بسم الله الرحمن الرحيم

مهداة إلى

.....

.....

.....

.....

أجمل الأوراق ...

ورقة تكتب فيها إلى أعز الناس ...

مصطفى

الإهداء

إلى الفؤاد الطاهر الذي ضخ نور الهداية في عروق البشرية ...

إلى معلم الناس الخير .. المشكاة التي يأتم بها الهداة ...

إلى رسول الإنسانية .. من أرسل رحمة للعالمين ...

سيدنا محمد صلى الله عليه و سلم

إلى القلب الذي يفيض بالحنان و الشفاه التي لا تمل الدعاء ...

الى من حاكت سعادتي بخيوط منسوجة من قلبها ...

إلى بحر تعجز الكلمات أن ترسو في شواطئه...

إلى من كانت الجنة تحت قدميها ...

أمي

إلى المشعل الذي أنار لي الطريق و علمني الفضيلة و الأمانة ...

إلى من استعذب السهر دون الأشواك لقطف الورود ...

إلى القلب الذي ينبض بالعطاء دون انتظار الثناء ...

إلى من زرع في أعماقي الأخلاق و القيم ...

أبي

إلى الورود التي ترعرعت في ظل ذاك الحنان و هذا العطاء ...

إلى الأفئدة النضرة ، و النجوم المضيئة في سمائي ...

إلى من رضعوا معي الصدق و الوفاء ...

أخوتي

د. ماهر ، د. عبد القادر ، أحمد ، أنس ، مالك

إلى زنابق في بستان حياتي ، و رياحين في جنة فؤادي ...

إلى الأزهار اليانعة ، و الورود العطرة في دنياي ...

إلى خلجات قلبي و توائم روحي ...

أخواتي

نسرال ، م.إيمان ، د.صفاء

إلى العصافير الصغيرة ، و البراعم المتفتحة...

إلى قصائد الغزل ، و لحظات الصغار ...

إلى براءة الطفولة ، و بسمة الحياة ...

أبناء أخوتي

نيرمين ، بتول ، أحمد ، لين ، آية ، محمد

إلى أهل الوفاء ، و منبع الاخاء ، و رصيدي في الحـــياة ...

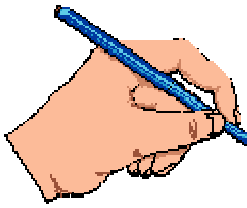
الأصدقاء

لم يخترعوا بعد لغة حروفها و مفرداتها أجزاء من القلب ...

و لو فعلوا لأهديتكم أبجديتها كاملة ...

إلى كل الأحبة ...

إلى كل قلب طاهر و ضمير حي .....



مصطفى

2009/07/13

بطاقة شكر و عرفان

لحظة حيرة نقفها في منتصف الطريق .. بين ماضٍ نحنُّ إليه بأساه و مره و حلوه ،و مستقبل غامض نتوق إليه و كلنا أمل بأن يحمل لنا في طياته السعادة و النجاح.

و لا يسعنا و نحن على عتبات منعطف جديد في حياتنا العلمية و العملية إلا أن نتوجه بالشكر الجزيل و الامتنان الوفير إلى مشاعل النور ،الذين لم يبخلوا أبدا بالعطاء و قاموا بواجبهم بكل صدق و أمانة .. أعطوا فأغدقوا و قدموا بلا مقابل .. إلى من سلحونا فأناروا طريقنا ،و جعلونا أكثر ثقة بالمستقبل، أساتذتنا الكرام – أعضاء الهيئة التدريسية في كلية الهندسة المعلوماتية بجامعة دمشق – و إن كانت تعتريني الرغبة في ذكر أسمائهم التي انطبعت في عقولنا الواحد تلو الآخر ، إلا أن خوفي من سقوط اسم زهرة من باقة الورود تلك أو خطأي في ترتيب أزهار الباقة يجعلني أكتفي بأن أنثر عبيرها على صفحتي دون ذكر أسماء الأزهار المشكلة لها.

أتمنى أن تفي كلمة شكراً بما يجول في نفسي تجاهكم ،و أقدم إليكم دعوة حب واحترام لمزيد من العطاء ،دعوة يفوح عبيرها فيغطي جميع الأرجاء.

و نخص بالشكر العميق :

الدكتور محمد نوّار العوا

الذي تفضل بالإشراف على هذا العمل و لم يبخل علينا بإرشاداته و نصائحه القيّمة.

كما نتقدم بأسمى آيات الشكر و العرفان إلى :

المهندس عرفان أبو الشامات

الذي كان الداعم الأكبر لنا في إنجاز هذا المشروع

دمشق

2009/07/13

وقفة للذكرى

انتهى المشوار و رست المراكب على الميناء ...

اجتمع الأصدقاء و ارتسمت الابتسامة و سالت الدمعة من العيون ...

حينما نادى المنادي أن قد حان الرحيل .. بدأت ألملم أشتات نفسي من كل مكان .. و رحلت و بقيت في ظلام ساعات الفراق و البعد ...و انطويت على ذاتي ... و انزويت مع ذكرياتي ...

لملمت السنوات الخمسة أمتعتها ،و أطلقت حمائم النورس تغاريد الوداع ،و أنشدت العنادل لحن الفراق ،و بات البين صاحب الموقف ... ليت الفرح لم يكن ناعما ،و ليت أشواك الزهور في أريجها ... العيون حائرة ... الدموع تنهمر ... حزنا على أيام خلت سنعيش ذكراها لواعج و تفاؤلا و أملاً بمستقبل غامض نتوق إليه بعد مشقة المشوار ...

و هذا شراع الوداع ينشر ذراعيه ليذكرنا بأيامٍ جميلة و لحظاتٍ خالدة في الذكرى كنّا خلالها نركض للهدف .. ننتظر النهاية .. نُعدّ لها و نتمناها منى الموعود ...

فهل ستتحول الأحلام التي رسمناها إلى حقيقة نعيش معها ... أم هل سنتذوق ثمار ما عملنا و ننعم بها ... أم هل ستلد أحلامنا مولدها بسلام بعد مخاض شاقٍ و طويل...؟!

لسنا ندري ،لكن ثقتنا بالله عز و جل أكبر من أن يطالنا اليأس و القنوط و باسمه الكريم أولا و بالهمة العالية و الإرادة ثانيا سوف نسير في خضم الحياة الزاخرة بالمصاعب دون خوف و لا وجل .

تعجز الكلمات في وداعكم .. و لا يفي إلا الدعاء من رب السماء بإطلالة جديدة مشرقة ..

مصطفى

2009/07/13

Moustafa-MN@Hotmail.com

الفهرس

الفصل الأول

توصيف المشروع

1-1 مقدمة:

لما كان انتشار الشبكات الحاسوبية و خدمات الانترنت تزداد يوما بعد يوم ،و بعد أن أضحت الشبكات الحاسوبية أمرا واقعا في معظم مواقع العمل لا سيما في قطاعات الأعمال و القطاعات الحكومية ،و انطلاقا من عبارة البروفسور Jone.M.Maklay الخبير العالمي بنظم تصميم و إدارة الشبكات :

"لا تكمن المشكلة بتصميم و تحقيق الشبكة و إنما المشكلة الحقيقية هي في الحفاظ عليها تعمل بشكل مناسب و توفير أكبر قدر من التحكم بها".

تبرز الحاجة إلى نظام يؤمن عملية إدارة و مراقبة الشبكة إما لتحقيق سياسات معينة ضمن المؤسسة ،أو للحفاظ على جاهزية الشبكة و عدم تعرضها للعبث من قبل العاملين في المؤسسات.

إن نظام إدارة الشبكات هو مجموعة من الأدوات تهدف إلى تأمين المراقبة و التحكم لوظائف الشبكة بحيث تكون متكاملة من حيث تأمين واجهة عمل مشتركة قوية،سهلة الاستخدام توفر جميع أوامر التحكم و المراقبة بأقل تجهيزات إضافية ممكنة.

ينبغي أن يكون نظام مراقبة (إدارة) الشبكة قادراً على:

- استحصال / تجميع البيانات الضروريّة من النظام.
- معالجة و عرض البيانات.
- عرض البيانات المجمّعة بمستوياتٍ مختلفةٍ من التفصيل.
- إتخاذ القرارات تلقائيّاً عند الحاجة.

إن بناء شبكة يمكن أن يتم بسهولة، أما بناء شبكةٍ ذات أداءٍ جيّدٍ فيتطلّب الكثير من الوقت والخبرة. هذا هو المبدأ الذي بني عليه نجاح الإنترنت بأكملها!

2-1 توصيف المشروع:

1-2-1 تعريف المشروع:

المشروع هو عبارة عن تصميم و تنفيذ نظام لإدارة و مراقبة شبكة تابعة لمزود خدمة انترنت (Neotech)،حيث يقوم بمراقبة خدمات مختلفة ضمن مكونات الشبكة (مثل عدد المستخدمين ،نسبة انشغالية المعالج ،نسبة استخدام القرص الصلب ...)،و يمكنه إرسال تحذير عند وجود مشكلة ما (مثلا : استخدام القرص الصلب تجاوز 80٪) ،بالإضافة إلى إظهار نتائج المراقبة على شكل مخططات بيانية.

2-2-1 الهدف من المشروع :

تصميم وتنفيذ نظام مراقبة و إدارة للشبكة يضمن ما يلي :

- الحفاظ على جاهزية الشبكة.
- تأمين جودة الخدمة ،و استمرارية العمل: من خلال جمع معلومات حول استخدام الشبكة و عرضها بشكل رسوم بيانية (يمكن معرفة أوقات الذروة) .
- تسهيل صيانة الشبكة : من خلال المراقبة المستمرة ،و تنبيه مدير الشبكة فور حدوث عطل و تحديد مكان العطل .
- الصيانة الوقائية: أي إجراء صيانة للشبكة قبيل حدوث أعطال ،و بالتالي يمكن تفادي الخطأ قبل حدوثه ،و ذلك من خلال معالجة المعلومات الاحصائية المخزنة نتيجة مراقبة عمل مكونات الشبكة و حساب مؤشرات مثل: عدد ساعات العمل، معدل الأخطاء Error Rate، و الزمن الوسطي بين عطلين MTBF .
- **التحكم في التكلفة : مراقبة استخدام الموارد والتحكم فيها بحيث تتم تلبية احتياجات المستخدم بتكلفة مناسبة.**

من خلال هذه المتطلبات يتبين أهمية منظومة المراقبة بالنسبة لمزود خدمة الانترنت ،و اعتبارها ركن أساسي.

بناء على تعريف المشروع و دراسة متطلبات الشركة نستنتج أن النظام المطلوب تصميمه يجب أن يحقق الخدمات التالية:

1- يعطي واجهة تحوي جميع مكونات الشبكة و الخدمات ضمن كل مكون التي يمكن مراقبتها و حالة الخدمة.
2- إرسال تنبيهات و تحذيرات عند وجود مشكلة ،عن طريق البريد الالكتروني أو على شكل SMS .
3- إجراءات Scripts لفحص حالة الخدمة.
4- تسهيل عملية الإدارة و المراقبة من خلال رسم مخططات بيانية.
5- رسم مخطط الشبكة و إظهار حالة الشبكة في لحظة ما.
6- مراقبة تجهيزات تعمل معا وفق أنظمة تشغيل مختلفة (Windows , Linux).
7- نظام سهل الاستخدام.

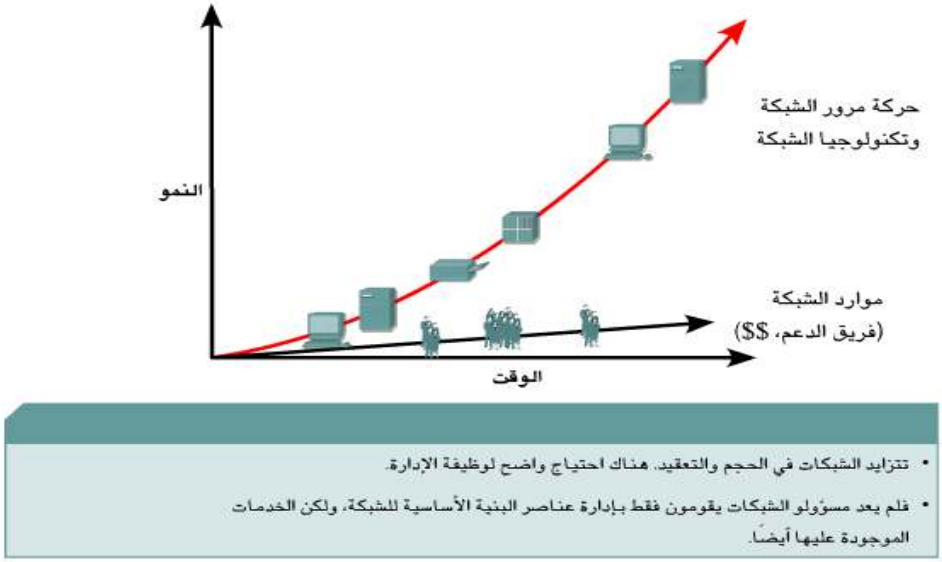
الفصل الثاني

أساسيات إدارة الشبكات

2-1 مقدمة حول إدارة الشبكة :

مع تطور الشبكة و زيادة حجمها، تزداد أهميتها كمورد خطير لا يمكن الاستغناء عنه في المؤسسة. و مع إتاحة المزيد من موارد الشبكة للمستخدمين، تصبح الشبكة أكثر تعقيدًا و تصبح صيانتها أيضًا أكثر تعقيدًا.

إن خسارة موارد الشبكة و الأداء السيئ هي نتائج لزيادة التعقيد و لن يقبلهما المستخدمون. و لذلك لابد أن يدير مسؤول الشبكة هذه الشبكة بنشاط و يشخص المشكلات و يمنع حدوثها و يوفر أفضل أداء شبكة للمستخدمين. و في وقت ما، ستصبح الشبكة كبيرة جدًا بحيث لا يمكن إدارتها دون أدوات إدارة الشبكة التلقائية .



الشكل 2-1 تطور إدارة الشبكة [1]

2-1-1 أهداف إدارة الشبكة :

هي القوى المحركة لإدارة الشبكة ،وهي موضحة فيما يلي:

- **التحكم في أصول الشركة**: إذا لم يتم التحكم في موارد الشبكة بشكل فعال، فلن توفر النتائج التي تتطلبها الإدارة.
- **التحكم في التعقيد**: مع التطور الهائل في عدد مكونات و مستخدمي و واجهات و بروتوكولات و بائعي الشبكات، أصبح فقدان التحكم في الشبكة و مواردها يمثل تهديدًا للإدارة .
- **تحسين الخدمة**: يتوقع المستخدمون نفس الخدمة أو خدمة محسنة مع نمو الشبكة و توزيع الموارد بشكل متزايد .
- **موازنة الاحتياجات المتنوعة**: يجب أن يتوفر للمستخدمين تطبيقات متنوعة على مستوى محدد من الدعم، مع متطلبات محددة في الأداء و الإتاحة و الأمان .
- **تقليل زمن التعطل**: ضمان الإتاحية العالية للموارد عن طريق التصميم المتكرر الصحيح .
- **التحكم في التكلفة**: مراقبة استخدام الموارد و التحكم فيها بحيث تتم تلبية احتياجات المستخدم بتكلفة مناسبة

2-1-2 مهام إدارة الشبكة :

تتضمن إدارة الشبكة الواجبات التالية:

- مراقبة توفر الشبكة .
- تحسين التشغيل التلقائي.
- مراقبة وقت الاستجابة.
- ميزات الأمان .
- إعادة توجيه حركة المرور .
- قدرة الاستعادة.
- سهولة الاستخدام .
- القدرة على إضافة و حذف المستخدمين.
- تسجيل المستخدمين

2-1-3 المصطلحات الأساسية في إدارة الشبكة :

المصطلح	التعريف
SNMP	بروتوكول إدارة الشبكات البسيط هو المعيار لإدارة موارد الشبكات، وهو معرّف بواسطة IETF.
MIB	قاعدة معلومات الإدارة هي تعريفات/بناء البيانات للكائن المدار.
RMON	المراقبة عن بعد هي مواصفات MIB/العميل (agent) التي تعرّف وظائف مراقبة الأجهزة البعيدة.
RFC	طلب التعليق هي مستندات يتم نشرها بواسطة IETF. وقد تم إقرار بعضها كمعايير إنترنت.
NMS	تعد محطة إدارة الشبكة محطة إدارة مستندة إلى SNMP لإدارة أجهزة الشبكات. ويعد ذلك مربع UNIX أوNT قيد التشغيل، أو HP Openview ، أو SunNET Mgr أو NetView لـ AIX.

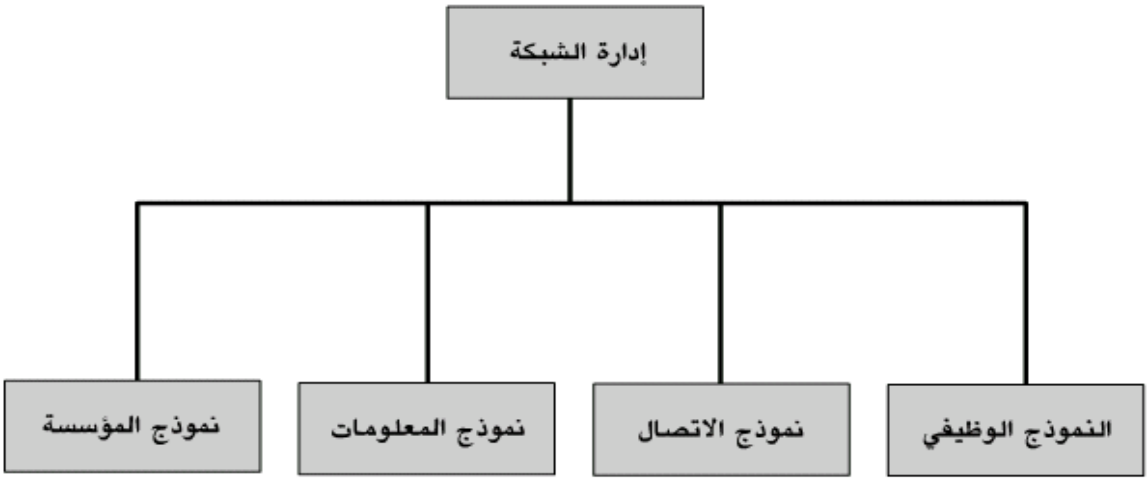
2-2 نموذج إدارة الشبكة وOSI :

قامت المنظمة الدولية للمعايير (ISO) بإنشاء لجنة لإنتاج نموذج لإدارة الشبكة، في ظل توجيه مجموعة OSI .

ويحتوي هذا النموذج على أربعة أجزاء:

- التنظيم
- المعلومات
- الاتصالات
- الوظائف

فيما يلي عرض لإدارة الشبكة من أعلى لأسفل، و قد تم تقسيمها إلى أربعة نماذج فرعية يتم التعرف عليها من خلال معيار OSI .



الشكل 2-2 نموذج إدارة الشبكة [1]

نموذج المؤسسة (التنظيم):

يصف نموذج التنظيم مكونات إدارة الشبكة مثل المدير و الوكيل (agent)، وغيرهم، بالإضافة إلى علاقاتهم . يؤدي تنظيم هذه المكونات إلى إنتاج أنواع مختلفة من البنيات، وهو ما سنناقشه في وقت لاحق.

نموذج المعلومات :

يختص نموذج المعلومات ببنية معلومات إدارة الشبكة و تخزينها .يتم تخزين هذه المعلومات في قاعدة بيانات، تسمى قاعدة معلومات الإدارة (MIB) حددت (ISO المنظمة الدولية لوضع المعايير) بنية معلومات الإدارة (SMI) لتحديد بناء جملة معلومات الإدارة المخزنة في MIB و دلالتها.

- يهتم ببنية وتخزين المعلومات
- تمثيل الكائنات والمعلومات المتعلقة بإدارتها
- قامت ISO بتعريف بنية معلومات الإدارة (SMI) لتعريف بناء الجمل ودلالات معلومات الإدارة المخزنة في MIB

نموذج الاتصال :

يتعامل نموذج الاتصالات مع كيفية توصيل بيانات الإدارة بين عملية المدير و الوكيل . و يختص هذا النموذج ببروتوكول النقل و بروتوكول التطبيق و الأوامر و الاستجابات بين النظائر.

- كيف يتم توصيل بيانات الإدارة بين العميل والمدير.
- ثلاثة مفاهيم
  - وسيطة النقل لتبادل الرسائل (بروتوكول النقل)
  - تنسيق الرسائل الخاص بالاتصال (بروتوكول التطبيق)
  - الرسالة الفعلية (الأوامر والاستجابات)

النموذج الوظيفي :

يتعامل النموذج الوظيفي مع تطبيقات إدارة الشبكة التي توجد في محطة إدارة الشبكة(NMS) . يوضح نموذج إدارة شبكة OSI خمسة مناطق للوظائف، ويطلق عليها أحيانًا نموذج FCAPS :

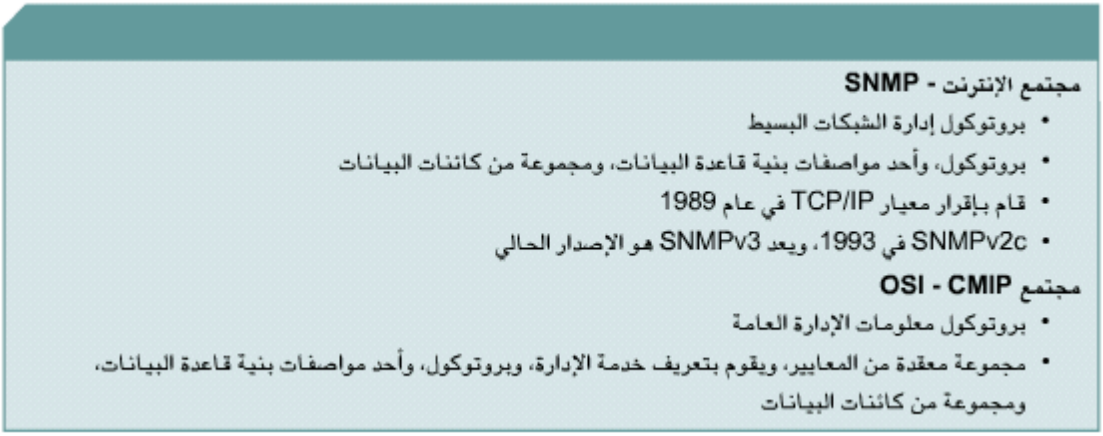
- يعالج تطبيقات إدارة الشبكة الموجودة على NMS
- يقوم نموذج IOS بتصنيف خمسة مناطق للتشغيل، وتتم الإشارة إليه أحيانًا بنموذج FCAPS:
  - خطأ
  - التكوين
  - المحاسبة
  - الأداء
  - الأمان

لقد اكتسب نموذج إدارة الشبكة هذا قبولاً واسعًا من البائعين لكونه طريقة مفيدة لوصف متطلبات أي نظام إدارة شبكة.

2-3 معايير SNMP وCMIP:

يلزم استخدام معايير إدارة الشبكة للسماح بالتشغيل المتداخل للإدارة عبر العديد من الأنظمة الأساسية المختلفة للشبكة و ذلك حتى يتمكن البائعون من تطبيق هذه المعايير و الالتزام بها. و قد ظهر معياران أساسيان :

- **بروتوكول إدارة الشبكات البسيط** : و ذلك في مجتمع مجموعة عمل هندسة الإنترنت (IETF)
- **بروتوكول معلومات الإدارة العامة** : و ذلك في مجتمع الاتصالات



يشير SNMP (بروتوكول إدارة الشبكات البسيط) إلى مجموعة من معايير إدارة الشبكة التي تتضمن بروتوكول و مواصفات بنية قاعدة البيانات و مجموعة من كائنات البيانات. و قد تم إقرار بروتوكول SNMP (بروتوكول إدارة الشبكات البسيط) بصفته معيار TCP/IP (بروتوكول التحكم في الإرسال/بروتوكول الإنترنت) عام 1989 و أصبح شائع الاستخدام بدرجة كبيرة .و قد تم إقرار ترقية، تعرف باسم الإصدار 2 c من SNMP أو SNMPv2c عام 1993. وقد وفرت SNMPv2c دعمًا لاستراتيجيات إدارة الشبكة الموزعة و المركزية كما تضمنت تحسينات في بنية معلومات الإدارة (SMI) و تشغيل البروتوكولات و بنية الإدارة و الأمان .و قد تم تصميم هذا الإصدار لتشغيله في شبكات تعتمد على OSI (الاتصال المتبادل بين الأنظمة المفتوحة) و الشبكات المعتمدة على TCP/IP. و بعد ذلك، تم إصدار SNMPv3 .و قد وفرت SNMPv3 وصولاً آمنًا إلى MIB (قواعد معلومات الإدارة) عن طريق مصادقة الحزم (packet) و تشفيرها عبر الشبكة، و ذلك لحل نقاط ضعف الأمان في SNMPv1 و SNMPv2c .

إن بروتوكول CMIP (بروتوكول معلومات الإدارة العامة) هو بروتوكول إدارة شبكة لـ OSI (الاتصال المتبادل بين الأنظمة المفتوحة) قامت بإنشائه و وضع المعايير الخاصة به منظمة ISO (المنظمة الدولية لوضع المعايير) بهدف مراقبة الشبكات المتباينة و التحكم فيها.

2-4 تشغيل SNMP :

إن بروتوكول SNMP (بروتوكول إدارة الشبكات البسيط) هو بروتوكول طبقة التطبيق المصمم لتسهيل تبادل معلومات الإدارة بين أجهزة الشبكة .و عن طريق استخدام SNMP للوصول إلى بيانات معلومات الإدارة، مثل عدد الحزم (packet) التي يتم إرسالها في الثانية عبر واجهة أو عدد من اتصالات TCP (بروتوكول التحكم في الإرسال) المفتوحة ،يتمكن مسؤولو الشبكة من إدارة أداء الشبكة بسهولة أكبر للعثور على مشكلات الشبكة وحلها .

لقد أصبح SNMP اليوم أشهر بروتوكولات إدارة الشبكات البينية التجارية و الجامعية و البحثية المتنوعة.

واستمر نشاط وضع المعايير حتى مع تطوير البائعين و إصدارهم لتطبيقات إدارة حديثة للغاية تعتمد على بروتوكول SNMP. إن SNMP هو بروتوكول بسيط، إلا أن مجموعة السمات الخاصة به تمتلك القوة الكافية لمعالجة المشكلات الصعبة التي تتصل بإدارة الشبكات المتباينة.

يتضمن النموذج التنظيمي لإدارة الشبكات المعتمدة على SNMP أربعة عناصر:

- محطة الإدارة
- وكيل الإدارة
- قاعدة معلومات الإدارة
- بروتوكول إدارة الشبكة

عادةً ما يكون نظام NMS (نظام إدارة الشبكة) محطة عمل قائمة بذاتها، ولكن يمكن تطبيقه عبر أنظمة متعددة. فهو يتضمن مجموعة من البرامج تسمى تطبيق إدارة الشبكة(NMA) . وتتضمن NMA واجهة مستخدم للسماح لمديري الشبكة المخولين بإدارة الشبكة. و تستجيب الواجهات لأوامر المستخدم و الأوامر التي يتم إصدارها إلى وكلاء الإدارة عبر الشبكة .وكلاء الإدارة هي أنظمة وأجهزة أساسية للشبكة مزودة ببروتوكول SNMP (بروتوكول إدارة الشبكات البسيط) بحيث يمكن إدارتها. و يستجيب الوكلاء لطلبات المعلومات و طلبات الإجراءات من NMS ، مثل رسائل الاستعلام، و قد توفر لنظام NMS معلومات مهمة و لكن غير مطلوبة، مثل رسائل التنبيه. يتم تخزين جميع معلومات الإدارة الخاصة بوكيل محدد في قاعدة معلومات الإدارة الخاصة بهذا الوكيل. بإمكان الوكيل تتبع ما يلي:

- عدد أنواع معينة من رسائل الخطأ المستقبلة .
- عدد البايتات و الحزم (packet) داخل الجهاز و خارجه .
- أقصى طول لرتل الإخراج لأجهزة التوجيه (router) و غيرها من أجهزة الشبكات البينية .
- رسائل البث المرسلة و المستقبلة .
- واجهات الشبكة المنخفضة و المرتفعة .

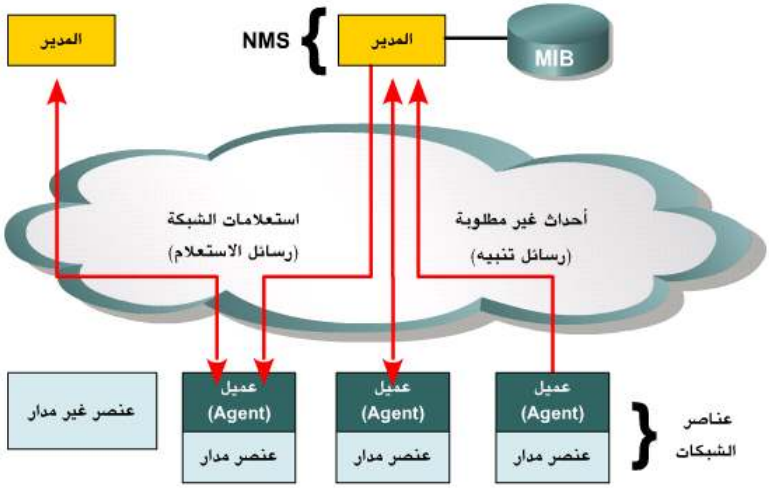
يُجري نظام NMS (نظام مراقبة الشبكة) وظيفة مراقبة باستعادة القيم من MIB (قاعدة معلومات الإدارة). و بإمكان NMS التسبب في حدوث إجراء عند الوكيل. يتم تنفيذ الاتصال بين المدير و الوكيل عن طريق بروتوكول إدارة الشبكة الخاص بطبقة التطبيق.

يستخدم SNMP (بروتوكول إدارة الشبكات البسيط) بروتوكول (UDP) و يقوم بالتواصل من خلال المنفذين 161 و 162. يعتمد هذا البروتوكول على تبادل الرسائل. هناك ثلاثة أنواع شائعة من الرسائل:

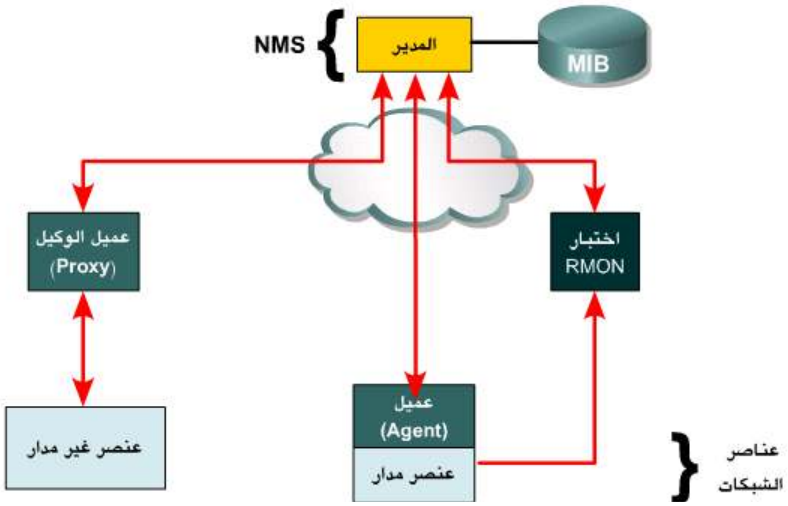
- **Get** – تمكن محطة الإدارة من استعادة قيمة كائنات MIB من الوكيل .
- **Set** – تمكن محطة الإدارة من تعيين قيمة كائنات MIB عند الوكيل .
- **Trap** – تمكن الوكيل (agent) من إعلام محطة الإدارة بالأحداث المهمة .

يطلق على هذا النموذج اسم النموذج ثنائي الطبقات. إلا أن هذا النموذج يفترض إدارة جميع عناصر الشبكة عن طريق SNMP. و لكن هذا لا يحدث دائمًا، حيث تحتوي بعض الأجهزة على واجهة إدارة تخضع لملكية جهات خاصة.

و في هذه الحالات، يلزم استخدام نموذج ثلاثي الطبقات. يتصل مدير الشبكة الذي يرغب في الحصول على معلومات، أو التحكم في هذه العقدة التي تخضع لملكية جهة خاصة بوكيل من نوعproxy . يترجم وكيل proxy بعد ذلك طلب SNMP الذي يقدمه المدير في شكل نموذج مناسب للنظام الهدف و يستخدم أي بروتوكول – يخضع لملكية جهة خاصة – يجده مناسبًا للاتصال بالنظام الهدف. تتم ترجمة الاستجابات من الهدف إلى الوكيل (proxy) في شكل رسائل SNMP يتم توصيلها مرة أخرى إلى المدير .



الشكل 2–3 مكونات نموذج المؤسسة – النموذج ثنائي الطبقات [4]

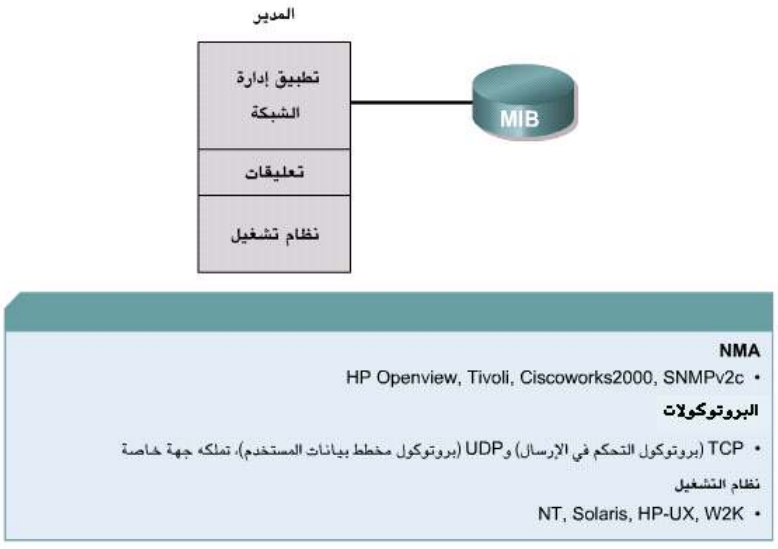


الشكل 2-4 مكونات نموذج المؤسسة – النموذج ثلاثي الطبقات[4]

عادةً ما توكل تطبيقات إدارة الشبكة بعض وظائف إدارة الشبكة إلى مختبر مراقبة عن بعد (RMON) . يجمع مختبر RMON معلومات الإدارة محليًا، ثم يستعيد مدير الشبكة ملخصًا لهذه البيانات دوريًا.

إن نظام NMS (نظام إدارة الشبكة) هو محطة عمل عادية تستخدم نظام تشغيل نمطي. يحتوي هذا النظام على مقدار كبير من ذاكرة الوصول العشوائي (RAM) ، و ذلك لتشغيل جميع تطبيقات الإدارة في نفس الوقت. يقوم المدير بتشغيل مجموعة بروتوكولات شبكة نمطية، مثل TCP/IP (بروتوكول التحكم في الإرسال/بروتوكول الإنترنت). تعتمد تطبيقات إدارة الشبكة على نظام تشغيل المضيف وعلى بنية الاتصالات.

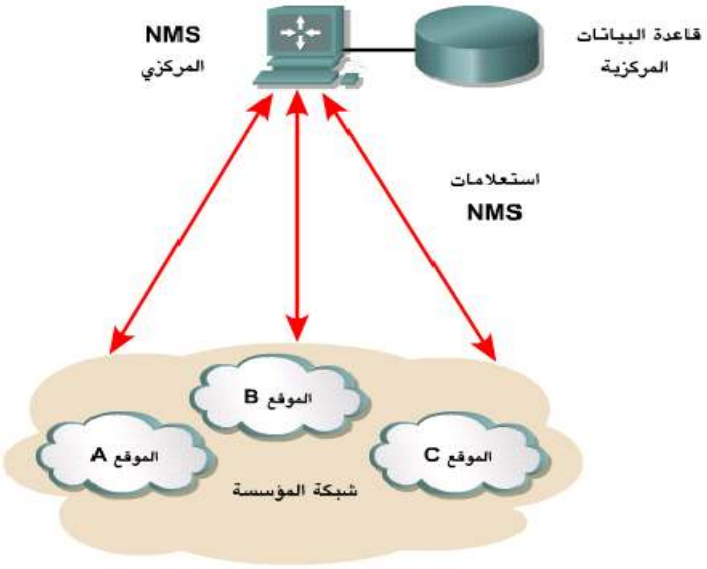
من أمثلة تطبيقات إدارة الشبكة Ciscoworks2000 و HP Openview و SNMPv2c.



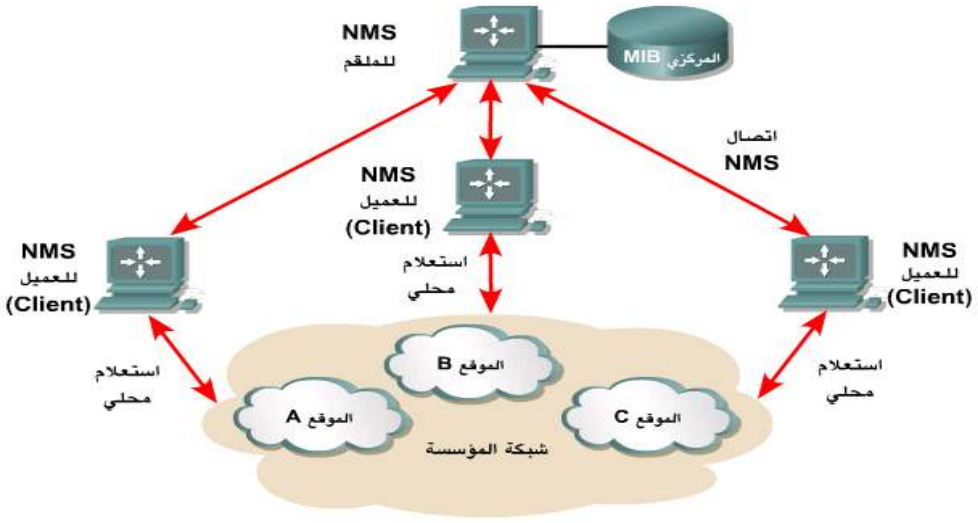
الشكل2-5 نموذج المؤسسة [4]

كما ناقشنا من قبل، قد يكون المدير محطة عمل مركزية قائمة بذاتها ترسل استعلامات إلى جميع الوكلاء ،بغض النظر عن موقعها (الشكل2-6).

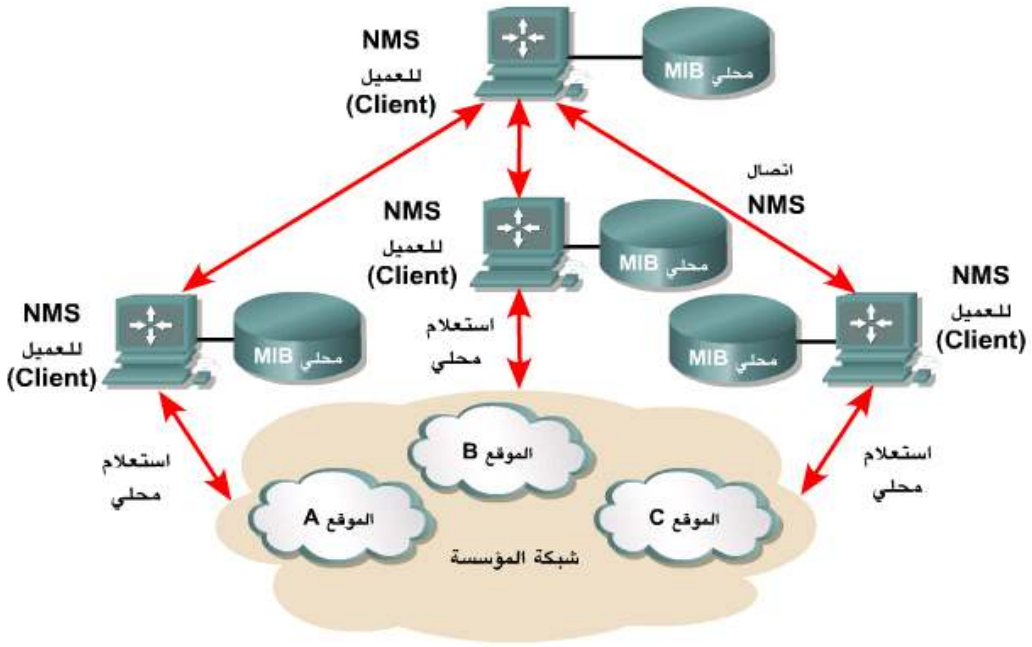
في الشبكة الموزعة، تعد البنية غير المركزية ملائمةً بشكل أكبر ، مع وجود NMS محلية في كل موقع. تعمل NMS الموزعة في بنية العميل – الملقم ،حيث تعمل NMS واحدة كملقم رئيسي و تعمل NMSالأخرى كعملاء (client). يرسل العملاء البيانات الخاصة بهم إلى الملقم الرئيسي لتخزينها مركزيًا (الشكل2-7). ومن الطرق البديلة لذلك منح مسئوليات متساوية لجميع أنظمة NMS الموزعة، بحيث يكون لكل منها قواعد بيانات المديرين الخاصة به، وبذلك يتم توزيع معلومات الإدارة عبر أنظمة NMS النظيرة (الشكل2-8).



الشكل2-6 بنية إدارة الشبكة المركزية [4]



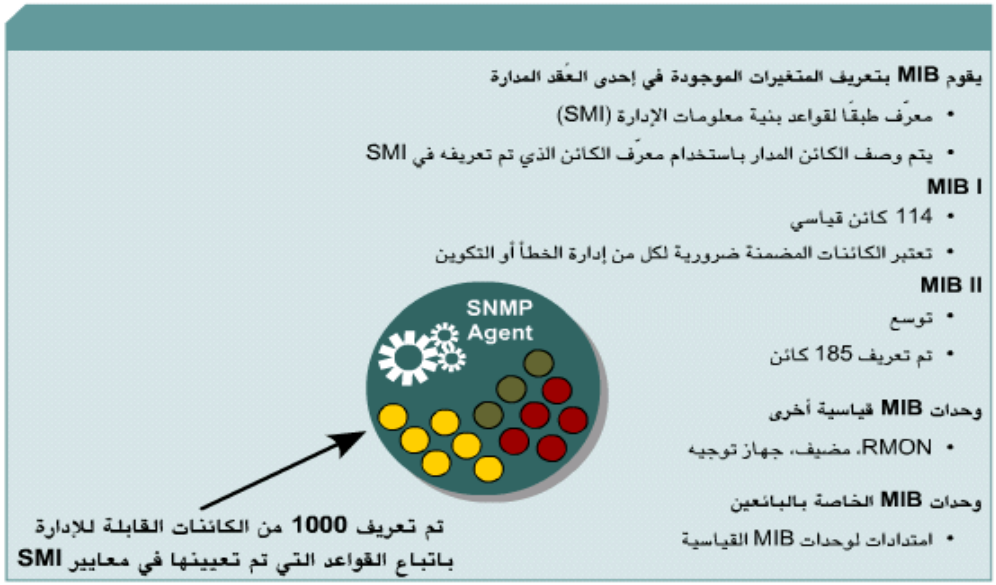
الشكل2-7 بنية إدارة الشبكة غير المركزية [4]



الشكل2-8 بنية إدارة الشبكة الموزعة [4]

2-5 بنية معلومات الإدارة و قواعد MIB :

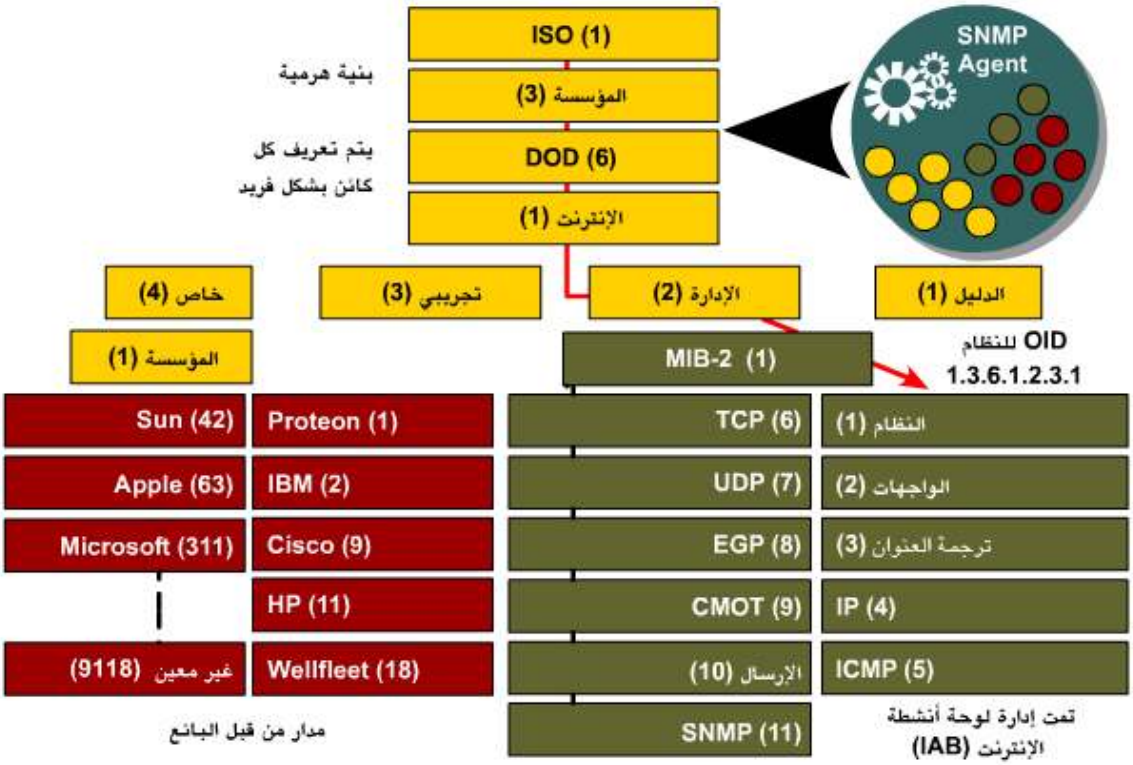
تُستخدم MIB (قاعدة معلومات الإدارة) لتخزين المعلومات البنيوية التي تمثل عناصر الشبكة و سماتها. و قد تم تعريف البنية ذاتها في معيار يسمى SMI (معلومات بنية الإدارة)، و الذي يحدد أنواع البيانات التي يمكن استخدامها لتخزين كائن و كيفية تسمية هذه الكائنات و كيفية ترميزها لإرسالها عبر شبكة (الشكل 2-9).



الشكل2-9 قواعد معلومات الإدارة [4]

تمثل قواعد MIB مستودعات معقدة التركيب لتخزين معلومات حول الجهاز. و توجد العديد من قواعد MIB القياسية، و لكن توجد المزيد من قواعد MIB التي تمتلكها جهات خاصة لإدارة أجهزة البائعين المختلفة بشكل فريد. لقد تم تصنيف SMI MIB الأصلية إلى ثمانية مجموعات مختلفة، بإجمالي 114 كائن مدار. و قد تمت إضافة المزيد من المجموعات لتعريفMIB-II ، التي تحل الآن محل MIB-I .

يتم ترتيب جميع الكائنات المدارة في بيئة SNMP (بروتوكول إدارة الشبكات البسيط) في بنية هرمية أو بنية شجرة. تمثل الكائنات الطرفية للشجرة، و هي العناصر التي تظهر أسفل المخطط، الكائنات الفعلية المدارة .يمثل كل كائن مدار موردًا أو نشاطًا أو معلومات ذات صلة يتم إدارتها. يحدد معرف الكائن الفريد، و هو الرقم المكتوب في شكل تدوين نقطي، كل كائن مدار. يتم وصف كل معرف كائن باستخدام التدوين النقطي لبناء الجملة المجرد (ASN.1) .



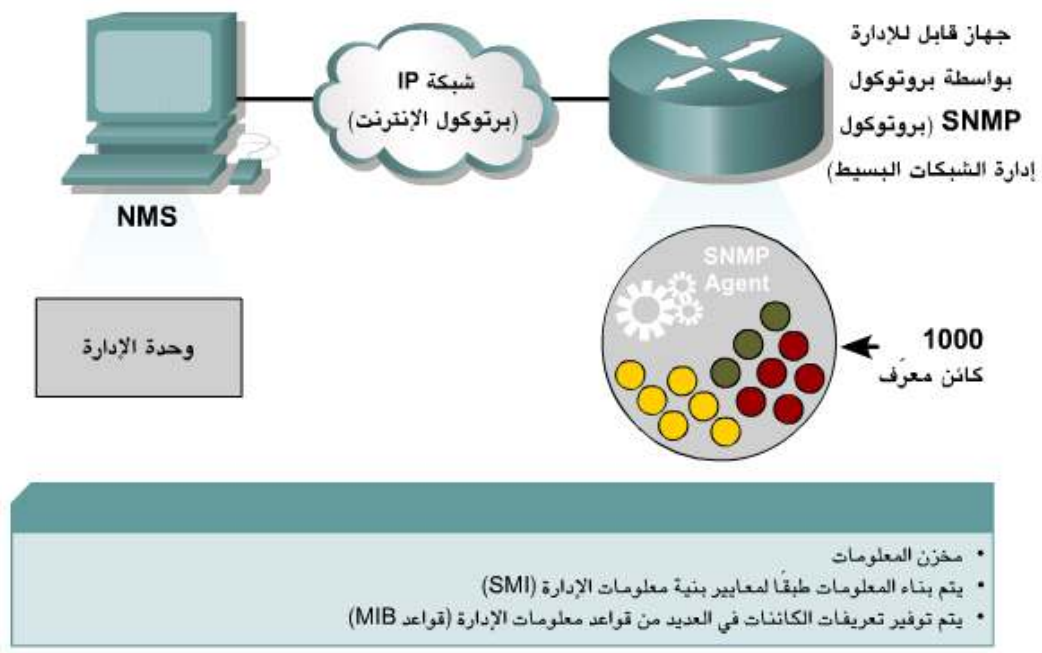
الشكل2-10 معرفات الكائنات [4]

تستخدم SNMP معرفات الكائنات هذه لتعريف متغيرات MIB التي ستتم استعادتها أو تعديلها. يتم وصف الكائنات التي توجد في المجال العام في MIB (قواعد معلومات الإدارة) التي تم تقديمها في RFC (طلبات التعليقات). و يمكن الوصول إليها بسهولة من الموقع http://www.ietf.org/ .

يتم تشجيع جميع البائعين على إعلان تعريفات MIB الخاصة بهم. وبمجرد تحديد قيمة مؤسسة معينة، يصبح البائع مسئولاً عن إنشاء الأشجار الفرعية وصيانتها.

2-6 بروتوكول SNMP :

إن العميل (agent) هي وظيفة برمجية مضمنة في أغلب الأجهزة التي تعمل على شبكة، مثل أجهزة التوجيه (router) و المبدلات (switch) و المجمعات (hub) و الطابعات و الملقمات المدارة .هذا العميل هو المسؤول عن معالجة طلبات SNMP (بروتوكول إدارة الشبكات البسيط) التي يرسلها المدير. كما أنه مسؤول أيضًا عن تنفيذ البرامج الفرعية التي تحافظ على المتغيرات كما تم تعريفها في قواعد MIB (معلومات الإدارة) المعتمدة المختلفة .

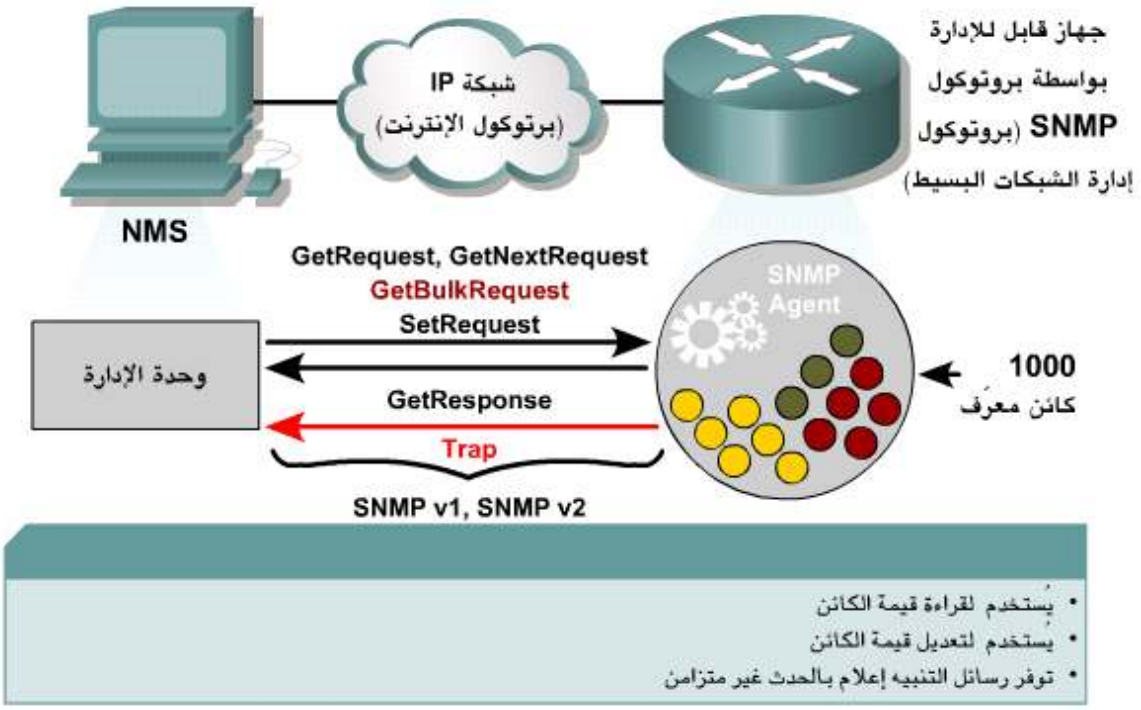


الشكل2-11 شرح الوكيل [2]

و يسهل SNMP التفاعل بين المدير و الوكيل. و يوضح مصطلح "البسيط" في اسم البروتوكول العدد المحدود من أنواع الرسائل التي تمثل جزءًا من مواصفات البروتوكول الأولية .لقد تم تصميم الإستراتيجية لكي يكون من السهل على المطورين تضمين قدرات الإدارة في أجهزة الشبكة. و يطلق على مواصفات البروتوكول الأولية الاسم SNMPv1 (الإصدار 1).

هناك ثلاثة أنواع من رسائل SNMP (بروتوكول إدارة الشبكات البسيط) التي يتم إصدارها بالنيابة عن NMS (نظام إدارة الشبكة). هذه الأنواع هي GetRequest و GetNextRequest و SetRequest .

يقر الوكيل بأنواع الرسائل الثلاثة في شكل رسالة GetResponse. و قد يصدر الوكيل رسالة تنبيه استجابةً لحدث يؤثر على MIB (قاعدة معلومات الإدارة) والموارد الأساسية.



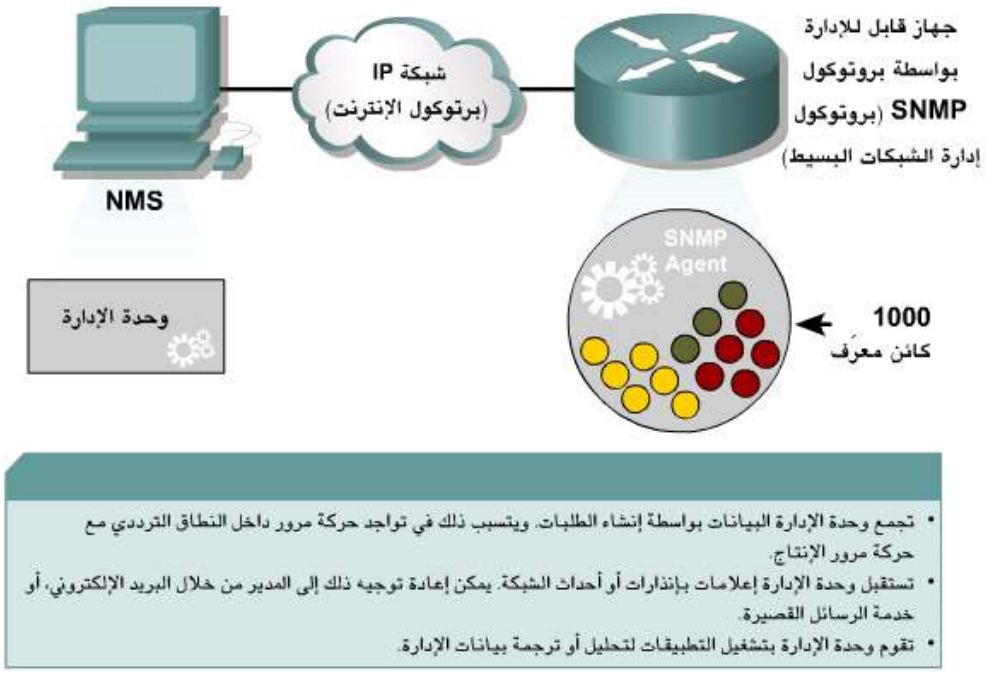
الشكل2-12 شرح البروتوكول SNMP [2]

لقد عالج تطوير SNMPv2c القيود الموجودة في SNMPv1 .و قد كانت أهم التحسينات التي تم إجراؤها هي تقديم نوع الرسالة GetBulkRequest و إضافة عدادات 64 بت إلى MIB .

لم تكن استعادة المعلومات باستخدام GetRequest و GetNextRequest طريقة فعالة لجمع المعلومات. فلم يكن من الممكن الحصول على أكثر من متغير واحد في المرة عند استخدام SNMPv1 . و قد عالجت GetBulkRequest هذا الضعف باستقبال المزيد من المعلومات من طلب واحد.

ثانيًا، عالجت عدادات 64 بت مشكلة دوران العدادات بسرعة شديدة، خاصةً مع الارتباطات عالية السرعة مثل Gigabit Ethernet.

يطلق على وحدة الإدارة أيضًا اسم المدير أو NMS (نظام إدارة الشبكة)(الشكل 2-12) .هذه الوحدة مسؤولة عن الحصول على المعلومات من العميل (agent) . و يعتمد هذا الحصول على طلبات محددة جدًا. يعالج المدير المعلومات التي تم استردادها بطرق متعددة. و يمكن تسجيل المعلومات التي تم استردادها لتحليلها فيما بعد، و يتم عرضها باستخدام أداة رسم بياني أو مقارنتها بالقيم التي تم تكوينها مسبقًا لاختبار ما إذا كان قد تم تلبية شرط معين.



الشكل2-13 شرح وحدة الإدارة [2]

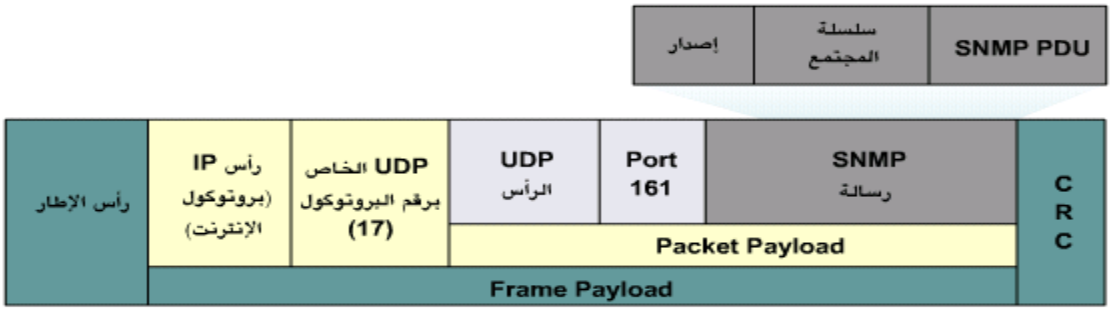
لا تعتمد كل وظائف المدير على استرداد البيانات. فهناك أيضًا القدرة على إجراء تغييرات على قيمة في الجهاز المدار. وهذه الميزة تمكن المسؤول من تكوين جهاز مدار باستخدام SNMP (بروتوكول إدارة الشبكات البسيط).

يؤثر التفاعل بين المدير و الجهاز المدار على حركة المرور في الشبكة.لذلك يجب توخي الحذر عند تقديم المديرين إلى الشبكة. فقد تؤثر استراتيجيات المراقبة المتشددة بشكل سلبي على أداء الشبكة. و سيزيد استخدام عرض النطاق الترددي مما قد يسبب مشكلة في بيئات WAN (الشبكة الواسعة). كما أن المراقبة تؤثر على أداء الأجهزة التي تتم مراقبتها، حيث إنها مطلوبة لمعالجة طلبات المديرين. و يجب ألا يكون لهذه المعالجة الأولوية على خدمات الإنتاج.

إن القاعدة العامة هي الاستعلام عن الحد الأدنى من المعلومات و بأقل تكرار ممكن. حدد الأجهزة والارتباطات الأكثر أهمية و نوع البيانات المطلوبة.

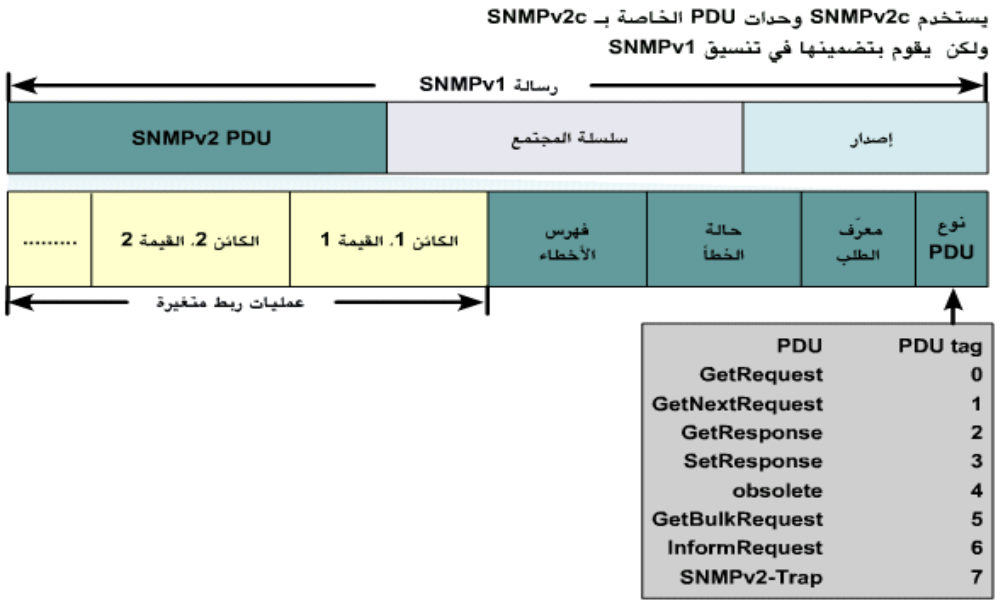
يستخدم SNMP (بروتوكول إدارة الشبكات البسيط) بروتوكول مخطط البيانات (UDP) المستخدم كبروتوكول نقل. لا تعتمد UDP على التواصل (لا يقيم رابطة connectionless) و لا يمكن الاعتماد عليها، و لذلك قد تفقد SNMP بعض الرسائل. بل إن SNMP نفسها لا تحتوي على ترتيب لضمان التسليم، و لذلك يعود الأمر للتطبيق الذي يستخدم SNMP للتكيف مع الرسائل المفقودة.

تحتوي كل رسالة SNMP على سلسلة نصية غير مشفرة تسمى سلسلة المجتمع (community string). يتم استخدام سلسلة المجتمع ككلمة مرور لتقييد الوصول إلى الأجهزة المدارة .لقد عالجت SNMPv3 مشكلات الأمان التي تسبب فيها إرسال سلسلة المجتمع بنص غير مشفر.



الشكل2-14 تنسيق رسالة SNMPV1 [2]

يوضح الشكل التالي مثالا لما تبدو عليه رسالة SNMPv2c .و يمكن العثور على تقديم مفصل للبروتوكول في معيار الإنترنت RFC1905 .

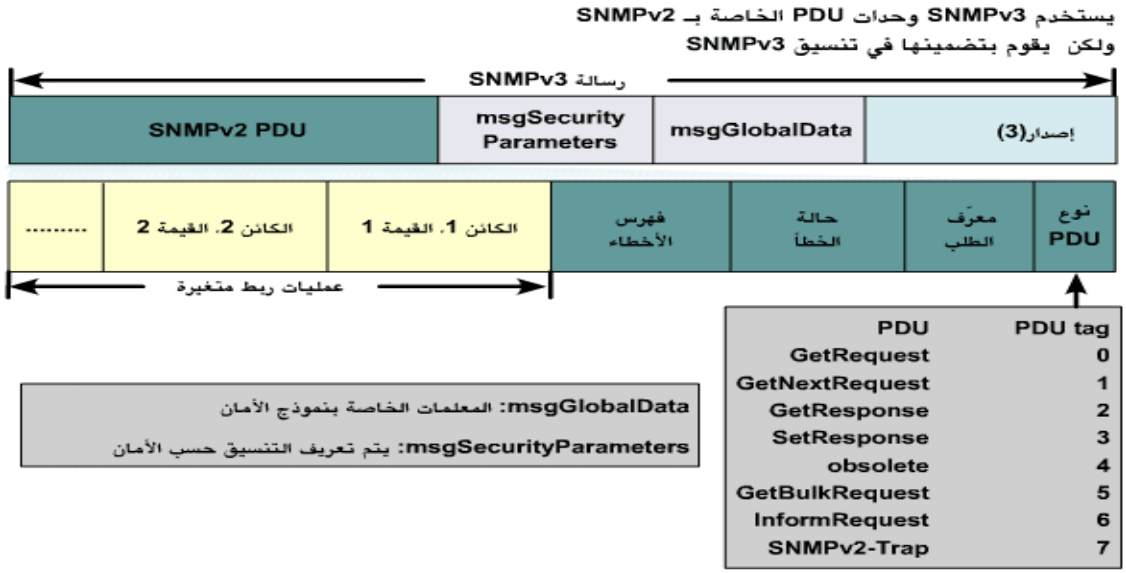


الشكل2-15 تنسيق رسالة SNMPV2 [4]

إن سلسلة المجتمع توجد بشكل غير مشفر ،و هذا لا يثير التساؤل ،فكل الحقول التي تم تحديدها في مجموعة البروتوكولات تمثل نصًا غير مشفر، فيما عدا مواصفات تشفير و مصادقة الأمان.

لقد كانت سلسلة المجتمع عنصر أمان نائب بشكل أساسي حتى تمكنت مجموعة عمل SNMPv2 من التصديق على آليات الأمان. وقد كان ذلك بفضل جهود مجموعة عمل SNMPv3 . تتطلب جميع تطبيقات الإدارة المعتمدة على SNMP(بروتوكول إدارة الشبكات البسيط) تكوينها بحيث تستخدم سلاسل المجتمع المناسبة. و تقوم بعض المؤسسات بشكل متكرر بتغيير قيم سلسلة المجتمع لتقليل مخاطر النشاط السيئ الناتج عن الاستخدام غير المرخص لخدمة SNMP.

على الرغم من وجود نقاط ضعف متعلقة بالمصادقة المعتمدة على المجتمع، ما زالت استراتيجيات الإدارة تعتمد على SNMPv1. تدعم أجهزة Cisco أنواع رسائل SNMPv3 و قدرات الأمان المتزايدة، إلا أن أغلب تطبيقات برامج الإدارة لا تدعم SNMPv3 (الشكل2-16).



الشكل2-16 تنسيق رسالة SNMPV3 [2]

تدعم SNMPv3 تواجد نماذج أمان متعددة متزامنة .

2-6-1 بروتوكولات و ميزات الإدارة :

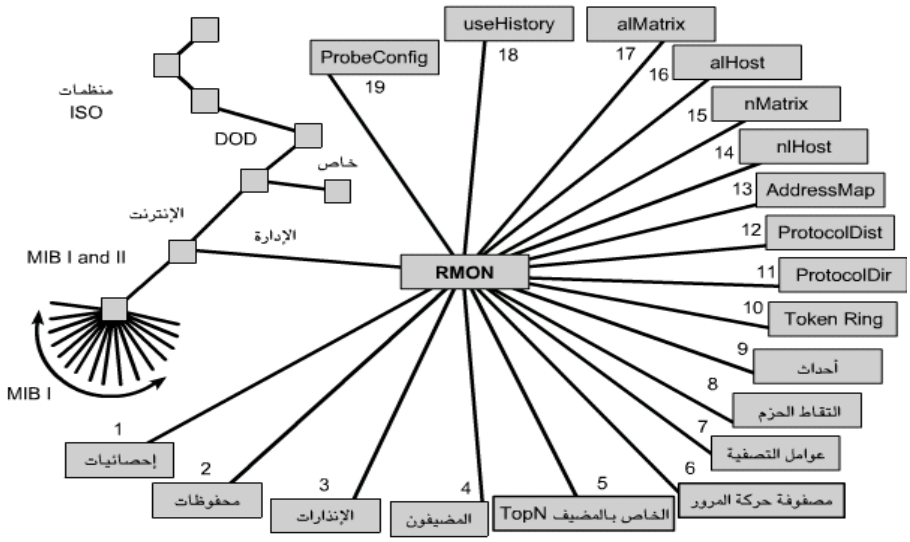
	المستوى	Auth	التشفير	ماذا حدث
SNMPv1	noAuthNoPriv	سلسلة المجتمع		استخدام تتطابق سلسلة المجتمع للمصادقة
SNMPv2c	noAuthNoPriv	سلسلة المجتمع		استخدام تتطابق سلسلة المجتمع للمصادقة
SNMPv3	noAuthNoPriv	اسم المستخدم		استخدام اسم المستخدم سلسلة المجتمع للمصادقة
SNMPv3	authNoPriv	MD5 or SHA		يوفر مصادقة استنادًا إلى خوارزميات HMAC-MD5 أو HMAC-SHA
SNMPv3	authPriv	MD5 or SHA	DES	يضيف تشفير DES ذا 56 بت بالإضافة إلى المصادقة المستندة إلى DES-56

2-7 بروتوكول RMON :

تمثل RMON (المراقبة عن بعد) خطوة هائلة للأمام في إدارة الشبكات البينية. فهي تحدد MIB (قاعدة معلومات الإدارة) الخاصة بالمراقبة عن بعد التي تكمل MIB-II و توفر لمدير الشبكة معلومات حيوية عن الشبكة. و هناك ميزة رائعة في RMON ، و هي أنه على الرغم من كونها مجرد إحدى مواصفاتMIB ، دون أي تغيير في بروتوكول SNMP الأساسي، فهي توفر توسيعًا ملحوظًا لوظائفSNMP .

- إن RMON هو MIB
- يستند RMON إلى IETF RFCs
- يجمع الإحصائيات بواسطة تحليل كل إطار على المقطع
- يُستخدم RMON1 لطبقة ارتباط البيانات
- يُستخدم RMON2 لطبقة الشبكة إلى طبقة التطبيقات
- العمل باستخدام مجس خارجي أو نمط تحليل الشبكة على عامل التنشيط

و مع استخدام MIB-II ، بإمكان مدير الشبكة الحصول على المعلومات المحلية فقط للأجهزة الفردية .و المثال على ذلك LAN (شبكة محلية) بها عدد من الأجهزة لكل منها عميل (agent) لبروتوكول SNMP. بإمكان مدير SNMP التعرف على قدر حركة المرور الواردة و الصادرة من كل جهاز، و لكن مع MIB-II لن يتمكن المدير من التعرف على حركة المرور على LAN بأكملها بسهولة.



الشكل 2-17 RMON MIB [1]

تتطلب إدارة الشبكة في بيئة الشبكات البينية مراقبة واحدة لكل شبكة فرعية.

لقد تم تصميم RMON (معيار المراقبة عن بعد) في البداية كـIETF RFC 1271 ، و قد أصبح الآن RFC 1757، لتوفير المراقبة الوقائية وعمليات التشخيص لشبكات موزعة تعتمد علىLAN. تسمح أجهزة المراقبة، و تسمى العملاء (agent) أو المجسات، في مقاطع الشبكة المهمة بإنشاء إنذارات معرفة من قبل المستخدم و تجميع مجموعة من الإحصائيات الحيوية عن طريق تحليل كل إطار (frame) على المقطع.

يقسم معيار RMON وظائف المراقبة إلى تسع مجموعات لدعم هياكل Ethernet و يضيف مجموعة عاشرة في RFC 1513 لوسطاء Token Ring . لقد تم إنشاء معيار RMON لتوظيفه كبنية كمبيوتر موزعة، حيث يتصل العملاء (agent) و المجسات بمحطة إدارة مركزية، و هي العميل (client) باستخدام SNMP (بروتوكول إدارة الشبكات البسيط). قام هؤلاء العملاء بتعريف بنيات SNMP MIB لجميع مجموعات Ethernet أو Token Ring RMON التسعة أو العشرة، مما يسمح بالتشغيل المتبادل بين بائعي أدوات التشخيص المعتمدة على RMON . يتم تعريف مجموعات RMON كما يلي :

- **مجموعة الإحصائيات** : تحافظ على إحصائيات الأخطاء و الاستخدام الخاصة بالشبكة الفرعية أو المقطع الذي تتم مراقبته. و من أمثلة ذلك استخدام عرض النطاق الترددي و البث و البث المتعدد و محاذاة CRC (فحص التكرار الدوري) و الأجزاء و غيرها .
- **مجموعة المحفوظات** : تحتفظ بنماذج الإحصائيات الدورية التي تحصل عليها من مجموعة الإحصائيات و تخزنها لاستعادتها فيما بعد. و من أمثلة ذلك الاستخدام و عدد الأخطاء و عدد الحزم (packet) .
- **مجموعة الإنذار** : تسمح للمسئول بتعيين فترات زمنية فاصلة بين أخذ العينات و نقطة بدء لأي عنصر قام العميل (agent) بتسجيله .من أمثلة ذلك القيم المطلقة أو النسبية و نقاط البدء المرتفعة أو المنخفضة .
- **مجموعة المضيف** : تحدد قياسات أنواع مختلفة من حركات المرور من الأجهزة المضيفة المتصل بالشبكة وإليها. من أمثلة ذلك الحزم المرسلة أو المستقبلة و البايتات المرسلة أو المستقبلة و الأخطاء و حزم البث و البث المتعدد .
- **مجموعة مضيفي TopN** : توفر تقريرًا حول مضيفي TopN بناءًا على إحصائيات مجموعة المضيفين .
- **مجموعة مصفوفة حركات المرور** : تخزن إحصائيات الاستخدام و الأخطاء لأزواج عقد الاتصال في الشبكة. من أمثلة ذلك الأخطاء و البايتات و الحزم .
- **مجموعة التصفية** : محرك تصفية يُنشئ تدفق حزم من الإطارات التي تطابق النمط الذي يحدده المستخدم .
- **مجموعة التقاط الحزم** : تحدد كيفية تخزين الحزم التي تطابق معيار التصفية داخليًا بشكل مؤقت .
- **مجموعة الأحداث** : تسمح بتسجيل الأحداث، التي تسمى أيضًا رسائل التنبيه المنشأة، في المدير، مع وقت و تاريخ حدوثها. من أمثلة ذلك التقارير المخصصة المعتمدة على نوع رسالة الإنذار .

الفصل الثالث

مراقبة الشبكات

3-1 تمهيد :

يعبر مصطلح مراقبة الشبكة عن استخدام أدوات تجميع و تحليل المعلومات لتحديد كيفية سير البيانات ضمن الشبكة و استهلاك مواردها بالإضافة إلى العديد من المؤشرات على أداء هذه الشبكة .توفر أدوات المراقبة الجيدة قياسات لمؤشرات أداء الشبكة إلى جانب قدرتها على تجميع هذه الأرقام و إظهارها بشكل بياني مما يساعد على تكوين صورة واضحة عن حالة الشبكة و بالتالي تقدير مدى الحاجة إلى أية تعديلات .

تتيح هذه الأدوات الإجابة على أسئلة فائقة الأهمية مثل:

- ما هي أكثر الخدمات استخداماً على الشبكة؟
- من هم المستخدمون الأكثر استهلاكاً لموارد الشبكة؟
- متى يبلغ استخدام الشبكة ذروته أثناء النهار؟
- ما هي المواقع التي يتردد عليها مستخدمو الشبكة؟
- هل يقارب حجم البيانات المرسلة أو المستقبلة الاستطاعة المتاحة للشبكة؟
- أتوجد مؤشرات على حالة غير طبيعية ضمن الشبكة تتسبب في استهلاك عرض الحزمة أو في مشاكل أخرى؟
- هل يوفر لنا مزود خدمة الإنترنت ISP مستوى الخدمة المتفق عليه؟ تنبغي الإجابة على هذا السؤال من حيث عرض الحزمة المتاح ومدى ضياع حزم البيانات والتأخير ومستوى وثوقية الشبكة.
- هل تتطابق الأنماط الفعلية لاستخدام الشبكة مع توقعاتنا؟

خلال هذا الفصل سنسلط الضوء على مجموعة من الأدوات المستخدمة في مراقبة الشبكة و نلقي نظرة على كيفية استثمار هذه الأدوات بشكل فعال من قبل مدير الشبكة.

3-2 مثال عن المراقبة الفعالة للشبكة:

سنفترض بأننا مسؤولين عن شبكة بنيت منذ ثلاثة أشهر و تضم 50 حاسوباً و ثلاثة مخدمات :مخدم للبريد الإلكتروني و مخدم للوب و مخدم وكيل .بعد فترة وجيزة عملت الشبكة خلالها بشكل جيد بدأ المستخدمون بالتذمر من بطء هذه الشبكة و من ازدياد ملحوظ في رسائل البريد الإلكتروني غير المرغوبة (Spam) ، و من الواضح أيضاً أن أداء الحواسيب يزداد بطأً مع مرور الوقت (حتى في حال عدم استخدام الشبكة) مما يتسبب في توتير و إزعاج المستخدمين.

دفع تزايد الشكاوى و الإستثمار شبه المعدوم للحواسيب مجلس إدارة الشركة إلى التساؤل عن مدى الحاجة إلى جميع تجهيزات الشبكة المستخدمة .يريد مجلس الإدارة أيضاً الحصول على أدلة عملية تثبت دون مجال للشك بأن كامل عرض الحزمة الذي يكلف الشركة مبالغ طائلة مستثمر فعلياً .

ستصل جميع هذه الشكاوى إلى مدير الشبكة .كيف سيستطيع اكتشاف السبب الكامن وراء الإنخفاض المفاجئ في أداء الشبكة والحواسيب المتصلة بها بالإضافة إلى تبرير تكاليف تجهيزات هذه الشبكة و عرض الحزمة المرافق؟

3-3 مراقبة الشبكة المحلية :

للحصول على فكرة واضحة عن أسباب انخفاض أداء الشبكة ينبغي البدء بمراقبة تدفق البيانات ضمن الشبكة المحلية . تنطوي مراقبة الشبكة المحلية على عدة فوائد:

- تبسيط عملية كشف الأعطال بشكل كبير
- إمكانية إكتشاف الفيروسات والتخلص منها
- إمكانية إكتشاف المستخدمين المزعجين و التعامل معهم
- إمكانية تبرير تكاليف تجهيزات و موارد الشبكة باستخدام إحصائيات حقيقية

3-4 مراقبة الشبكة الواسعة WAN :

يتوجب بالإضافة إلى مراقبة تدفق البيانات ضمن الشبكة المحلية الاثبات لمجلس الإدارة بأن عرض الحزمة الذي يوفره مزود خدمة الإنترت للوصلة التي تصل المؤسسة بالإنترنت يساوي ذلك المتفق عليه أثناء التعاقد، و هو ما يتطلب مراقبة البيانات المنقولة إلى خارج الشبكة المحلية.

تطلق تسمية تدفق البيانات الخارجي على أية بيانات ترسل عبر الشبكة الواسعة WAN و يشمل أية بيانات مرسلة إلى (أو مستقبلة من) شبكة أخرى غير الشبكة المحلية .

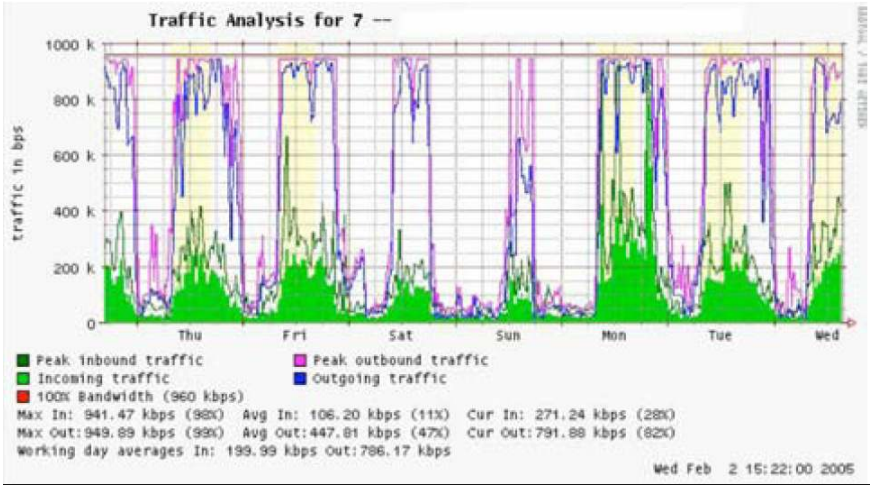
من فوائد مراقبة تدفق البيانات الخارجي:

- تبرير تكاليف الإتصال بشبكة الإنترنت عبر إظهار الإستثمار الفعلي و فيما إذا كان الإتفاق المبرم مع مزود خدمة الإنترنت ملائماً لهذا المستوى من الإستهلاك.
- تقدير المتطلبات المستقبلية للشبكة عبر متابعة أنماط الإستخدام الحالية والتنبؤ باحتمالات النمو والتوسع.
- اكتشاف المتطفلين القادمين من شبكة الإنترنت وإيقافهم قبل إيذاء الشبكة.

3-5 كشف إنقطاعات الشبكة :

نستطيع بعد تركيب أدوات مراقبة الشبكة الحصول على قياسات أفضل لعرض الحزمة الذي سيستهلكه المستخدمون في المؤسسة .تشير هذه القياسات أيضاً إلى الإستطاعة الفعلية لوصلة الإنترنت في حال اقتراب استهلاك هذه الوصلة في ساعات الذروة من عرض الحزمة الأقصى المتاح. تعتبر الرسوم البيانية و التي تكون قمتها مسطحة إشارة واضحة إلى استهلاك كامل عرض الحزمة المتاح للوصلة الموافقة.

يوضح الشكل 3-1 عدة قمم مسطحة لتدفق البيانات الصادر من الشبكة في ساعات الذروة منتصف النهار كل يوم تقريباً باستثناء العطلة الأسبوعية.



الشكل3-1 مخطط تدفق البيانات [3]

من الواضح بأن استهلاك وصلة الإنترنت الحالية في ساعات الذروة يتجاوز استطاعتها القصوى مما يتسبب بالكثير من التأخير في استجابة الشبكة .

يمكن بعد تقديم هذه الرسوم البيانية لمجلس الإدارة التخطيط لتحسين أداء الوصلة الحالية و توقع الفترة الزمنية التي ستضطر بعدها إلى تطوير وصلة الإنترنت لكي تتجاوب مع تزايد الطلب عليها .تمثل هذه العملية أيضاً فرصة ممتازة لمراجعة سياسة تشغيل الشبكة مع مجلس الإدارة و مناقشة إمكانيات إعادة الإستثمار الفعلي للشبكة ليتوافق مع هذه السياسة.

يأتي بعد أيام من معالجة هذه المشاكل إتصال طارئ في منتصف الليل لإعلام مدير الشبكة بأن جميع المستخدمين في الشركة دون استثناء غير قادرين على تصفح الإنترنت أو إرسال بريدهم الإلكتروني .سيسرع لاهثاً إلى الشركة لإعادة تشغيل المخدم الوكيل لكن دون فائدة، فما زالت الإنترنت مقطوعة عن الشبكة .يقرر حينها إعادة تشغيل الموجه دون أن يفلح في حل المشكلة. سيتابع عزل مواقع الخلل واحداً تلو الآخر حتى يجد بأن مبدل الشبكة لا يعمل بسبب عدم تركيب مقبس التغذية الكهربائية بشكل جيد .وبمجرد إعادة توصيل هذا المقبس ستعود الشبكة إلى العمل.

كيف يمكن اكتشاف عطل كهذا دون أن نسلك طريق التجربة والخطأ المضيع للوقت؟ هل يمكن الاعلام بانقطاعات الشبكة عند حدوثها عوضاً عن انتظار شكاوى المستخدمين؟ والجواب هو نعم، يمكن الاعلام بانقطاعات الشبكة عند حدوثها باستخدام برامج مثل **Nagios** و الذي يقوم بتفقد تجهيزات الشبكة دورياً و الاعلام عند حدوث أي انقطاع، كما ينتج هذا البرنامج تقارير عن توفر التجهيزات والخدمات المختلفة ضمن الشبكة و إرسال تنبيه عند تعطل إحداها عن العمل . يمكن لهذا البرنامج أيضاً بالإضافة إلى عرض وضعية الشبكة بشكل بياني عبر متصفح الوب أن يرسل التنبيهات عبر خدمات الرسائل القصيرة SMS أو البريد الإلكتروني للإعلام مباشرة عند وقوع المشكلة.

سنتمكن باستخدام أدوات جيدة لمراقبة الشبكة من تبرير تكاليف التجهيزات و عرض حزمة وصلة الإنترنت عبر إثبات كيفية استثمارها في المؤسسة، عدا عن الاعلام مباشرة بمشاكل الشبكة عند وقوعها و الإحتفاظ بإحصائيات تاريخية عن

كيفية أداء تجهيزات الشبكة المختلفة. يمكن مقارنة أداء الشبكة الحالي مع هذه الإحصائيات لاكتشاف أية تصرفات مشبوهة و بالتالي معالجة أية مشاكل محتملة قبل حدوثها .و سيصبح بمقدورنا أيضاً في حال وقوع مشكلة ما تحديد مصدر و طبيعة هذه المشكلة بسهولة .أي باختصار ستسهل مهمة مدير الشبكة و يرضي مجلس الإدارة و يرسم البسمة على وجوه المستخدمين.

3-6 مراقبة الشبكة:

تشبه عملية إدارة الشبكة دون مراقبة قيادة السيارة دون عداد السرعة أو مؤشر الوقود و بأعين مغلقة .كيف سنتمكن من تحديد السرعة؟ هل يتلاءم استهلاك السيارة الفعلي للوقود مع وعود مندوب المبيعات؟ هل ستزداد سرعة السيارة أو سينخفض استهلاكها للوقود بعد صيانة المحرك بعد عدة أشهر؟
كيف سنتمكن من دفع فواتير الماء والكهرباء دون قراءة الاستهلاك الشهري من العداد؟ كذلك أيضاً يتوجب الإحتفاظ بسجل عن مدى استهلاك عرض الحزمة ضمن الشبكة لتبرير تكاليف الخدمات ونفقات التجهيزات وللإطلاع على طبيعة استهلاك الشبكة بشكل عام.

ينطوي بناء نظام فعال لمراقبة الشبكة على عدة فوائد منها:

1. **تبرير مصاريف الشبكة والموارد المرافقة**: توفر أدوات المراقبة الجيدة إثباتات لا تدع مجال للشك بأن البنية التحتية للشبكة (عرض الحزمة والتجهيزات والبرمجيات) ملائمة لمتطلبات المؤسسة و بأنها قادرة على تلبية احتياجات مستخدمي هذه الشبكة.
2. **إكتشاف المتطفلين على الشبكة و منعهم من إيذائها**: يمكن من خلال مراقبة الشبكة اكتشاف أية محاولات للهجوم عليها و إحباط هذه المحاولات قبل وصولها إلى الخدمات الحساسة في الشبكة.
3. **إكتشاف الفيروسات بسهولة**: تمكن مراقبة الشبكة من التنبه إلى أية فيروسات و اتخاذ القرارات الملائمة قبل أن تستهلك هذه الفيروسات كامل عرض الحزمة المتاح لوصلة الإنترنت و الإضرار بالشبكة بأكملها.
4. **تبسيط معالجة مشاكل الشبكة بشكل هائل**: يمكن بواسطة مراقبة الشبكة التنبه إلى مشاكل الشبكة عند حدوثها عوضاً عن اتباع أسلوب "التجربة والخطأ" لحل هذه المشاكل، حتى أن بعض أنواع المشاكل قد تحل بشكل تلقائي.
5. **تحسين أداء الشبكة بشكل كبير**: يستحيل دون المراقبة الفعالة للشبكة تحسين أداء التجهيزات و البروتوكولات العاملة ضمنها للوصول إلى أفضل أداء ممكن.
6. **تسهيل عملية تخطيط إستطاعة الشبكة**: يكمن الحل الوحيد لمواجهة محدودية عرض الحزمة و ضمان التوزيع العادل لجميع المستخدمين في التأكد من أن استثمار الشبكة يتلاءم مع الغرض المرجو منها.

لا تتطلب مراقبة الشبكة ولحسن الحظ تكبد مصاريف باهظة حيث توجد الكثير من البرمجيات مفتوحة المصدر المتاحة مجاناً و التي بمقدورها إظهار حالة الشبكة بالتفصيل .سنعرض ضمن هذا الفصل بعض الأدوات الهامة.

3-7 أنواع أدوات المراقبة :

سنلقي فيما يلي نظرة على بعض أنواع أدوات المراقبة .أدوات **كشف الأعطال Spot check** مصممة لأغراض كشف الأعطال و تعمل عادة بشكل تفاعلي لفترات وجيزة من الزمن .يمكن اعتبار البرنامج Ping على سبيل المثال أداة كشف فعالة لأنه يقوم بتوليد حزم البيانات للإستعلام عن وجود جهاز معين .تعتبر **محللات البروتوكولات Analyzers Network** أدوات كشف خاملة لأنها تتفحص كل حزمة بيانات تمر عبر الشبكة لتقديم تفاصيل كاملة عن أية محادثة تتم عبر الشبكة (بما فيها عنوان كل من المصدر و الوجهة ومعلومات بروتوكول الإتصال المستخدم وحتى معلومات التطبيقات كمحتوى رسائل البريد الإلكتروني). تقوم أدوات **تحليل الأنماط Trending** بمراقبة الشبكة كلياً لفترات طويلة من الزمن و إظهار هذه المعلومات على شكل رسم بياني، في حين تقوم **أدوات المراقبة في الزمن الحقيقي real-time monitoring** بنفس المهمة لكنها تعلم مدير الشبكة مباشرة عند اكتشافها لأي خلل .توفر أدوات **اختبار إنتاجية الشبكة throughput testing** معلومات عن عرض الحزمة المتاح فعلياً بين نقطتين ضمن الشبكة بينما تقوم أدوات **كشف التسلل intrusion detection** بالمراقبة المستمرة لاكتشاف أي بيانات غير طبيعية أو غير مرغوب فيها و اتخاذ الإجراءات اللازمة (و التي تتطلب عادة إيقاف المتسلل و/أو تنبيه مدير الشبكة). أما أدوات **القياس benchmarking** فتقوم بتقدير أقصى أداء ممكن لخدمة ما أو لوصلة محددة ضمن الشبكة.

3-7-1 أدوات كشف الأعطال Spot Check Tools :

- **Ping**:

تحتوي غالبية أنظمة التشغيل (بما فيها ويندوز Windows ، Mac OS X، وبالتأكيد GNU/Linux و BSD) على نسخة من أداة **ping**. تعتمد هذه الأداة على حزم بروتوكول رسائل تحكم الإنترنت ICMP لمحاولة الإتصال بمضيف ما لتعود و تخبرنا بالزمن الذي استغرقه الحصول على رد من هذا المضيف.

إن تأخر الرد على الحزم المرسلة لفترة طويلة من الزمن يعني بأن الشبكة تعاني من الإزدحام في مكان ما، أما إذا كانت قيمة **زمن البقاء على قيد الحياة (TTL)** Time To Live في الحزم العائدة صغيرة جداً فقد يكون السبب في ذلك وجود مشاكل في التوجيه بين الحاسوب المحلي و بين الحاسوب البعيد .ولكن ما الذي ينبغي عمله إذا لم تظهر أداة ping أية بيانات على الإطلاق؟ إذا حاولنا الإتصال بإسم نطاق DNS قد يعني ذلك وجود مشاكل محتملة في خدمة ترجمة أسماء النطاق DNS.

نحاول الإتصال بعنوان ما IP على شبكة الإنترنت .إذا لم نتمكن من الوصول إلى هذا العنوان ينبغي تجربة الإتصال بموجه الشبكة الرئيسي .إذا لم نتمكن من الإتصال بالموجه الرئيسي فلن نستطيع على الأغلب الإتصال بالإنترنت .أما إذا لم نتمكن من الإتصال بعناوين إنترنت IP أخرى ضمن الشبكة المحلية يجب التأكد من الوصلة.

- **Traceroute و mtr** (*http://www.bitwizard.nl/mtr/*)

تتواجد أداة traceroute كما ping في معظم أنظمة التشغيل (وتسمى **tracert** في بعض إصدارات نظام التشغيل ويندوز ،و يمكن استخدام traceroute لتحديد موقع الخلل في الوصلة بين الحاسوب المحلي و أي نقطة على شبكة الإنترنت:

```
$ traceroute -n google.com
traceroute to google.com (72.14.207.99), 64 hops max, 40 byte packets
1 10.15.6.1 4.322 ms 1.763 ms 1.731 ms
2 216.231.38.1 36.187 ms 14.648 ms 13.561 ms
3 69.17.83.233 14.197 ms 13.256 ms 13.267 ms
4 69.17.83.150 32.478 ms 29.545 ms 27.494 ms
5 198.32.176.31 40.788 ms 28.160 ms 28.115 ms
6 66.249.94.14 28.601 ms 29.913 ms 28.811 ms
7 172.16.236.8 2328.809 ms 2528.944 ms 2428.719 ms
8 * * *
```

يقوم الخيار **n–** بإعلام traceroute لإهمال ترجمة أسماء النطاق DNS ويؤدي بالتالي إلى تسريع العمل .نلاحظ أن زمن رحلة الذهاب والإياب يزداد بحدة ليفوق الثانيتين عند المحطة السابعة في حين يبدو أن حزم البيانات تضيع كلياً عند المحطة الثامنة .قد يدل ذلك على وجود مشكلة في تلك المنطقة من الشبكة، و في حال كانت هذه المنطقة تابعة للشبكة المحلية يجب البدء بكشف العطل إنطلاقاً منها.

يجمع برنامج My TraceRoute **(mtr)** أداتي ping و traceroute في برنامج واحد. يمكن باستخدام هذا البرنامج الحصول على متوسط زمن التأخير وخسارة حزم البيانات في مضيف واحد عوضاً عن المعلومات اللحظية التي توفرها أداتي ping و traceroute.

3-7-2 أدوات تحليل البروتوكولات Protocol Analyzers

تستخلص برمجيات تحليل البروتوكولات الكثير من التفاصيل عن المعلومات المنقولة عبر الشبكة من خلال تفحص حزم البيانات المارة كل على حدة .يمكن باستخدام هذه البرمجيات تفحص حزم البيانات ضمن الشبكة السلكية بدءاً من مستوى طبقة وصلة البيانات فما فوق، أما في الشبكات اللاسلكية فيمكن التمحيص في جميع المعلومات وصولاً إلى إطارات بروتوكول 802.11. فيما يلي مجموعة من البرمجيات الشهيرة (والمجانية) لتحليل البروتوكولات:

- **tcpdump** (*http://www.tcpdump.org/*)

وهي أداة تعمل ضمن سطر الأوامر command line لمراقبة تدفق البيانات ضمن الشبكة، وعلى الرغم من أنها لا تتمتع بجميع الميزات التي يشملها برنامج wireshark إلا أنها أخف حملاً على استهلاك موارد النظام .يمكن لهذه الأداة تجميع وعرض معلومات جميع بروتوكولات الشبكة وصولاً إلى طبقة الوصلة link layer كما يمكنها عرض جميع ترويسات حزم البيانات بالإضافة إلى البيانات المحمولة ضمن هذه الحزم أو عرض حزم البيانات التي تحقق شروطاً معينة فقط .

- **Wireshark** (*http://www.ethereal.com/*).

وهو برنامج حر لتحليل البروتوكولات يعمل ضمن أنظمة التشغيل يونيكس Unix وويندوز Windows ،و يعتبر "أكثر برمجيات تحليل البروتوكولات شعبية في العالم".

يتيح برنامج Wireshark تفحص البيانات المارة عبر الشبكة بشكل حي و مباشر أو من ملف يحتوي على بيانات ملتقطة مسبقاً و استعراض هذه البيانات وترتيبها حسب الحاجة. يمكن عرض المعلومات بشكل مختصر أو بالتفصيل لكل حزمة من حزم البيانات بما فيها معلومات الترويسة بالكامل إضافة إلى البيانات المحمولة ضمن الحزمة .يتميز برنامج Wireshark بالعديد من الميزات المتطورة والتي تشمل لغة متقدمة لفلترة البيانات و آلية لإعادة تركيب معطيات بروتوكول TCP.

3-7-3 أدوات تحليل الأنماط Trending Tools

تستخدم أدوات تحليل الأنماط لمراقبة استخدام الشبكة على مدى فترة من الزمن، وتقوم هذه الأدوات بمراقبة أداء الشبكة بشكل دوري وعرض ملخص بالنتائج بصيغة يسهل استيعابها (كرسم بياني مثلاً). تقوم أدوات تحليل الأنماط بتجميع البيانات وتحليلها وعرضها في آن معاً.

ينبغي استخدام بعض هذه الأدوات مع بعضها البعض لأنها ليست برمجيات متكاملة بحد ذاتها.

فيما يلي بعض أمثلة أدوات تحليل الأنماط .:

- **MRTG** (*http://people.ee.ethz.ch/~oetiker/webtools/mrtg/*)

تقوم أداة التمثيل البياني لتدفق البيانات ضمن عدة موجهات Multi Router Traffic Grapher (MRTG) بمراقبة استهلاك وصلات الشبكة بواسطة بروتوكول إدارة الشبكة البسيط SNMP وتوليد رسوم بيانية تمثل البيانات الصادرة والواردة ضمن كل وصلة .تعرض هذه الرسوم البيانية عادة ضمن برنامج لتصفح الوب.

- **Ntop** : http://www.ntop.org/

تقوم هذه الأداة ببناء تقرير تفصيلي بالزمن الحقيقي لنشاط الشبكة وعرضه ضمن متصفح للوب .يمكن تضمينها مع برنامج RDDtool لكي تظهر الأشكال والرسوم البيانية بشكل مرئي كيفية استخدام الشبكة مع مرور الزمن .تستهلك هذه الأداة الكثير من موارد المعالج ومساحة القرص الصلب في الشبكات المزدحمة لكنها تمنح رؤية دقيقة عن كيفية استخدام الشبكة .تعمل هذه الأداة مع أنظمة التشغيل Mac OS X، BSD، GNU/Linux و ويندوز Windows .

من الميزات التي توفرها أداة ntop ما يلي:

- ترتيب عرض نشاط الشبكة وفق معايير مختلفة (المصدر، الوجهة، البروتوكول، عنوان MAC إلخ) .
- تجميع إحصائيات نشاط الشبكة وفق البروتوكول أو رقم البوابة .
- مصفوفة تدفق البيانات والتي تظهر الوصلات بين الأجهزة المختلفة.
- تدفق البيانات للموجهات أو المبدلات التي تدعم بروتوكول NetFlow .
- تحديد نظام التشغيل المستخدم على كل جهاز.
- تحديد البيانات المرسلة من قبل برمجيات الند للند P2P.
- تشكيلة هائلة من الأشكال البيانية.
- واجهة برمجة التطبيقات API لكل من Python و PHP، Perl .

وهو متوفرة لأغلب أنظمة التشغيل، كما تأتي مرفقة على الأرجح مع الكثير من توزيعات نظام التشغيل GNU/Linux الشهيرة مثل ريد هات RedHat ديبيان Debian و أوبونتو Ubuntu . قد تستهلك هذه الأداة قسطاً لا بأس به من استطاعة المعالج في الحاسوب المضيف تبعاً لكمية البيانات التي تتم مراقبتها.

من أبرز مساوئ الأداة ntop عجزها عن توفير معلومات لحظية لأنها تعتمد أساساً على القيم الكلية والمتوسطة على مدة فترة زمنية محددة، مما يحول دون إمكانية استخدامها لكشف المشاكل التي قد تظهر فجأة.

- **Cacti** : http://www.cact.net

وهي واجهة لحزمة الأدوات RDDtool تحتفظ بجميع المعلومات الضرورية لتوليد الرسوم البيانية ضمن قاعدة بيانات MySQL . كتبت هذه الأداة بلغة PHP وتتولى مهام إدارة الرسوم البيانية و مصادر المعلومات بالإضافة إلى القيام بعملية تجميع البيانات، و تدعم أيضاً بروتوكول إدارة الشبكة البسيط SNMP و البرمجة المخصصة لاستحضار أي حدث يمكن أن يقع ضمن الشبكة.

بمقدور الأداة Cacti إدارة تجميع البيانات من تجهيزات الشبكة المختلفة وبناء رسوم بيانية معقدة جداً لكيفية تصرف الشبكة.

- **NetFlow** http://en.wikipedia.org/wiki/NetFlow

وهو بروتوكول لتجميع معلومات تدفق بيانات بروتوكول الإنترنت IP صممته شركة سيسكو Cisco اقتبسنا المقتطفات التالية من موقع الشركة :

يوفر بروتوكول Cisco IOS NetFlow مجموعة من الخدمات الأساسية لتطبيقات بروتوكول الإنترنت IP تشمل إحصائيات تدفق البيانات ضمن الشبكة ، تخطيط الشبكة، الأمن، إمكانيات مراقبة هجمات إيقاف الخدمة Denial of Service و مراقبة الشبكة .يقدم هذا البروتوكول معلومات قيمة عن مستخدمي الشبكة و تطبيقاتها و أوقات الذورة في استهلاك الشبكة و توجيه حزم البيانات.

يمكن لموجهات سيسكو Cisco توليد معلومات بروتوكول NetFlow على شكل حزم UDP و يعتبر هذا البروتوكول أقل نهماً لموارد المعالج CPU في الموجه مقارنة ببروتوكول إدارة الشبكة البسيط SNMP مما يتيح الحصول على صورة أكثر وضوحاً عن طبيعة استخدام البروتوكولات و بوابة الإنترنت ضمن الشبكة. يتم تجميع هذه المعلومات بواسطة مجمّع لبروتوكول NetFlow يحتفظ بالبيانات و يعرض حاصل جمعها مع مرور الزمن .يمكن عبر تحليل تدفق البيانات عبر الشبكة بناء صورة واضحة لسير البيانات و كميتها ضمن الشبكة بأكملها أو عبر إحدى وصلاتها .

- **Flowc** http://netcad.kiev.ua/flowc

وهو برنامج مفتوح المصدر لتجميع معلومات بروتوكول NetFlow ،صغير الحجم وسهل الإعداد .يعتمد **Flowc** على قاعدة بيانات MySQL لتخزين معلومات تدفق البيانات المجمعة، لذلك يمكن تعديل تقارير المولدة تبعاً لمتطلبات المستخدم بناء على هذه المعلومات أو استخدام التقارير القياسية الموجودة أساساً في البرنامج .بمقدور أداة توليد التقارير المضمنة في البرنامج إعداد التقارير بصيغة HTML أو كملفات نصية أو بصيغة رسومية .

- **Argus** : http://qosient.com/argus/

تعود هذه التسمية إلى اختصار عبارة "نظام توليد سجلات التدقيق والإستثمار " Audit Record Generation and Utilization System كما تشير أيضاً إلى إسم أحد الآلهة اليونانية الأسطورية والذي يقال بأن له مئات الأعين.

اقتبسنا المقتطف التالي من موقع Argus على الإنترنت:

يقوم Argus بتوليد إحصائيات تدفق البيانات كعدد الوصلات و الإستطاعة و الطلب و الخسارة و التأخير و التقطّع jitter لكل معاملة تتم عبر الشبكة، ويمكن استخدامه لتحليل محتويات ملفات تجميع حزم البيانات أو بشكل حي عبر الشبكة حيث سيقوم بتفحص البيانات المارة عبر منفذ ما ضمن الشبكة وتوليد سجل بجميع النشاطات التي تمت عبر هذا المنفذ .قد يستخدم Argus لمراقبة أنشطة تجهيزات معينة أو للشبكة بأكملها .يوفر Argus أثناء عمله ضمن نمط التفحص الحي للشبكة أسلوبين للتعامل مع البيانات :الضغط Push أو السحب Pull لإتاحة مرونة أكبر في تجميع

معلومات الشبكة .تدعم برمجيات الزبائن من Argus طيفاً واسعاً من التطبيقات كالتصنيف و التجميع و الأرشفة و توليد التقارير.

يتألف Argus من جزئين منفصلين :مجمع رئيسي Master Collector يقوم بقراءة حزم البيانات من الشبكة وبرنامج زبون client يتصل بهذا المجمع الرئيسي لعرض إحصاءات استخدام الشبكة .يعمل Argus ضمن أنظمة التشغيل BSD ، GNU/Linux و معظم أنظمة التشغيل Unix الأخرى.

لا تقوم أدوات تحليل الأنماط عادة بالتنبيه عند حدوث أية مشاكل ضمن الشبكة، لذلك ينصح باستخدام أداة لمراقبة الشبكة مثل Nagios لهذا الغرض .

3-7-4 أدوات فحص انتاجية الشبكة Throughput Testing

ما هي السرعة القصوى لنقل البيانات ضمن الشبكة؟ ما هي الإستطاعة الفعلية الممكن تحصيلها في وصلة معينة؟ يمكن الحصول على تقدير لا بأس به لاستطاعة نقل البيانات ضمن الشبكة عبر التحميل الزائد للوصلة بالبيانات وقياس الزمن الذي ستستغرقه في نقل هذه البيانات.

توفر بعض مواقع الإنترنت خدمات قياس سرعة الوصلة (مثل *http://www.dslreports.com/stest* أو *http://speedtest.net*) لكن دقة هذه الخدمات تتناقص بشكل كبير مع ازياد البعد عن مصدر القياس.

والأسوأ من ذلك أن هذه المواقع لن تمكن من قياس سرعة وصلة معينة ضمن الشبكة لأنها قادرة فقط على قياس سرعة الوصلة التي تربط الشبكة بالإنترنت .

فيما يلي مثال عن الأدوات التي تساعد على إجراء قياسات السرعة والإستطاعة ضمن الشبكة المحلية.

- **Bing** *http://fgouget.free.fr/bing/index-en.shtml*

تقوم هذه الأداة عوضاً عن التحميل الزائد للوصلة بالبيانات ومراقبة الزمن اللازم لنقلها بالكامل بمحاولة تقدير الإستطاعة المتاحة لوصلة تربط بين نقطتين من خلال تحليل زمن رحلة الذهاب والإياب لحزم ICMP مختلفة الأحجام .لا يمكن مقارنة دقة هذا الأسلوب مع تجربة التحميل الزائد للشبكة إلا أنه يوفر تقديرات جيدة دون الحاجة إلى إرسال كميات كبيرة من البيانات.

يمكن لأداة bing تقدير استطاعة الشبكات الكبيرة ومحاولة تخمين استطاعة الوصلات الخارجية دون الحاجة إلى تشغيل برنامج زبون خاص في الطرف المقابل نظراً لاستخدام هذه الشبكات لطلبات ICMP بشكل دوري .تمتاز هذه الأداة باستهلاكها المنخفض لعرض الحزمة مما يتيح الحصول على فكرة تقريبية عن أداء الشبكة دون الحاجة إلى إغراق الشبكة بالبيانات لمجرد قياس أدائها.

3-7-5 أدوات المراقبة في الزمن الحقيقي Realtime

يعتبر اكتشاف محاولات التسلل إلى الشبكة أو تعطل أجزاء معينة منها أمراً فائق الأهمية للحفاظ على أداء وأمن هذه الشبكة .نظراً لاستحالة مراقبة الشبكة من قبل الفني المختص على مدار الساعة فقد تم تطوير بعض البرمجيات التي ستتولى هذه المهمة لمتابعة وضعية الشبكة باستمرار و تنبيه الفني المسؤول عند حدوث أية مشاكل .

فيما يلي بعض البرمجيات مفتوحة المصدر التي قد تعين على القيام بهذه المهمة.

- **Snort** *http://www.snort.org*

وهو برنامج لتحسس الشبكة sniffer وتوليد السجلات يمكن استخدامه كنظام مبسط لاكتشاف المتسللين .يتميز هذا البرنامج بقدرته على الإحتفاظ بسجلات تفصيلية بناء على قواعد محددة كما يمكنه القيام بتحليل البروتوكولات و البحث ضمن المحتويات و إيجاد حزم البيانات المتطابقة .يمكن استثمار هذا البرنامج لاكتشاف الكثير من الهجمات و التهديدات كهجمات مسح البوابات و هجمات النصوص البرمجية CGI و الإستعلام عن حزم SMB و محاولات تحديد نوعية نظام التشغيل OS fingerprinting و غيرها من الأنشطة المشبوهة ضمن الشبكة .يتمتع Snort أيضاً بقدرته على تنبيه مدير الشبكة عن أية مشاكل أثناء حدوثها باستخدام عدة وسائل للإتصال.
لا يعتبر تثبيت و تشغيل Snort أمراً هيناً و قد تحتاج تبعاً لحجم البيانات المنقولة عبر الشبكة إلى حاسوب متطور مخصص لأغراض المراقبة .لكن Snort و لحسن الحظ موثق بشكل ممتاز و يتمتع بمجتمع نشط من المطورين و المستخدمين .يتيح تطبيق مجموعة متكاملة من القواعد في برنامج Snort تحديد الأنشطة غير المتوقعة ضمن الشبكة و التي قد تتسبب في إضعاف أدائها.

- **Zabbix** http://www.zabbix.org/

و هي أداة مفتوحة المصدر لمراقبة الشبكة بشكل مستمر يمكن تصنيفها في موقع وسيط بين Nagios و Cacti . تستخدم هذه الأداة قاعدة البيانات MySQL لتخزين المعلومات و تحتوي على حزمة خاصة لتوليد الرسوم البيانية وتقوم بجميع المهام المتوقعة من برنامج متطور للمراقبة المستمرة (كميزات طلب المعلومات عبر بروتوكول إدارة الشبكة البسيط SNMP و التنبيه الفوري عن المشاكل).

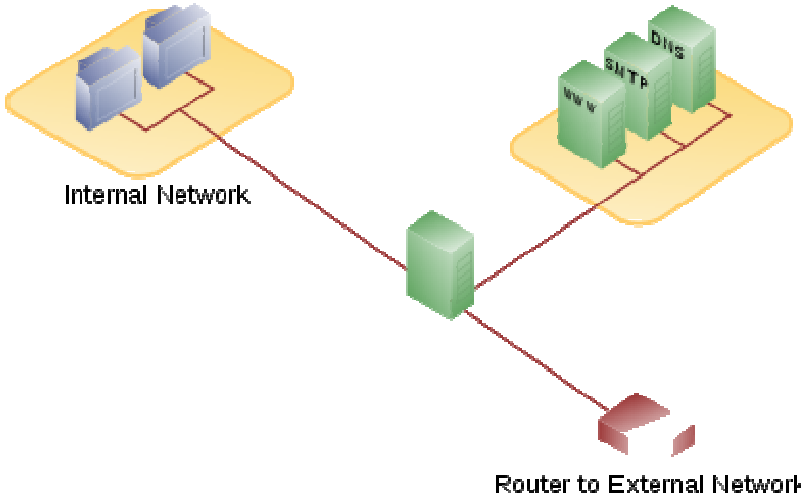
الفصل الرابع

بنية الشبكة

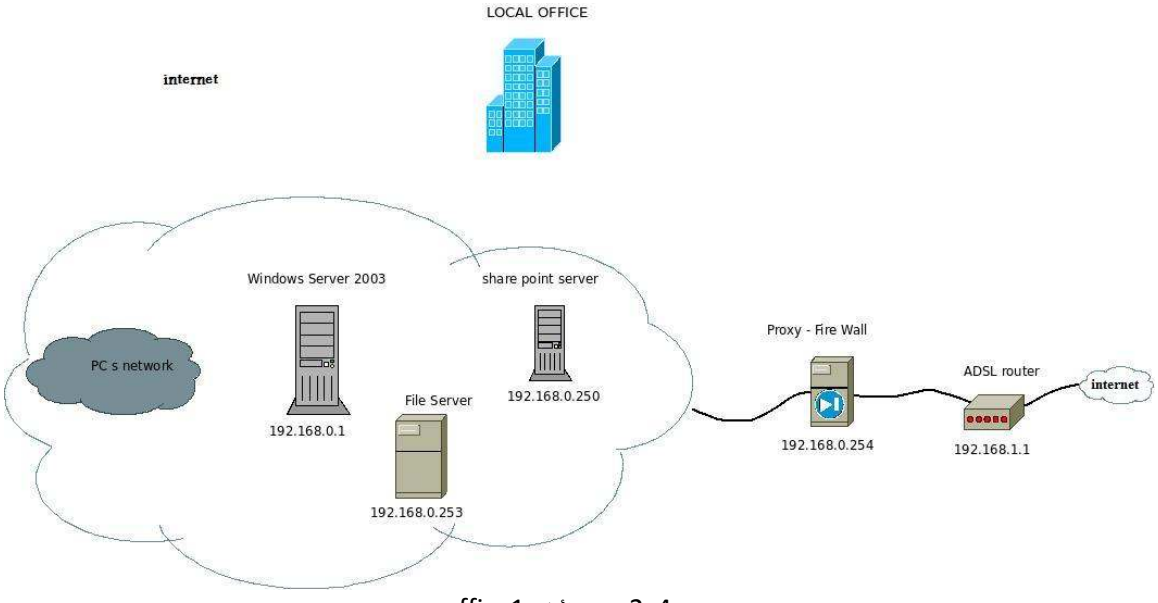
4-1 بنية الشبكة :

تتألف الشركة من قسمين في مكانين مختلفين ،يتصلان مع بعضهما عبر وصلة ADSL ،كما تتصل الشبكة المحلية مع الشبكة الخارجية عبر موجه .

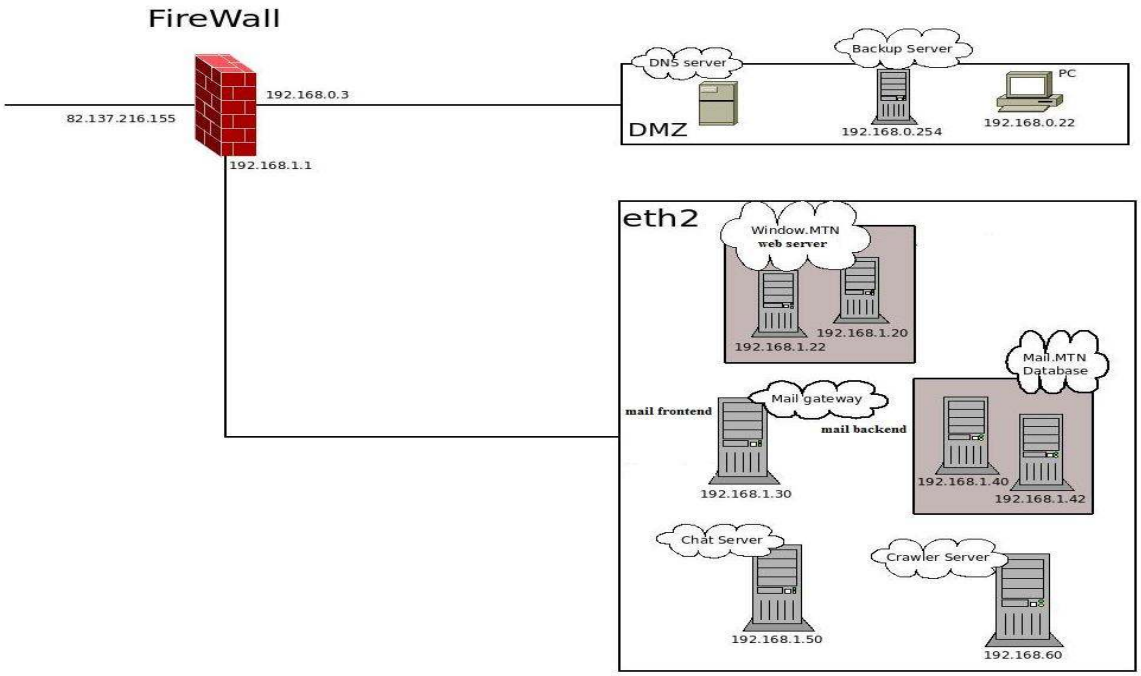
نضع المخدمات التي يمكن الوصول إليها من خارج الشبكة ضمن منطقة منزوعة السلاح DMZ ،و تكون مفصولة عن الشبكة الداخلية عبر جدار ناري Firewall يحميها من الداخل و الخارج. و توضح الأشكال التالية بنية الشبكة :



الشكل 4-1 بنية الشبكة



الشكل4-2 القسم الأول office1



الشكل 4-3 القسم الثاني office2

و الآن سنقدم دراسة بسيطة عن كل مخدم من هذه المخدمات ،حتى نعرف عمله ،و مدى أهميته ،و كيفية مراقبته ،و ما هي الوسطاء التي يجب مراقبتها ضمنه.

4-2 تحليل بنية الشبكة :

- مخدم **Crawler**

هو برنامج بسيط نسبيا أو سكريبت يقوم بمسح منتظم لصفحات الأنترنت ويقوم بإنشاء دليل للبيانات التي يبحث عنها ، هناك تسمية أخرى ل web crawler وهي web spider ،web robot ،automatic indexer .

أهم استخدامات web crawler مرتبط بمحرك البحث حيث يستخدمه محرك البحث لجمع المعلومات من صفحات الأنترنت، عندما يقوم ال crawler بزيارة صفحة فإنه يقرأ النصوص غير المشفرة و الإرتباطات بالإضافة إلى كل الأعلام tags في الصفحة ،و بالتالي باستخدام المعلومات المجمعة من ال crawler يستطيع محرك البحث تحديد مضمون الصفحة ويقوم بفهرسة البيانات في قاعدة معطيات خاصة به.

ليست محركات البحث وحدها من يستخدم ال crawler بل الباحث في المجالات اللغوية أيضا حيث يستخدم في تحليل الملفات النصية ،يتم من خلاله التنقيب عن الكلمات الشائعة في الأنترنت .و بالتالي يمكن القول أنه يستخدم من قبل أي شخص يبحث عن المعلومات ضمن الأنترنت و يمكن برمجته للقيام بعمليات البحث بشكل دوري مما يمكن الشخص الذي يستخدمه من تحديث قاعدة بياناته بشكل أتوماتيكي (و هذا استخدامه في مشروعنا).

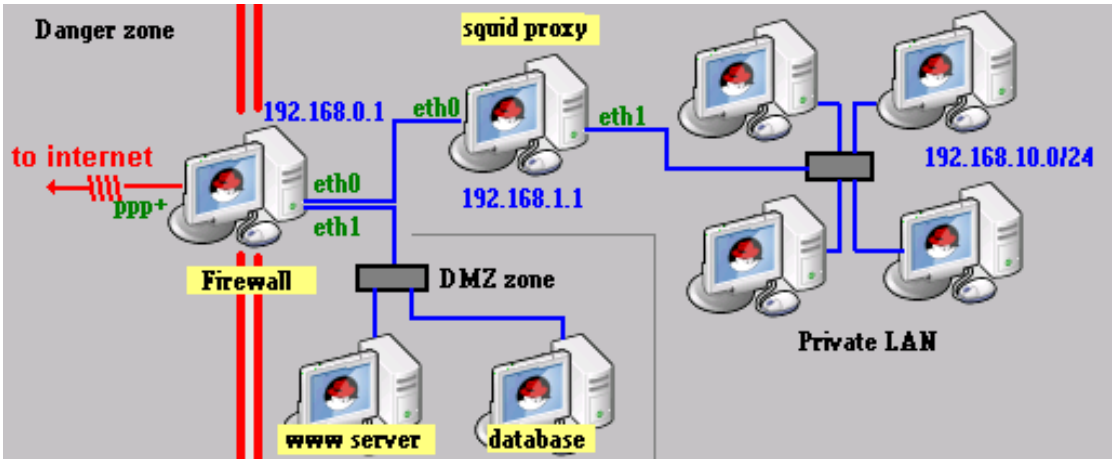
- **الجدار الناري Firewall**

الجدار الناري أو جدار الحماية أو Firewall هو تركيبة من الأجهزة و البرامج التي توفر نظام آمن، تُستخدم عادًة لمنع الوصول غير المصرح به من الخارج إلى شبكة اتصال داخلية.

كما يمكن أن يكون على هيئة جهاز متكامل أو برنامج يتم تحميله إلى الحاسوب الآلي بمواصفات جيدة،وظيفته حماية شبكات الحاسوب الآلي من الاختراقات الخارجية، أي أنه يكون كالجدار الحاجز بين شبكة الحاسوب الآلي الداخلية و شبكة الإنترنت، وظيفته الرئيسية مراقبة كل البيانات الداخلة و الخارجة من الشبكة فهي توفر نظام آمن، أي هو مجموعة نظم تطبق سياسة السيطرة على دخول بين شبكتين.

يُستعمل الجدار الناري بكثرة في الشبكات الداخلية التابعة للشركات ،كما أنه يُستعمل في الشبكات التابعة للمترل أو المدرسة ،الجدار الناري يسمح للمستخدم بإرسال طلباته إلى الإنترنت ،و لكنه لا يسمح للبيانات بالمرور إلى المستخدم من الإنترنت ،ميزة التنقيح الموجودة في المخدم الوكيل يسمح لمسئولي الشبكة بمنع مرور البيانات من قبل مواقع ممنوعة.

بصورة تقنية ،فإن الجدار الناري يختلف عن المخدم الوكيل، فكثيرا ما يقوم مسئولي الشبكة بترتيب و تشغيل عتاد الجدار الناري بصورة منفصلة عن عتاد المخدم الوكيل ،مخدمات الوكلاء التي نُظمت على أساس إنها أجهزة خروج Gateway Devices لديها أكثر من بطاقة شبكية واحدة لدخول الإنترنت و الخروج منها ،و على ذلك فإن الأمر يصبح أفضل اقتصاديا لو تم إضافة الجدار الناري هناك.



الشكل 4-4 الجدار الناري [14]

البرمجيات المستخدمة : IP Tabels

- **مخدم البريد الإلكتروني Email:**

يعمل وفق البروتوكولات التالية :

بروتوكول نقل البريد البسيط SMTP: (Simple Mail Transfer Protocol)

يستخدم لتناقل الرسائل بين مخدميّ بريد إلكتروني. وذلك باستعماله من قبل برامج البريد الموجودة على الحاسب في إرسال الرسائل إلى المخدم.

وهو بروتوكول بسيط جداً, يقوم بتوصيل الرسائل إلى مستقبل أو أكثر وفور توصيل الرسالة لا يمكن استدعاؤها أو إلغاؤها, كما أنها تحذف من المخدم المرسل حالما تصل.

يعمل بروتوكول SMTP وفق مبدأ "Push", والذي يعني أن الاتصال يبدأ من قبل المخدم المرسل وليس المستقبل. الأمر الذي يجعله غير مناسب لتلقي الرسائل من الحواسيب الشخصية والتي يصعب ضمان بقائها قيد التشغيل طوال الوقت.

تخزن الرسائل المستقبلة محليّاً, لتتم استعادتها لاحقاً من نظام الملفات المحلي من قبل برنامج البريد المستخدم. ففي حالة كان ذلك البرنامج هو الـ Webmail, فإنه يتم ترجمة الرسائل إلى صيغة HTML لتترك المهمة بعد ذلك للمتصفح.

ولا بد من ملاحظة أن SMTP هو البروتوكول الوحيد المستخدم لتبادل الرسائل بين المخدمات, أما آلية تخزينها فتختلف من نظام إلى آخر.

بروتوكول الـ POP: (Post Office Protocol)

يعتبر بروتوكولاً لاستقبال الرسائل من مخدم البريد الإلكتروني, حيث يستخدم من قبل معظم الحواسيب الشخصية في الحصول على الرسالة من المخدم.

ويسمح هذا البروتوكول بتحميل كل الرسائل في صندوق الوارد دفعة واحدة. حيث يعمل وفق مبدأ "PULL", والذي يعني أنه يتم طلب الاتصال من قبل الحاسب المستقبل دون المرسل. وتقوم الحواسيب الزبونة التي تعتمد على بروتوكول الـ POP3 بهذه العملية تلقائياً في وقت مسبق.

عندما يفتح الحساب البريدي للوصول إلى صندوق بريد POP3, فإن المخدم البريدي يقوم بالاتصال بمخدم الـ POP3 تماماً كما يفعل أي تطبيق حاسوبي آخر. بعدها يتم نسخ الرسائل إلى صندوق الوارد ليتم قراءتها عن طريق المتصفح. ونظراً إلى أن الـ POP3 يقوم بتحميل نسخة من كافة الرسائل إلى صندوق الوارد, فإنه يمكن الحفاظ على نسخة من الرسائل جميعها على المخدم و الوصول إليها لاحقاً من أي جهاز آخر و دون فقدان أي منها. ولكن السلبية ضرورة تحميل الرسائل جميعها في كل مرة نريد تفقد البريد الأمر الذي قد يستغرق وقتاً مطولاً. فضلاً عن أن معظم أنظمة البريد الالكتروني لا تدرك أياً من الرسائل قد تم تحميلها سابقاً و أيها لم تحمل وبالتالي سوف تتكرر كل الرسائل التي لم تحذف .

بروتوكول الولوج إلى البريد IMAP:

هذا البروتوكول شبيه بسابقه من حيث العمليات التي يقوم بها و لكنه يتيح أريحية أكبر في الرسائل المراد تحميلها. حيث يقوم مبدئياً بتحميل ترويسات تلك الرسائل لتعطي معلومات عن المرسل و عنوان الرسالة ،و بعدها يتم اختيار الرسائل المراد قراءتها فقط وتحميلها. كما يمكن حذف الرسائل بشكل إفرادي من المخدم.

يتألف مخدم البريد الالكتروني من جزأين :

الواجهة الأمامية : Frontend و هي واجهة التخاطب مع المستخدم ،حيث يقوم بإرسال الرسائل ،كما يقوم باستقبال الرسائل و تخزينها في DataBase (في Backend)،و عندما يريد المستخدم قراءة الرسائل ،فإنه يقوم باسترجاع الرسائل من Backend عن طريق أحد البروتوكولين IMAP أو POP.

الواجهة الخلفية : Backend و هي تمثل قاعدة معطيات (DataBase) لتخزين الرسائل.

نشغل على الواجهة الأمامية البروتوكولات SMTP (للإرسال) و IMAP و POP (للاستقبال) ،بينما نشغل على الواجهة الخلفية POP و IMAP فقط.

البرمجيات المستخدمة :

Mail Getway (Frontend): Courier (IMAP & POP)+ postfix (SMTP)

Mail.MTN.DataBase (Backend): Courier mail Server

- **مخدم DHCP**:

عادة وعند إعداد أي شبكة صغيرة كانت أو كبيرة هناك أمور لا بد من تحقيقها و هي أن يكون لكل جهاز عنوان فريد خاص به IP و أن يتمكن كل جهاز من التعرف على أقرب DNS في حال وجوده و أن يعرف عنوان البوابة gateway أو الموجه router الذي يوفر الأتصال بالأنترنت بالإضافة إلى التعرف على المجال الذي ينتمي له الجهاز في حال توفره،من الممكن إدخال المعلومات في كل جهاز بشكل يدوي و لكن ذلك مرهق جدا في حال الشبكات الكبيرة ، وهنا يأتي دور DHCP (Dynamic Host Configuration Protocol) حيث تتلخص مهمته في إعطاء كل جهاز عنوان IP خاص به و إدخال باقي المعلومات التي يحتاجها تلقائيا دون تدخل من المدير و دون المرور على كل جهاز على حدا فيكفي أن تقوم بإعداد مخدم DHCP ليقوم تلقائيا بإعطاء كل جهاز ينضم إلى الشبكة كافة المعلومات التي يحتاج لها.

البرمجيات المستخدمة : DHCP Server

- **مخدم الملفات FTP:**

معظم عمليات الإنترنت هي إرسال واستلام الملفات ،أو بمعنى أبسط هي قراءة و كتابة الملفات .و من هنا كانت الفكرة الأساسية لبروتوكول نقل الملفات (FTP) هو نقل الملفات من جهة إلى جهة أخرى .

عند إجراء اتصال بين حاسوبين أي أحدهما يرسل ملفا للأخر فلا بد من لغة اتصال بينهما، لتبليغ كل حاسوب بعض المعلومات عن الملفات المنقولة مثل حجم الملف ومحتويات الملف واسم الملف...الخ ،وأيضا لتبليغ كل حاسوب ببداية الإرسال ،أو التوقف اللحظي أثناء الإرسال أو إعادة جزء من الملف مرة أخرى ، أو إتمام عملية الاستلام عند الطرف الأخر وغيرها .والذي يدير جميع الموضوعات المتعلقة بنقل الملفات هو بروتوكول نقل الملفات(FTP) ،و هذا البروتوكول عبارة عن تطبيق يعمل في الطبقة الرابعة من طبقات (tcp/ip) و هذه الطبقة تدعى بطبقة التطبيقات و يقوم هذا البروتوكول عادة بنقل نسخة من الملفات إلى الجهاز الهدف مع ترك نسخة منها في الجهاز المصدر .و قد صمم هذا البرتوكول لكي يعمل بين أجهزة مختلفة في النوع . كذلك ليعمل بين جهازين يعملان بنظامي تشغليين مختلفين مثلاً يمكن لجهاز يستخدم نظام الويندوز و جهاز آخر يعمل بنظام Linux أن يتم الربط بينهما دون التأثير على عمل البروتوكول .و بروتوكول نقل الملفات يستطيع أن ينقل فقط أنو اع محدودة من الملفات (binary, ASCII) و لكي يستطيع مستخدم ما استخدام هذا البرتوكول لا بد أن يكون له حساب على المخدم وهذا الحساب يكون باسم مستخدم خاص وكذلك كلمة مرور .

البرمجيات المستخدمة :

Samba & WinBind: يسمح للأجهزة التي تعمل وفق نظام ويندوز بالاتصال مع Linux Server.

- **مخدم الأسماء DNS:**

تقنية الـ DNS تشبه إلى حد كبير دليل الهاتف، حيث يمكننا في دليل الهاتف من خلال معرفة اسم الشخص الحصول على رقمه من أجل القيام بعملية الاتصال، اسم الشخص في الدليل يقابل في الشبكة الاسم المعرف للجهاز المراد الاتصال به عبر الشبكة و رقمه يقابل عنوان الـ IP الموافق للاسم المعرف للجهاز،عند الاتصال بحاسوب آخر على الشبكة فمن الأفضل استعمال اسم هذا الحاسوب بدلاً من استعمال عنوان IP له، عندها فإن الجهاز المتصل يقوم بالاتصال مع مخدم DNS الذي يقوم بعملية إلحاق عنوان IP الموافق للاسم المعرف للجهاز المطلوب الاتصال به، حيث أن عنوان الـ IP ضروري من أجل تأسيس عملية الاتصال عبر الشبكة.

البرمجيات المستخدمة: BIND9

- **المخدم الوكيل Proxy Server** :

يعتبر حلاً من الحلول العديده المتاحة للمشاكل التي تواجه الإتصال من قبل الشبكات الداخلية أو المحدودة أو الشبكات المتصلة بالانترنت. إن المخدم الوكيل هو البرنامج الذي يتعامل مع النقل ويقوم بمراقبة التحركات(traffic) ما بين الإنترنت و الشبكة.

بدلا من إتصال الشبكات بالانترنت مباشرة، يذهب كلا الاتصالين الى المخدم الوكيل .المخدم الوكيل يوهم المستخدم أنه يتعامل مع مخدم الوب الحقيقي الذي طلبه ، كما يوهم المخدم أنه المستخدم الحقيقي ،لذلك فإنه يعمل كمخدم (بالنسبة للمستخدم) و زبون (بالنسبة للمخدم) ،يعتمد ذلك على طريقة الاتصال.
مخدم الوكيل يعمل على تمرير الطلبات من المستخدم الى شبكة الانترنت و بالعكس. لأنه يعمل على التفحص لهذه الطلبات التي يتم معالجتها،و يمكنه التحكم بعمل المستخدمين. على حسب التعليمات الخاصة بالسياسة الأمنية،فإما يتم الموافقة على طلبات الزبون و يتم ارسالها،أو من الممكن أن يتم منعها .كمثال: عند تصفح الانترنت ، نتصفح و نستقبل الصفحات المرغوبة، بعض المواقع تكون محظورة أو ممنوعة الدخول لأسباب معينة ، وهذا من يتم من خلال المخدم الوكيل.

التخبئة في المخدم الوكيل : Proxy Server Caching

يمكن للعديد من مخدمات الوكلاء تخزين البيانات محليا،و هذه طريقة مفيدة إذا كان هناك عدد من الزبائن يطلبون نفس هذه البيانات. باستخدام تقنية التخبئة (Caching) ،يمكن تخديم الزبائن بسرعة أكبر بالإضافة إلى تخفيف حركة النقل إلى الشبكة الخارجية (الانترنت).

نميز نوعين للتخبئة Caching و هما:

التخبئة الفعالة Active Caching:
يقوم المخدم الوكيل بجلب البيانات و تخزينها محليا ،و ذلك عند التخمين بأنه سيتم طلب البيانات في وقت قريب.

التخبئة السلبية Passive Caching:
ينتظر المخدم الوكيل طلب الزبون ليستضيف البيانات، وبعدها يقرر هل سيتم عمل caching لهذه البيانات أم لا.

البرمجيات المستخدمة: Squid

- **مخدم الويب Web Server**:

و هو المخدم الذي يستضيف المواقع الالكترونية.

برمجيات مخدم الويب هي برامج يتم تنصيبها على جهاز المخدم، سواء كان نظام تشغيل المخدم هو Unix أو NT أو غير ذلك. وهناك برنامج ضمن برمجيات مخدم الويب يدعى HTTP Daemon، مهمته قبول وتنفيذ الأوامر .

بكلام آخر، عندما يقوم المستخدم بالضغط على أحد الروابط Hyperlink الموجودة في صفحة الويب، يتم إرسال الطلب إلى مخدم الويب للبحث عن موقع هذا الرابط ، أما إرسال المعطيات إلى جهاز المستخدم فهي مهمة HTTP Daemon التي تم تطويرها ودمجها داخل برمجيات مخدمات الويب المتوفرة حالياً .

البرمجيات المستخدمة : Apache Server

- **مخدم المحادثة Chat Server:**

وهو المخدم الذي يقوم بإدارة غرف المحادثة للمستخدمين ،و عندما يقوم أحد المستخدمين بإرسال رسالة لكل المستخدمين يقوم هذا المخدم بإذاعة هذه الرسالة للجميع فالوظيفة الأساسية لهذا النوع من المخدمات هو القراءة و الإذاعة و الإستجابة لغرف المحادثة و تأمين خدمات التواصل في الزمن الحقيقي.

يمكن تأسيس هذا المخدم من خلال برامج لإعداد غرف المحادثة ، من صفات هذا المخدم أنه مستقر بشكل كبير و عمليات الصيانة له قليلة ،فعند الإنتهاء من عملية إعداده لا نحتاج إلى العودة إليه لمدة ،فلن يكون هناك مشاكل لا في الذاكرة و لن يكون هناك أي انهيار للمخدم،و سبب هذه الوثوقية العالية من استقرار هذا المخدم هو اختباره من قبل الملايين من المستخدمين منذ أن تم إنشاؤه.

البرمجيات المستخدمة: Open Fire

4-3 ما الذي ينبغي مراقبته؟

يمكن اختيار أي حدث نريد مراقبته ضمن الشبكة و إظهاره بيانياً مع مرور الزمن .لكن اختلاف الشبكات عن بعضها البعض يفرض ضرورة تحديد المعلومات الهامة التي تجب متابعتها لقياس أداء الشبكة.

فيما يلي بعض المؤشرات التي يجب متابعتها:

إحصائيات المبدل:

- إستهلاك عرض الحزمة لكل منفذ
- إستهلاك عرض الحزمة لكل بروتوكول
- إستهلاك عرض الحزمة لكل عنوان MAC
- النسبة المئوية لحزم البث broadcast مقارنة بجميع حزم البيانات
- خسارة حزم البيانات ونسبة الخطأ

إحصائيات الإنترنت :

- إستهلاك عرض حزمة الإنترنت لكل جهاز و بروتوكول
- عدد الطلبات الواردة إلى الذاكرة المؤقتة للمخدم الوكيل Proxy server cache hit
- طلبات ترجمة أسماء النطاق DNS
- عدد رسائل البريد الإلكتروني الصادرة (الرسائل التجاريةspam ، رسائل البريد الإلكتروني المرتجعة)
- حجم رتل البريد الإلكتروني الصادر
- وثوقية الخدمات الحساسة (مخدمات الوب، البريد الإلكتروني، إلخ)
- زمن الإستعلام Ping time ونسب خسارة البيانات المرسلة إلى مزود خدمة الإنترنت
- وضعية الوصلات الإحتياطية

إحصائيات صحة النظام :

- إستهلاك الذاكرة
- إستهلاك ملف التبادل swap file
- عدد المهام و المهام الهامدة zombie processes
- تحميل النظام system load
- فرق الكمون و مستوى تحميل وحدة عدم إنقطاع التيار الكهربائي UPS
- درجة الحرارة و سرعة المروحة و فروق الكمون في النظام
- وضعية SMART للقرص الصلب
- وضعية الأقراص الصلبة المكررة RAID array status

سنضطر مع ازدياد تعقيد الشبكة إلى اختيار المزيد من المؤشرات الأساسية على أدائها والتي يتوجب مراقبتها باستمرار ينبغي أيضاً مراقبة توفر أي مورد في حال كان تعطل هذا المورد سيؤثر على مستخدمي الشبكة.

الفصل الخامس

تحليل النظام

5-1 منهجية العمل :

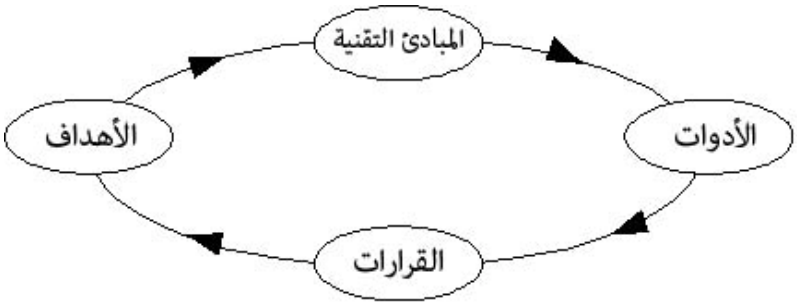
من الأخطاء الشائعة عند مزوّدي خدمات الإنترنت ISPs تبنّي أسلوبٍ يعتمد على الأدوات tool-centric في اتخاذ القرار. على سبيل المثال، عند تركيب أداة إدارةٍ معينّةٍ في نظامٍ لإدارة الشبكة يتم اتخّاذ جميع القرارات بناء على إمكانيّات هذه الأداة عوضاً عن أهداف و أولويّات مزوّد الخدمة.

نعتمد ضمن هذا المشروع أسلوباً مبنيّاً على الأهداف goal-centric في إدارة الشبكة. حيث نقدم (بعكس الأسلوب المعتمد على الأدوات) منهجيّةً لإدارة الشبكة تبدأ بتحديد أهدافٍ واضحةٍ لإيجاد الأدوات الصحيحة.

5-1-1 الأهداف في مقابل مراقبة البيانات :

تعتبر الخطوة الأولى والأكثر أهميّةً والتي يجب على أيّ مزوّدٍ لخدمات الإتصالات / الإنترنت اتخاذها قبل البدء بتركيب أيّ نوعٍ من أدوات المراقبة تحديد الأهداف التي يريد تحقيقها والتحديّات التي يواجهها.

يعتبر تحديد (1) **الهدف** أمراً أساسيّاً للتفكير (2)**بالمبادئ التقنيّة** المطلوبة للحصول على المعلومات الضروريّة من النظام. يمكّننا تحديد المبادئ التقنيّة من اختيار، تصميم وتركيب (3) **الأدوات** اللازمة. توفّر المعلومات التي ستقدّمها هذه الأدوات معرفةً إضافيّةً لإتخاذ (4) **القرارات** الصائبة.



الشكل 5-1 المنهجيّة المعتمدة على الأهداف لمراقبة (إدارة) الشبكة [18]

و كنا قد ذكرنا الأهداف المراد تحقيقها من خلال تصميم و تنفيذ نظام الإدارة و نعود لنذكر بها :

- الحفاظ على جاهزية الشبكة.
- تأمين جودة الخدمة ،و استمرارية العمل
- تسهيل صيانة الشبكة
- الصيانة الوقائية
- التحكم في التكلفة

5-2 المتطلبات الوظيفية :

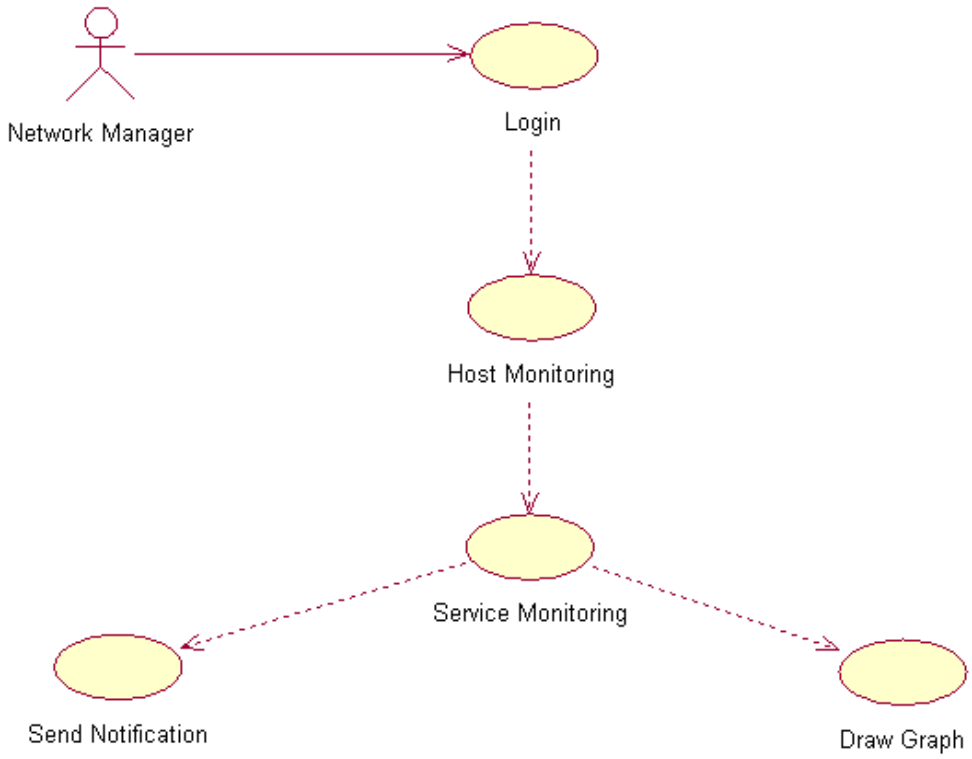
5-2-1 حالات الاستخدام :

1- تسجيل دخول login
2- مراقبة مضيف Host Monitoring
3- مراقبة خدمة Service Monitoring
4- رسم مخطط بياني Graph
5- إرسال تنبيه Notification

مستخدمو النظام :

لدينا مستخدم واحد و هو مدير الشبكة.

5-2-2 مخطط حالات الاستخدام :



الشكل 5-1 مخطط الحالات

5-2-3 توصيف حالات الاستخدام :

1- تسجيل الدخول : Login

Use case name	تسجيل الدخول
Actors	مدير الشبكةNagios
Preconditions	
Main flow of events	1- يطلب المدير عنوان واجهة الويب لنظام المراقبة URL . 2- يطلب النظام من المدير إدخال اسم المستخدم و كلمة المرور. 3- يدخل المدير اسم المستخدم و كلمة المرور. 4- يتحقق النظام من صحة المعلومات المدخلة. 5- يتم تسجيل الدخول إلى النظام.
Post conditions	يقوم النظام بعرض واجهة رسومية تحوي قائمة بالمضيفين الخاضعين للمراقبة و الخدمات لكل مضيف.
Alternatives	4-1 في حال كانت المعلومات خاطئة : يطلب النظام إعادة إدخال المعلومات (اسم المستخدم و كلمة المرور)
Exceptions	4-2 في حال الخطأ ثلاث مرات : يتم حجب الدخول لمدة خمس دقائق و إرسال تنبيه لمدير الشبكة

2- مراقبة خدمة : Service Monitoring

يتم مراقبة خدمة ما تابعة لمضيف . حيث نميز عدة حالات للخدمة .

Use case name	مراقبة خدمة
Actors	مدير الشبكة
Preconditions	تم تسجيل الدخول تم تحديد المضيف
Main flow of events	1- يطلب المدير من النظام إظهار حالة خدمة ما. 2- يطلب النظام من المدير تحديد الخدمة . 3- يحدد المدير الخدمة . 4- يحصل النظام على المعلومات المتعلقة بالخدمة من ملف تعريف الخدمات.

	5- يقوم النظام بتنفيذ الإجراء Script الخاص بفحص الخدمة (في حال مراقبة الجهاز المحلي) . 6- يرد النظام نتيجة تنفيذ الإجراء. 7- يقارن النظام نتيجة التنفيذ بالحالات المحددة ضمن الإعدادات 8- يعرض النظام نتيجة الفحص و حالة الخدمة .
Post conditions	عرض حالة الخدمة و بعض المعلومات حول الخدمة.
Alternatives	4-1 في حال كانت الخدمة تابعة لمضيف بعيد : يقوم النظام بالاتصال بالزبون client ضمن المضيف البعيد و يطلب منه مراقبة الخدمة. يقوم الزبون بتنفيذ إجراء الفحص. يعيد النتيجة إلى مخدم نظام المراقبة.
Exceptions	4-1 في حال عطل في الشبكة : يظهر النظام رسالة بأنه غير قادر على الاتصال مع الجهاز البعيد. 5-2 النظام لم يستطيع تفسير النتيجة : يظهر رسالة بخصوص ذلك و يضع حالة الخدمة unknown

3- مراقبة مضيف : Host Monitoring

يرتبط بكل مضيف مجموعة من الخدمات التي يمكن مراقبتها ،و التي يتم تحديدها ضمن ملفات الإعدادات. و مراقبة المضيف تعني مراقبة مجموعة الخدمات المرتبطة بهذا المضيف.

بالإضافة إلى مراقبة خدمات المضيف ،نراقب المضيف بشكل عام فقد يكون خارج نطاق العمل Down.

Use case name	مراقبة مضيف
Actors	مدير الشبكة
Preconditions	تم تسجيل الدخول
Main flow of events	1- يطلب المدير من النظام إظهار حالة مضيف. 2- يطلب النظام من المدير تحديد المضيف. 3- يحدد المدير المضيف. 4- يحصّل النظام الخدمات المعرفة و المرتبطة بهذا المضيف . 5- يقوم بمراقبة كل خدمة منها (تنفيذ حالة الاستخدام السابقة لكل خدمة) 6- يعرض النظام حالة المضيف و حالة كل خدمة مرتبطة به.

Post conditions	يقوم النظام بعرض واجهة رسومية تحوي الخدمات المرتبطة بهذا المضيف و حالة كل منها
Alternatives	
Exceptions	5-1 النظام غير قادر على الاتصال بالمضيف :(ربما لأنه لا يعمل حاليا) يظهر النظام حالة المضيف Down و حالة الخدمات Critical.

4- إرسال تنبيه :

يقوم النظام بمراقبة الخدمات بشكل تلقائي دوريا كل فترة محددة (يتم تحديدها في الإعدادات لكل خدمة) و يحتفظ بمعلومات المراقبة ضمن قاعدة معطيات (أو ملفات) كما يتم تعريف عتبة تنبيه ،و يقوم النظام بتنبيه مدير الشبكة عند تجاوز الخدمة عتبة التنبيه

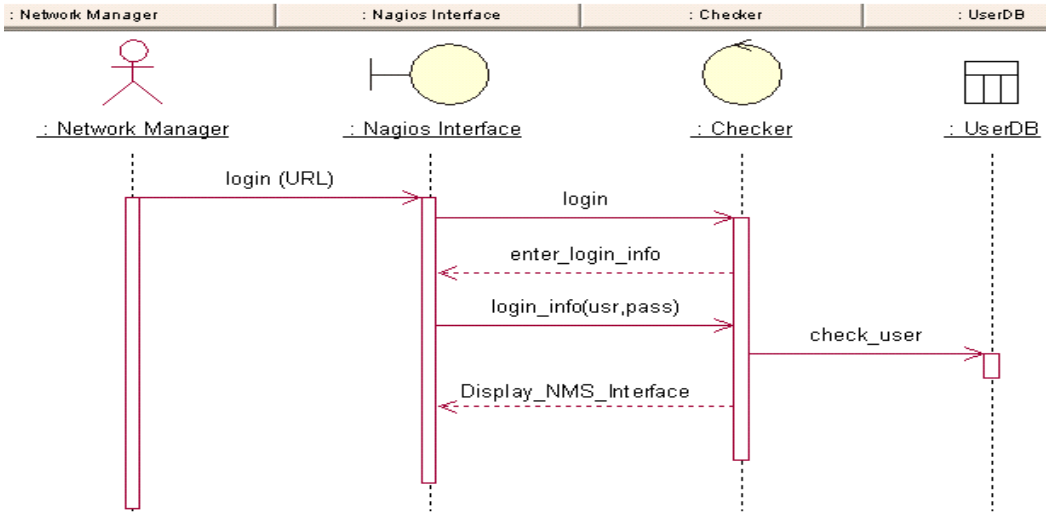
Use case name	إرسال تنبيه
Actors	النظام
Preconditions	
Main flow of events	1- يقوم النظام بمراقبة دورية للخدمات المختلفة. 2- يقارن حالة الخدمة مع عتبة التنبيه (ضمن الإعدادات) 3- في حال تجاوز العتبة :يقوم النظام بتحديد معلومات مدير الشبكة من ملفات الإعداد (ملف Contact). 4- يرسل النظام رسالة تنبيه إلى البريد الالكتروني لمدير الشبكة. 5- يرسل النظام رسالة SMS إلى مدير النظام.
Post conditions	يصل إلى مدير الشبكة رسالة تنبيه تحدد العطل الذي حصل
Alternatives	3-1 يتم إرسال تنبيه عندما تعود الخدمة إلى الحالة الطبيعية. 4-1 ، 5-1 لتقليل رسائل التنبيه : إذا بقيت الخدمة في حالة Critical لفترة معينة (أو عدة مرات فحص) يرسل رسالة تنبيه و ليس مباشرة. في حال إرسال تنبيه و بقيت الخدمة في حالة Critical لا يتم إرسال تنبيه مرة أخرى إلا بعد فترة محددة.
Exceptions	

5 – رسم المخططات البيانية :

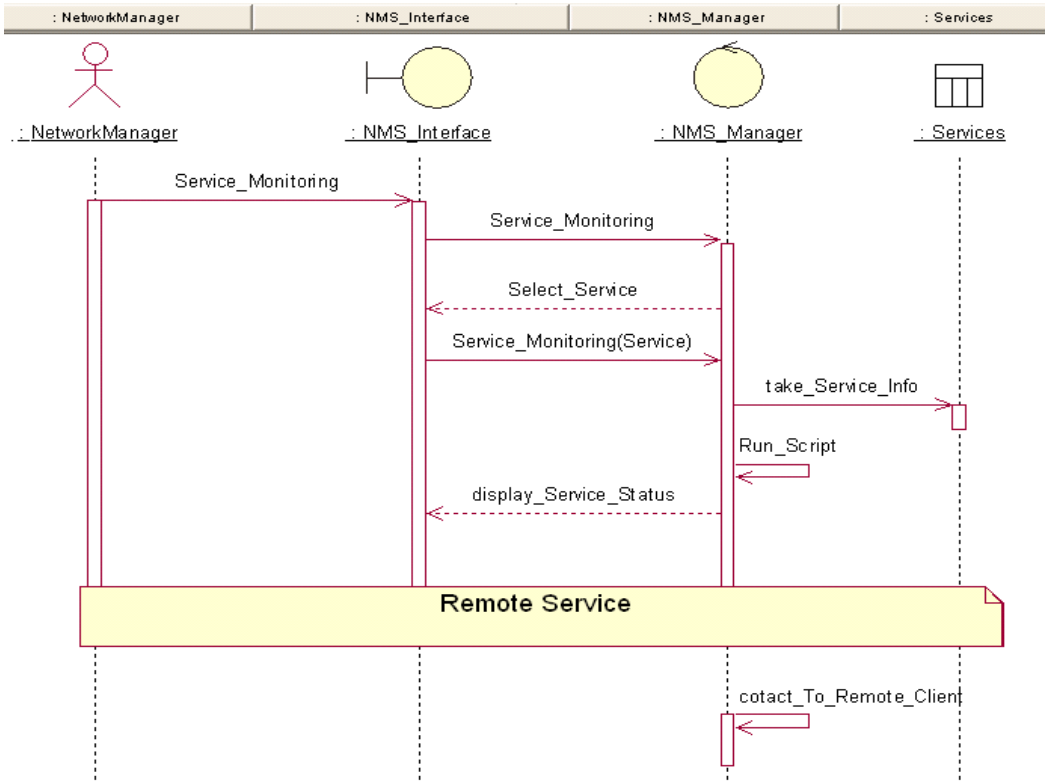
Use case name	رسم المخططات البيانية
Actors	مدير الشبكة
Preconditions	تم تسجيل الدخول تم اختيار المضيف تم اختيار الخدمة
Main flow of events	1- يطلب المدير من النظام رسم المخطط البياني لخدمة ما. 2- يقوم النظام باستخلاص معلومات الخدمة من ملف المعلومات التاريخية History (يحوي جميع معلومات المراقبة). 3- يخزن النظام معلومات الخدمة في ملف. 4- تقوم أداة الرسم بقراءة معلومات الخدمة من الملف. 5- تقوم أداة الرسم بقراءة وسطاء الرسم من ملفات الإعدادات. 6- تقوم أداة الرسم برسم المخطط البياني للخدمة. 7- يقوم النظام بعرض المخطط البياني.
Post conditions	تم عرض المخطط البياني للخدمة
Alternatives	
Exceptions	

5-2-4 مخطط التتالي: Sequence Diagram

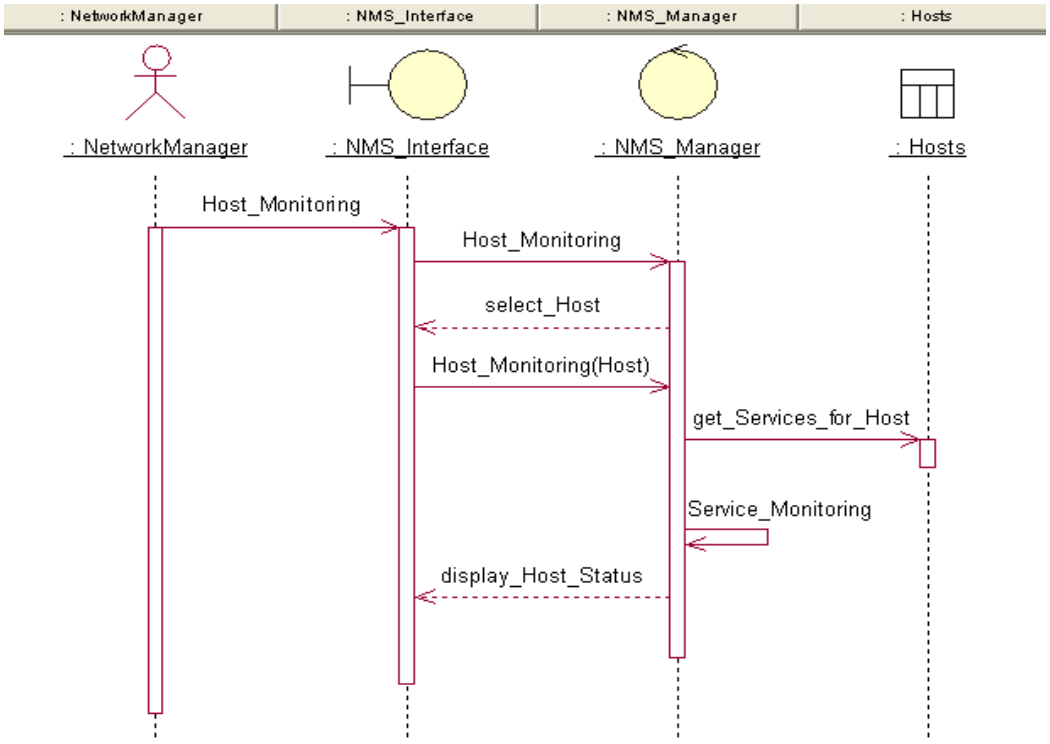
1- تسجيل الدخول : Login



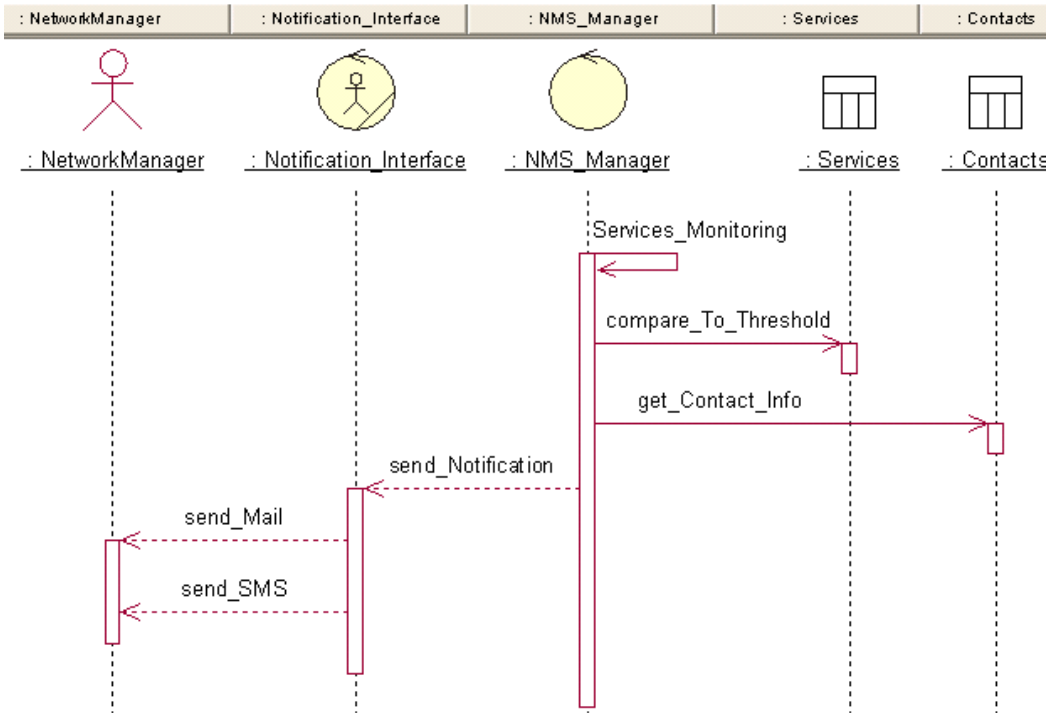
2- مراقبة خدمة : Service Monitoring



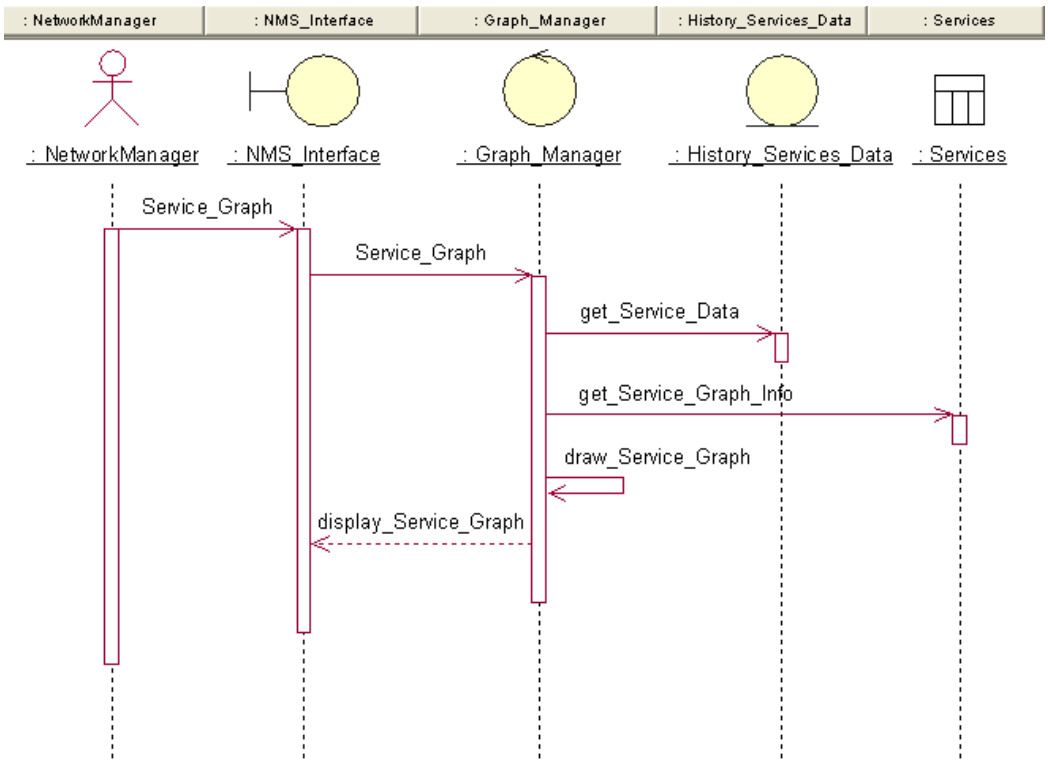
3- مراقبة مضيف : Host Monitoring



4- إرسال تنبيه :



5 – رسم المخططات البيانية :



5-3 المتطلبات غير الوظيفية :

و هي متطلبات إضافية لا تتعلق بمهام النظام ،إنما بطريقة تنفيذ النظام، و لا يؤدي تعطلها إلى توقف النظام، و قد طرحت المؤسسات انطلاقا من حاجاتها مجموعة من المتطلبات غير الوظيفية،منها:

- برامج تعمل في عدة مواقع و فروع و تتكامل مع بعضها البعض .
- برامج سهلة التعامل
- سرعة في التحقيق
- برامج رخيصة الكلفة

1 – الأمن الوظيفي: functional security

قدرة النظام على استيقان Authentication المستخدم ،و عدم السماح إلا بدخول مدير الشبكة (و هو المستخدم الوحيد للنظام).

2 – الوثوقية: Reliability

وثوقية الاتصال : نستخدم في الاتصال عن بعد بروتوكول SSL (Secure Socket Layer) و الذي يحقق عدة خدمات أمنية ،مثل :الاستيقان Authentication و تشفير المعطيات .

3 – تحمّل الخلل : fault tolerance

و هذا يعني عدم توقف النظام في حال حدوث خطأ ،و قد تم تحقيق ذلك من خلال معالجة الحالات المختلفة للأخطاء التي يمكن أن تحصل (مثل الحالات التي لا تمكن فيها النظام من الاتصال بالمضيف البعيد أو لا يستطيع تفسير نتيجة مراقبة الخدمة).

4 – التصعّد: scalability

أي التأقلم مع ازدياد الضغط و إمكانية إضافة آلات وفق الطلب.

5 – البنيان الموجه للخدمة: SOA (Service Oriented Architecture)

أي إمكانية إضافة خدمات جديدة دون إعادة البرمجة أو إيقاف النظام

6 – العمل في الزمن الحقيقي : Realtime

7 – الأداء الجيد : High Performance

8 – كلفة زائدة منخفضة: Low Overhead

أي لا يؤثر نظام المراقبة على الشبكة أو المضيفين و يستهلك مواردها.

الفصل السادس

الأدوات و التقنيات المستخدمة

اختيار بيئة العمل :

إن اختيار بيئة العمل بالنسبة لأي منتج تعتبر عاملاً أساسياً في نجاحه و استمراره، و تتألف بيئة العمل بالنسبة لمشروعنا بشكل أساسي من :نظام التشغيل ،أداة المراقبة ،أدارة رسم المخططات البيانية ،أداة التبيه.
و سنعرض فيما يلي الأدوات و التقنيات التي اعتمدنا عليها في تنفيذ المشروع.

6-1 نظام التشغيل :

يعتبر اختيار نظام تشغيل مناسب أمراً مهماً ،و يؤدي الاختيار الخاطئ إلى إضاعة الوقت و ربما التعرض لانخفاض الأداء و عدم توفر المزايا المطلوبة، و يؤدي ذلك لعدم تحقيق الغرض المطلوب، و لا يوجد عملياً نظام تشغيل يستطيع تحقيق كافة المتطلبات لكن هناك مقاييس رئيسية يمكننا الاعتماد عليها للمقارنة :

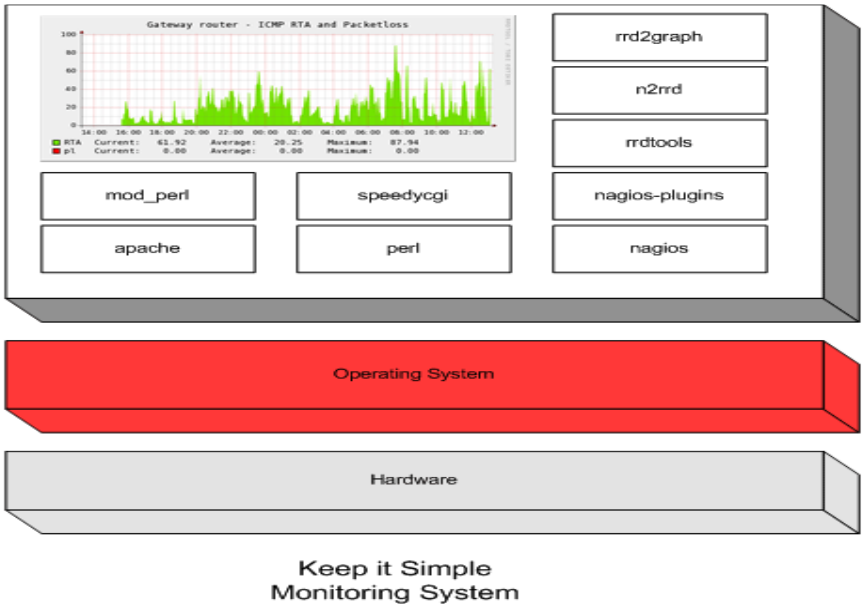
- الدعم العتادي و التقني الذي يقدمه
- الأمن
- الأداء
- سهولة التعامل و الإدارة
- ثبات النظام

وقد اخترنا نظام التشغيل Linux (ubuntu 8.1) و قد وقع اختيارنا عليه بسبب دعمه لمتطلبات مشروعنا (التطوير و البحث) من حيث البيئة بحد ذاتها، بالإضافة إلى وجود ميزات تميّزه عن غيره من حيث السرعة و القوة و الأمن من الفيروسات إلى حد كبير و الوثوقية، و يتمتع لينوكس بدرجة عالية من الحرية في تعديل و تشغيل و توزيع و تطوير أجزاءه ،كما أنه يوفر إمكانيات هائلة تمكننا من التحكم الكامل بكافة الموارد.

6-2 الأداة Nagios:

و هو برنامج يتولى مهام مراقبة الحواسيب والخدمات ضمن الشبكة و تنبيه المدير المسؤول مباشرة عند حدوث أية مشاكل .بمقدور هذا البرنامج إرسال رسائل التنبيه من خلال البريد الإلكتروني أو خدمة الرسائل القصيرة SMS أو تشغيل برنامج معين، كما سيقوم بإرسال هذه الرسائل إلى الشخص المسؤول أو مجموعة الأشخاص المسؤولين تبعاً لطبيعة المشكلة .يعمل Nagios ضمن أنظمة التشغيل BSD و GNU/Linux و يوفر واجهة استخدام تعمل من خلال متصفح الويب لعرض آخر أوضاع النظام.
يتميز برنامج Nagios بمرونته الفائقة و قدرته على مراقبة أي حدث قد يحدث على الشبكة تقريباً .يقوم هذا البرنامج بإجراء الفحوصات عبر تشغيل نصوص برمجية صغيرة بشكل دوري و مقارنة النتائج مع القيم المتوقعة، مما يتيح إجراء فحوصات أكثر تعقيداً من الفحص البسيط للشبكة .باستطاعة الأداة ping على سبيل المثال الاعلام فيما إذا كان الجهاز يعمل بشكل صحيح أم لا، في حين يمكن للأداة nmap الاعلام بأن منفذاً معيناً مازال قادراً على إجابة الطلبات التي سترده، أما Nagios فسيمكن مثلاً من طلب صفحة ويب معينة أو إرسال استعلام إلى قاعدة بيانات و التحقق من أن الرد الواصل خال من أي خطأ.

يمكن لبرنامج Nagios أيضاً التنبيه عند تجاوز استهلاك عرض الحزمة أو ضياع حزم البيانات أو درجة حرارة المخدم أو غيرها من المؤشرات على صحة الشبكة حداً معيناً مما سيعطي تنبيهاً مبكراً للتعامل مع المشاكل.



الشكل 6-1 بنية النظام [6]

لماذا nagios ؟

– القدرة على مراقبة عدد كبير من المخدمات :

من أجل مساعدة أصحاب شركات الإستضافة وتأجير المخدمات على توضيح كيفية مراقبة عدة مخدمات، فهذه معضلة يواجهها أصحاب الشركات على وجه التحديد حينما يكون لديك 50 او 80 او 100 مخدم أو أكثر فكيف سيقوم موظفوك بمراقبة هذا العدد الكبير من المخدمات إلا من خلال هذا البرنامج ومعرفتهم الجيدة بطرق التعامل معه.

– القدرة على مراقبة تجهيزات Windows و Linux و بالتالي يمكن استخدامها في منظومة شبكية تعمل وفق عدة أنظمة تشغيل.

– هي أداة مفتوحة المصدر ،و بالتالي لا يحتاج صاحب العمل إلى دفع المزيد من الأموال لشرائها بالإضافة إلى إمكانية التعديل عليها لتلائم احتياجات المشروع و تحقق الأهداف المرجوة.

– توفر العديد من المراجع و مواقع الانترنت التي تطرح حلول للمشاكل التي يمكن أن تعترضنا.

متطلبات nagios :

نظام linux , C Compiler , TCP/IP ، إعدادات Configuration

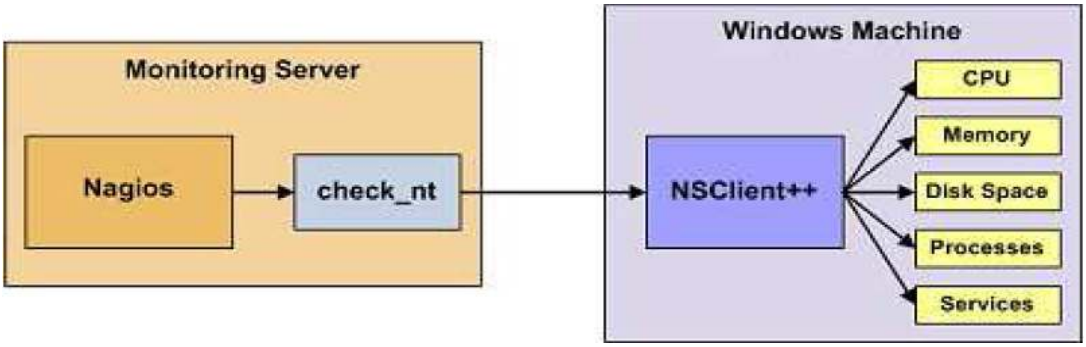
الميزات التي تتيحها nagios :

- مراقبة خدمات الشبكة (SMTP,POP3,HTTP,FTP.....)
- مراقبة مصادر ال Hosts (processor load,disk usage.....)
- إيصال التنبيهات عند ظهور مشكلة لدى ال Hosts
- القدرة على مراقبة عدد كبير أو فائض من ال Hosts
- واجهة ويب اختيارية لمراقبة حالة الشبكة ،ملاحظات وتاريخ الأعطال ،الخ....
- (**plugin**) بسيطة تسمح للمستخدم بتطوير خدمات التفحص الخاصة

خدمات المراقبة التي تتيحها Nagios بالإضافة إلى مراقبة المضيف المحلي localhost :

1. مراقبة الحواسيب العاملة وفق نظام ويندوز Windows machines
2. مراقبة الحواسيب العاملة وفق نظام لينكس Linux machines
3. مراقبة الطابعات الشبكية Network printers
4. مراقبة الموجهات و المبدلات Routers and Switches

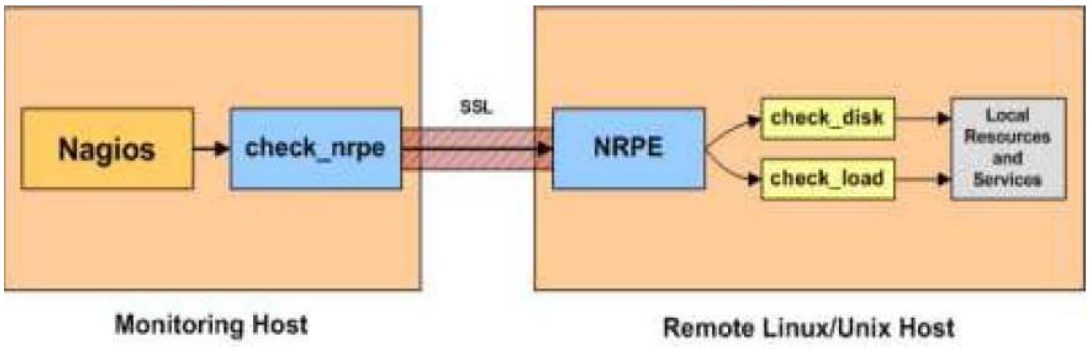
6- 2 -1 مراقبة الحواسيب العاملة وفق نظام ويندوز Windows machines:



الشكل 6-2 مراقبة الحواسيب العاملة وفق نظام ويندوز [12]

مراقبة مخدمات ويندوز يتطلب وجود وكيل عليها NSClient، هذا الوكيل يمثل الوسيط بين المراقب nagios والخدمات الموجودة في ويندوز حيث تستخدم nagios برنامج مساعد هو check_nt للتخاطب مع الوكيل.
يقوم nagios بتنفيذ الأمر check_nt وهو عبارة عن برنامج يتخاطب مع NSClient الذي بدوره يقوم بتنفيذ الأمر الموجه إليه عن طريق تنفيذ بعض البرامج أيضا كحساب انشغالية المعالج أو الحمل على القرص الصلب أو عدد المهام الشغالة بالإضافة إلى العديد من البرامج الأخرى فيقوم بتلقي النتائج وإعادتها إلى ال Nagios ليتم تحليلها وعرضها على واجهة الويب.

6-2-2 مراقبة الحواسيب العاملة وفق نظام لينكس Linux machines:



الشكل 6-3 مراقبة الحواسيب العاملة وفق نظام لينكس [6]

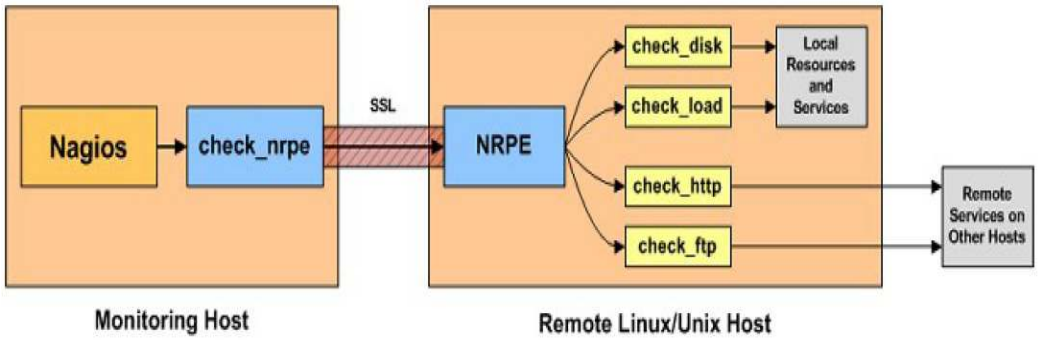
لمراقبة مخدمات لينكس يتطلب ذلك وجود وكيل هو NRPE يسمح بتنفيذ الأوامر لمراقبة مصادر الجهاز .

يقوم nagios بتنفيذ الأمر check_nrpe (يتبعه بالأمر المراد تنفيذه على الجهاز البعيد) هو عبارة عن برنامج يتخاطب مع الوكيل NRPE عن طريق فتح قناة اتصال أمنة (secure socket) الذي بدوره يقوم بتنفيذ الأمر الموجه إليه عن طريق تنفيذ بعض البرامج أيضا كحساب انشغالية المعالج أو الحمل على القرص الصلب أو عدد المهام الشغالة بالإضافة إلى العديد من البرامج الأخرى فبقوم بتلقي النتائج وإعادتها إلى ال Nagios ليتم تحليلها وعرضها على واجهة الويب.

6-2-2-1 NRPE :

وهو عبارة عن برنامج مصمم ليسمح لنا بتنفيذ الأوامر والتحكم عن بعد بأنظمة Linux ،والسبب الرئيسي لهذه العملية هو السماح ل nagios بمراقبة مصادر الجهاز (CPU,memory,..) ولأن هذه الموارد غير ظاهرة بالنسبة للألات الخارجية لذلك يجب تنصيب NRPE .

من الممكن تنفيذ أوامر Nagios عن طريق SSH حيث هناك برنامج check_by_ssh يسمح لنا القيام بذلك لكنه يحتاج إلى معالجة كبيرة عند كل من المراقب والجهاز البعيد،وهذا يسبب عبء عند مراقبة عدد كبير من الأجهزة لذلك يفضل استخدام NRPE لأنه لا يحتاج معالجة كبيرة.



الشكل 6-4 NRPE [17]

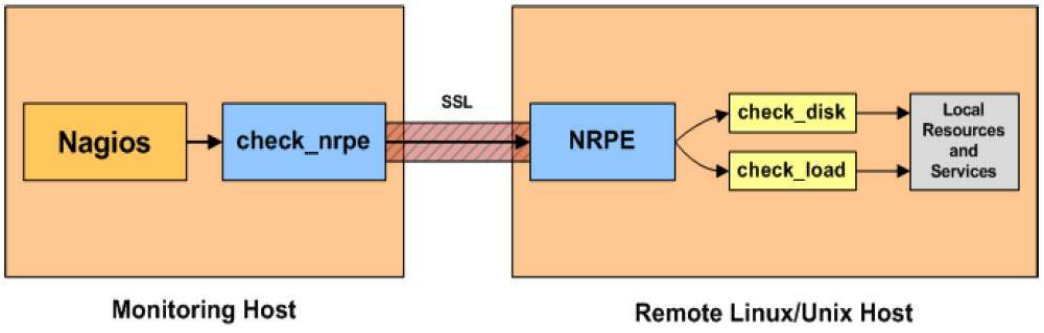
يتألف NRPE من جزئين:

- Check_nrpe وهو عبارة عن برنامج يوجد عند الجهاز الذي يقوم بعملية المراقبة.
- NRPE Daemon موجود عند الجهاز البعيد.

عندما تحتاج Nagios لمراقبة خدمة في جهاز Linux-Unix تقوم بعدد من الخطوات كالتالي:
تقوم بتنفيذ البرنامج check_nrpe وتخبره ماالخدمة التي تريد مراقبتها فيقوم هو بمخاطبة NRPE-Daemon عبر قناة اتصال أمنة SSl (secure socket layer) فيقوم بتنفيذ الأوامر المناسبة لفحص الخدمة المطلوبة والحصول على النتائج التي يتم إعادتها إلى check_nrpe ليعطيها إلى Nagios لتقوم بتحليل النتائج وعرضها في واجهة بيانية.
هناك حالتان للاستخدام:

مراقبة مباشرة:

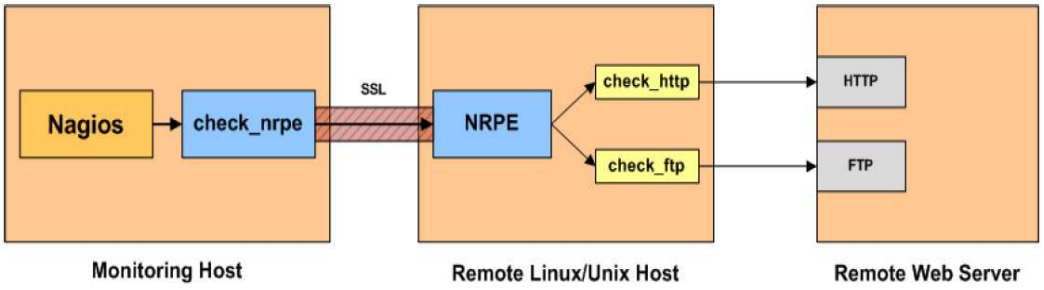
إن الإستخدام العام ل NRPE Deamon هو لمراقبة المصادر المحلية مثل انشغالية المعالج والحمل في الذاكرة والحمل على القرص الصلب بالإضافة إلى عدد المستخدمين وحالة المهام.



الشكل 6-5 مراقبة مباشرة عبر NRPE [17]

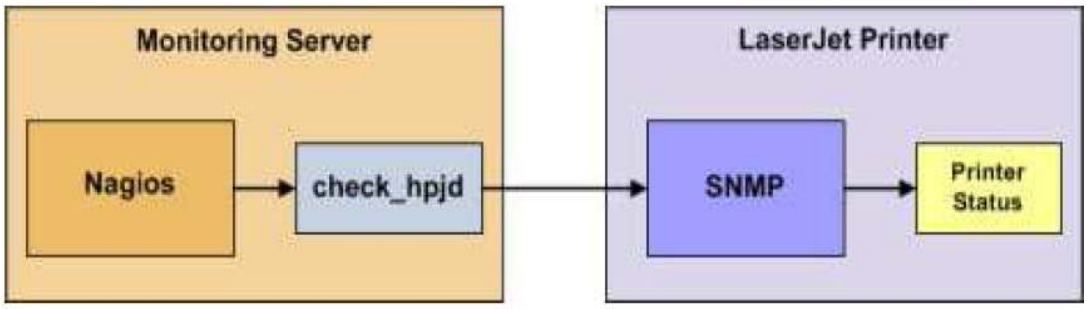
مراقبة غير مباشرة:

يمكن استخدام NRPE Daemon لفحص أجهزة بعيدة لايمكن لNagios الوصول إليها أي إذا كان بإمكان NRPE Daemon والبرامج المحملة على الجهاز البعيد التخاطب مع مخدم الويب مثلا يمكن إعدادها لمراقبة مخدم الويب بشكل غير مباشر.



الشكل 6-6 مراقبة غير مباشرة عبر NRPE [17]

6-2-3 مراقبة الطابعات الشبكية Network printers:

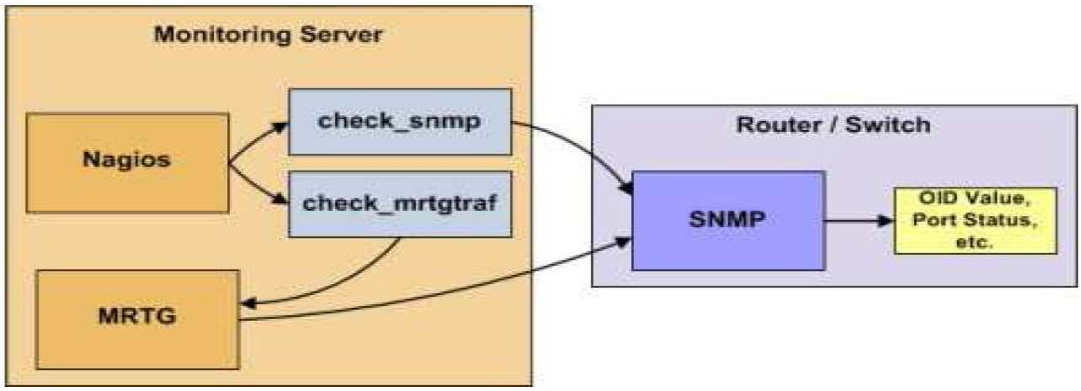


الشكل 6-7 مراقبة الطابعات الشبكية [6]

مراقبة الطابعات يتطلب وجود وكيل SNMP الذي يسمح بمراقبة حالة الطابعة عن طريق التخاطب مع البرنامج check_hpjd والذي يتحسس للحالات التالية:

Paper Jam Out of Paper
Printer Offline
Intervention Required
Toner Low
Insufficient Memory
Open Door
Output Tray is Full

6-2-4 مراقبة الموجهات و المبدلات Routers And Switches:



الشكل 6-8 مراقبة الموجهات و المبدلات [6]

يمكن مراقبة الموجهات و المبدلات بعمل ping لتحديد الطرود الضائعة ،إذا كان المبدل يدعم SNMP يمكن مراقبة حالة المنافذ عن طريق البرنامج check_snmp .و يمكن التخاطب مع snmp عن طريق برنامج أخر هو MRTG يمثل وسيط بين Nagios وSNMP .

أدوات الرسم البياني:

6-3 الأداة RRDTool :

RRD هي اختصار لعبارة (قاعدة بيانات الذهاب والإياب Round-Robin Database) وهي قاعدة بيانات تقوم بتخزين البيانات بصيغة متراصة لا يزداد حجمها مع مرور الزمن .يشيرمصطلح RRDtools إلى حزمة من الأدوات التي تتيح بناء و تعديل قواعد بيانات RRD بالإضافة إلى توليد رسوم بيانية واضحة لعرض هذه البيانات .تستخدم هذه الأدوات للإحتفاظ بسجل للبيانات مع مرور الزمن (كعرض حزمة الشبكة أو درجة حرارة الغرفة أو متوسط تحميل المخدم) وعرض هذه البيانات كقيمة متوسطة مع مرور الزمن. نلاحظ بأن أدوات RRDtool بحد ذاتها لا تتصل بتجهيزات الشبكة للحصول على المعلومات،فهي لا تعدو كونها مجرد أداة للتفاعل مع قاعدة البيانات .يمكن استخدام برمجيات بسيطة(تكتب عادة بلغة shell أو Perl) للقيام بهذه المهمة . تستخدم أدوات RDDtool أيضاً من قبل الكثير من برمجيات إدارة الشبكة المتطورة والتي توفر ميزة استعراض المعلومات أو تعديل الإعدادات من خلال متصفح الوب .تتميز أدوات RDDtool بمرونة أكبر في تحديد خيارات العرض و كمية المعلومات المعروضة ضمن الشكل البياني مقارنة بأداة MRTG. تتوفر أدوات RDDtool في جميع توزيعات نظام التشغيلGNU/Linux تقريباً .يمكن للأداة RRDtool إظهار أي نوع من البيانات كاستهلاك الذاكرة والمعالج مثلاً على شكل قيمة وسطية مع مرور الزمن.

6-4 Nagios Graph:

هو عبارة عن أداة يتم تركيبها مع Nagios ،تقوم بجمع معطيات من Nagios عن أداء الخدمات المعرفة في النظام ،و تضعها في قاعدة معطيات ،ثم يتم عرض هذه النتائج كمخططات بيانية عبر واجهة ويب.

Nagios Graph في الأساس هو عبارة عن واجهة بسيطة بين Nagios و ملفات RRD .

البساطة تأتي من ثلاثة عوامل :

- لا يحتاج إلى كثير من العمل الزائد.
- السلوك مبرمج أكثر من أنه قابل للإعداد.
- اكتشاف المعطيات الجديدة في Nagios تلقائيا.

Nagios Graph يعمل وفق نمطين :

1- يقوم بجمع معطيات من نتائج مراقبة الخدمات من Nagios .

2- عرض المعطيات التي تم جمعها بشكل مخططات بيانية.

5-6 Notification Tools :

هناك العديد من الطرق لإرسال التنبيهات في Nagios ولكل طريقة هناك أداة خاصة وهذه الأدوات هي :

Gnokii (SMS software for contacting Nokia phones via GSM network)
QuickPage (alphanumeric pager software)
Sendpage (paging software)
SMS Client (command line utility for sending messages to pagers and mobile phones)

في مشروعنا استخدمنا خدمة الرسائل القصيرة SMS المزودة من قبل مشغل شبكة الخلوي لإرسال رسائل تنبيه إلى الهاتف المحمول .

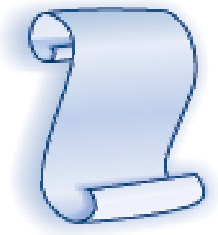
6-6 أدوات أخرى:

لغة Perl :

تم استخدام هذه اللغة في كتابة إجراءات الفحص[1] .

التعابير المنتظمة Regular Expression:

تم استخدام التعابير المنتظمة في عملية رسم الخطوط البيانية من خلال استخلاص معلومات المراقبة لخدمة ما من ملف معلومات التاريخ والذي يحوي معلومات المراقبة[2].

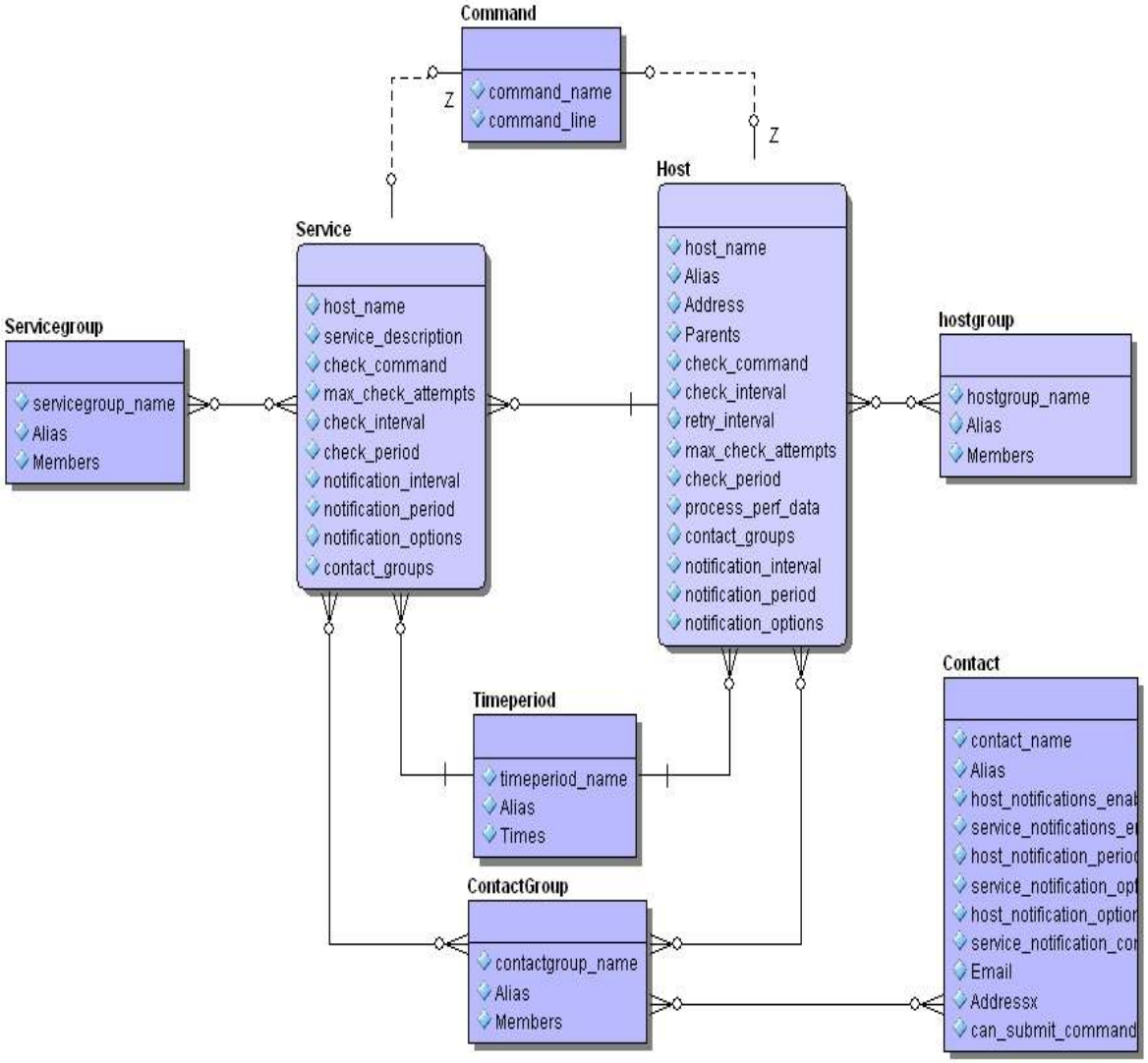


1- للإطلاع على لغة perl انظر الملحق A
2- للإطلاع على التعابير المنتظمة انظر الملحق B
3- للاطلاع عى تنصيب و إعداد الأدوات انظر الملحق C

الفصل السابع

تصميم النظام

7-1 تصميم بنية النظام :



الشكل 7-1 بنية النظام

يوضح الشكل 7-1 قاعدة المعطيات التي يرتكز عليها النظام وفيمايلي شرح للعلاقة بين هذه الكيانات hosts.cfg يمثل المخدمات وهو يرتبط بخدمة service.cfg او أكثر ، كما ترتبط الخدمة بكيان الأوامر commands.cfg الذي يستخدم للتفحص ، كما يرتبط المخدم بكيان hostgroup.cfg الذي يمكن من خلاله تجميع عدد من المخدمات الذين يشتركون بخصائص متشابهة ، ويمكن أيضا ربط مجموعة من الخدمات من خلال الكيان servicegroup.cfg ،كما نلاحظ الكيان contacts.cfg الذي يمثل الأعضاء المراد إيصال التنبيهات لهم عند حدوث عطل في الشبكة ويرتبط مع الكيان contactgroup.cfg الذي يضم أكثر من عضو، وهناك كيان timeperiods.cfg الذي يحدد الفترات الزمنية التي يمكن خلالها القيام بعملية التفحص وإرسال التنبيهات .

7-2 بنية الأغراض:

هي جميع العناصر المعنية بمنطق المراقبة والتنبيه.

وتتضمن الأغراض التالية:

- Services
- Service Groups
- Hosts
- Host Groups
- Contacts
- Contact Groups
- Commands
- Time Periods
- Notification Escalations

تعريف مضيف host:

host_name	اسم يستخدم لتعريف المضيف ،يستخدم ضمن تعريف Hostgroup و Servicedefinition .
Alias	يستخدم كأسم بديل أطول من السابق وهو عبارة عن توصيف للمضيف .
Address	يستخدم لتعريف عنوان المضيف و هو غالبا IP و يمكن أن يكون FQDN و لكن إذا كان DNS غير موجود يمكن أن يكون هناك مشكلة.
Parents	يستخدم لتحديد قائمة آباء هذا المضيف و هذه القائمة يمكن أن تتضمن : مبدلات أو موجهات أو جدران نارية ،و لكن إذا كان المضيف في نفس مقطع المراقب فإنه ليس بحاجة لذكر الآباء parents.
check_command	يستخدم لتعريف اسم الأمر الذي يقوم بفحص حالة الجهاز (UP or DOWN) ،إذا ترك هذا الخيار لن نستطيع تحديد حالة الجهاز ،هذا الخيار جيد في حال الأجهزة التي تطفئ مثل الطابعات.
check_interval	لتحديد عدد الوحدات الزمنية التي تفصل بين محاولات تفحص المضيف ،و القيمة الإفتراضية 60 ثانية.
retry_interval	لتحديد فترة الإنتظار بعد انتهاء عدد المحاولات الأعظمي .
max_check_attempts	تحدد عدد المرات التي تقوم فيها النظام بتنفيذ أمر التفحص check_command في حال فشل إعادة الحالة OK ، إذا وضعت هذه القيمة على الواحد لن يقوم النظام بإعادة التفحص و يكتفي بإصدار تحذير.

check_period	لتخصيص اسم لفترة زمنية يمكن أن يقوم المضيف خلالها بعمليات مراقبة نشطة
process_perf_data	تستخدم لتخزين معلومات تاريخية حول مراقبة الجهاز (لاستخدامها في عملية رسم الخطوط البيانية)
contact_groups	تعريف مجموعة جهات الاتصال الذين نريد أن تصلهم رسائل التنبيهات.
notification_interval	لتحديد عدد الوحدات الزمنية اللازمة للإنتظار قبل إعادة تنبيه جهات الاتصال بأن الخدمة في حالة down أو Unreachable.القيمة الإفتراضية هي 60 ثانية
notification_period	اسم يحدد فترات زمنية يمكن أن ترسل خلالها التنبيهات
notification_options	يستخدم لتحديد متى ينبغي إرسال التنبيهات المتعلقة بالمضيف و يأخذ إحدى القيم التالية : d- إرسال التنبيهات في حالة Down u- إرسال التنبيهات في حالة Unreachable r- إرسال التنبيهات في حالة recoveries (OK state) f- إرسال التنبيهات في حالة بدأ المضيف و توقف عملية ال flapping s- إرسال التنبيهات في الحالة التي تبدأ أو تنتهي عملية Scheduled downtime n- لايتم إرسال أي تنبيه عند ذكر أحد الخيارات السابقة يتم إرسال التنبيه المتعلق به فقط.

تعريف مجموعة مضيفين HostGroup:

hostgroup_name	لتعريف اسم يستخدم لتحديد المجموعة التي ينتمي إليها المضيف.
Alias	اسم بديل لمجموعة المضيفين Hostgroup وهو اسم أطول من السابق وقد يكون عبارة عن وصف.
Members	قائمة من أسماء المضيفين Hosts الذين ينتمون لهذه المجموعة .

تعريف خدمة Service:

يستخدم لتعريف خدمة تعمل على المضيف ,نقصد بها أحيانا خدمة فعلية تعمل على المضيف مثل :
(pop,smtp,http) أو مثلا الإستجابة لأمر Ping أو عدد المستخدمين الداخلين للنظام أو المساحة الحرة على القرص.

host_name	قائمة من أسماء المضيفين Hosts الذين يرتبطون مع هذه الخدمة، يفصل بين أسماء المضيفين بفواصل
service_description	توصيف الخدمة حيث أنه لايوجد خدمتان ترتبطان مع نفس المضيف لهما نفس التوصيف أو نفس الأسم،الخدمة يجب أن تكون وحيدة الأسم و التوصيف.
check_command	يستخدم لذكر اسم الأمر الذي سيستخدمه النظام لفحص حالة الخدمة .
max_check_attempts	هذا الخيار يمكن من تحديد عدد المرات التي سيقوم فيها النظام بإعادة تنفيذ أمر التفحص check_command في حال إعادة قيمة غير OK وفي حال وضع قيمتها على الواحد سيكتفي بإصدار تحذير دون إعادة تنفيذ أمر التفحص.
check_interval	لتحديد عدد الوحدات الزمنية التي تفصل بين محاولات تفحص الخدمة ،القيمة الافتراضية 60 ثانية.
check_period	يحدد الفترات التي تتم فيها عملية التفحص للخدمة.
notification_interval	يستخدم لتحديد عدد الوحدات الزمنية اللازمة للإنتظار قبل إعادة تنبيه جهة الاتصال طالما الخدمة ليست في حالة OK ،القيمة الإفتراضية 60 ثانية، وإذا وضعت قيمتها على الصفر فإن النظام لن يقوم بإعادة تنبيه جهات الاتصال حول مشاكل هذه الخدمة بل يتم إصدار تنبيه واحد فقط
notification_period	اسم يحدد فترات زمنية يمكن خلالها إرسال التنبيهات لجهات الاتصال.
notification_options	يستخدم لتحديد متى ينبغي إرسال التنبيهات المتعلقة بالخدمة و يأخذ إحدى القيم التالية: w- إرسال التنبيهات في حالة Warninig u- إرسال التنبيهات في حالة Unknown c- إرسال التنبيهات في حالة Critical r- إرسال التنبيهات في حالة recoveries (OK state) f- إرسال التنبيهات في حالة بدء الخدمة وتوقف عملية ال flapping s- إرسال التنبيهات في الحالة التي تبدأ أو تنتهي عملية Scheduled downtime n- لايتم إرسال أي تنبيه عند ذكر أحد الخيارات السابقة يتم إرسال التنبيه المتعلق به فقط.
contact_groups	لتحديد مجموعات جهات الاتصال الذين لابد من تنبيههم عند حدوث مشكلة ،يفصل بين أسماء المجموعات بفواصل ولابد من ذكر اسم جهة اتصال واحدة أو مجموعة اتصال واحدة على الأقل.

تعريف مجموعة خدمات servicegroup :

servicegroup_name	عبارة عن اسم لتحديد اسم المجموعة
Alias	اسم بديل للمجموعة قد يكون أطول من السابق أو عبارة عن توصيف للمجموعة.
Members	قائمة من أسماء الخدمات و أسماء المضيفين التي ترتبط معها ،يستخدم هذا الخيار كبديل ل servicegroup في تعريف الخدمة،وتكون الصيغة التي يكتب بها الأمر بالشكل: members=<host1>,<service1>,<host2>,<service2>

تعريف جهة اتصال Contact:

يستخدم لتعريف الشخص الذي سيتم تنبيهه عند حدوث مشكلة في الشبكة.

contact_name	لتعريف اسم يحدد جهة الاتصال
Alias	يستخدم كاسم بديل يكون أطو ل من السابق أو توصيف لجهة الاتصال
host_notifications_enabled	يحدد فيما إذا ستتلقى جهة الاتصال التنبيهات المتعلقة بمشاكل المضيفين Values: 0 = don't send notifications, 1 = send notifications
service_notifications_enabled	يحدد فيما إذا ستتلقى جهة الاتصال التنبيهات المتعلقة بمشاكل الخدمات Values: 0 = don't send notifications, 1 = send notifications
host_notification_period	يستخدم لتخصيص اسم للفترة الزمنية التي يمكن خلالها أن تتلقى جهة الاتصال التنبيهات المتعلقة بمشاكل المضيف
service_notification_options	يستخدم لتحديد التنبيهات (المتعلقة بحالة الخدمة) التي سترسل إلى هذا جهات الاتصال
host_notification_options	يستخدم لتحديد حالات المضيف التي سترسل فيها التنبيهات إلى جهة الاتصال
service_notification_commands	يستخدم لتعريف قائمة من أسماء الأوامر التي تستخدم لتنبيه جهة الاتصال عند حدوث مشكلة في خدمة ما،يتم تنفيذ جميع الأوامر عندما يكون هناك حاجة لتنبيه جهة الاتصال ،يمكن التحكم بزمن أمر التنبيه من خلال خيار notification_timeout
Email	يستخدم لتعريف عنوان بريد الكتروني لجهة الاتصال الذي ستصل إليه رسائل

	التنبيه
Addressx	يستخدم لتعريف عناوين إضافية لجهة الاتصال مثل رقم تلفون أو غيره ويمكن أن يصل عدد العناوين إلى 6 حيث يمكنه استقبال رسائل التحذير على هذه العناوين
can_submit_commands	يستخدم لتحديد فيما إذا كان يسمح لجهة الاتصال إرسال أوامر خارجية للنظام عبر واجهة الويب ،إذا كانت قيمة هذا الخيار 0 لا يسمح له بإرسال الأوامر، 1 السماح له بإرسال الأوامر.

تعريف مجموعة جهات اتصال contactgroup :

contactgroup_name	اسم يستخدم لتعريف مجموعة جهات الاتصال
Alias	اسم اطول من السابق أو توصيف يعرف مجموعة جهات الاتصال
Members	لتعريف قائمة من أسماء جهات الاتصال التي يجب أن تضمن في مجموعة الاتصال ،هذا الخيار يستخدم كبديل أو بالإضافة إلى خيار contactgroup في تعريف جهة الاتصال contact .

تعريف قائمة فترات زمنية timeperiod :

قائمة من الأوقات تحدد أوقات مختلفة للقيام بعمليات التنبيه وتفحص الخدمات بشكل دوري .

timeperiod_name	اسم يعرف قائمة الأوقات timeperiod
alias	اسم بديل للأسم السابق
times	فترات زمنية

تعريف أمر command :

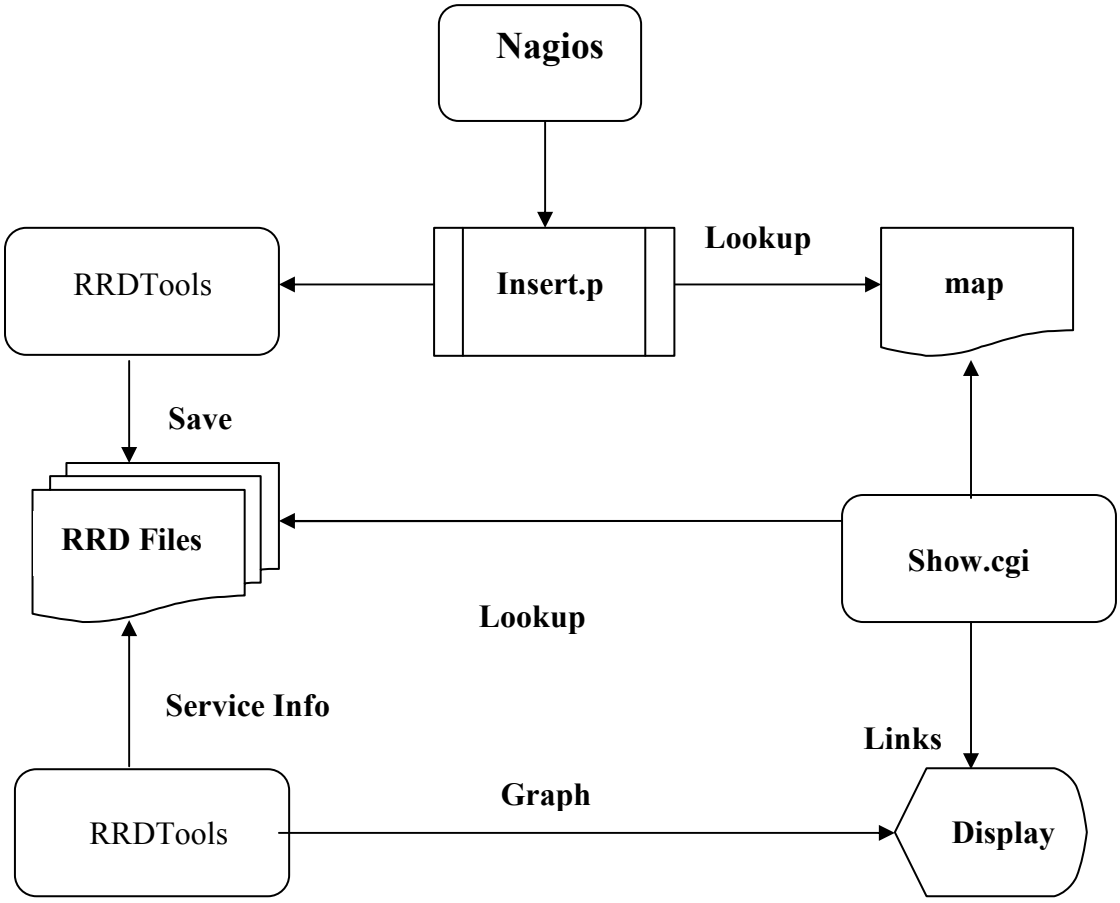
يستخدم لتعريف أمر (command) ،الأوامر يمكن أن تضمّن في الأغراض الأخرى فهي تستخدم في تفحص الخدمات، تنبيهات الخدمات، تفحص المضيفين ،تنبيهات المضيفين.الخ....

command_name	اسم يستخدم لتعريف الأمر و يستخدم هذا الاسم ضمن تعريف المضيف و الخدمة و جهة الاتصال.
command_line	هو عبارة عن مسار الإجراء script الواجب تنفيذه عند استدعاء الأمر من قبل المضيف أو الخدمة

للاطلاع على أمثلة عن تعريف الأغراض انظر الملحق D

7-3 تصميم مخطط عملية الرسم :

نوضح كيف تتم عملية الرسم من خلال المخطط التالي:



الشكل 7-2 عملية رسم الخطوط البيانية

تقوم Nagios بمراقبة الخدمات و الحصول على النتائج ثم تمرر نتائج المراقبة إلى الإجراء insert.pl ، و الذي يقوم بمطابقة نتائج المراقبة مع نماذج معرّفة ضمن ملف map باستخدام التعابير المنتظمة [2] ،و بالتالي يتم فصل معلومات كل خدمة ضمن ملف مستقل.

show.cgi هو إجراء يقوم بعرض وصلات لمعلومات الخدمات فقط ،حيث يقوم بالبحث عن ملفات RRD و ذلك بمساعدة ملف map ،و يتم عرض رابط لكل خدمة في الصفحة الرئيسية ،يتيح الوصول إلى المخطط البياني لهذه الخدمة.

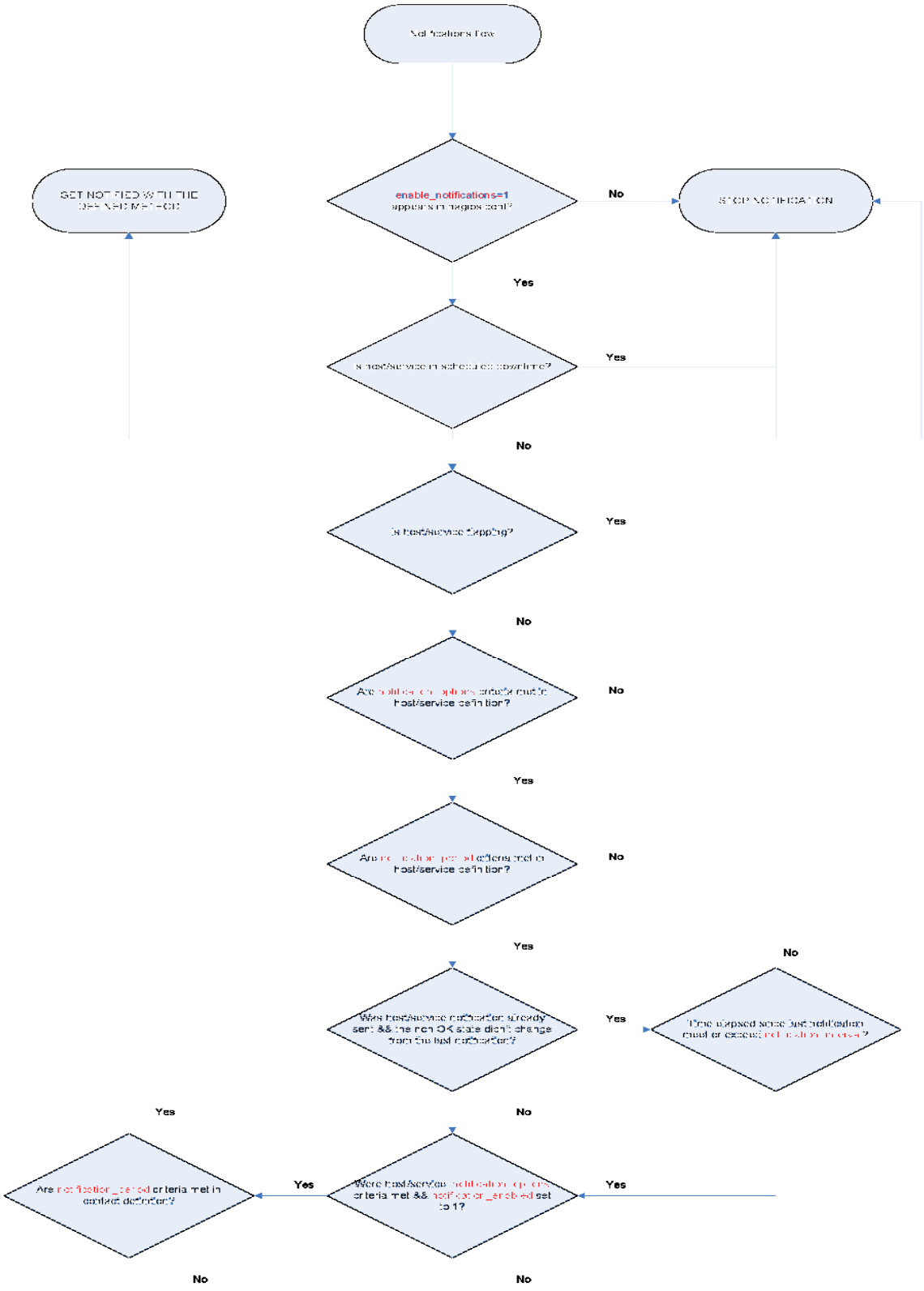
افتراضيا كل معطيات الخدمات المتاحة ستظهر في مخطط بياني واحد ،و لكن يمكن من خلال الإعدادات ،و تحديد روابط URL تغيير عدد المعاملات المعروضة أو تقسيم المعطيات لعدة مخططات بيانية.

7-4 تصميم مخطط التنبيهات:

يوضح الشكل 7-3 عملية التنبيه و فيمايلي شرح للشكل:

عند ظهور حالة حرجة <critical> و انقضاء فترة من الزمن على حالة nonOK(غير طبيعية)

1. يتم تفحص إذا تم تفعيل خيار التنبيه في ملف nagios.cfg إذا كان مفعلا يتم الإستمرار
2. فحص الخيار scheduled downtime المتعلق بالخدمة أو المضيف (يتم فحص الخدمة إذا كانت مجدولة ضمن قائمة الخدمات المعطلة حاليا – يتم تعطيل مراقبة بعض الخدمات خلال فترة زمنية) إذا لم يكن هذا الخيار مفعلا يتم الإستمرار
3. فحص خيار falpping (عدم الإستقرار) حيث يتم حفظ أخر واحد وعشرين قراءة لحساب نسبة التغيرات ومقارنتها مع المجال المسموح للتغيرات فإذا كانت أكبر من الحد المسموح نعتبر أن الحالة غير مستقرة ولا يتم التنبيه أما إذ أصغر يتم الإستمرار
4. فحص خيارات التنبيه ضمن الخدمة أو المضيف في حال كانت مفعلة يتم الإستمرار
5. فحص خيار notification period أي أن التنبيه ضمن الفترة المحددة فإذا كانت الحالة ضمن الفترة المسموحة يتم الإستمرار
6. فحص حالة الخدمة منذ أخر تنبيه إذا لم تتغير من nonOK
   أ- يتم فحص الخيار notification interval (فترة زمنية يجب انتظارها في حال لم تتغير الخدمة) إذا تجاوزت هذه الفترة يتم الإستمرار لفحص notification enabled .
   ب- إذا تغيرت الحالة من nonOK يتم الإنتقال فورا لفحص notification enabled
7. في حال كان الخيار notification enabled مفعلا يتم الإستمرار
8. يتم فحص فيما إذا أحد الأعضاء ضمن فترة التنبيه ليتم إرسال التنبيه إليه.



الشكل7–3 مخطط التنبيه

الفصل الثامن

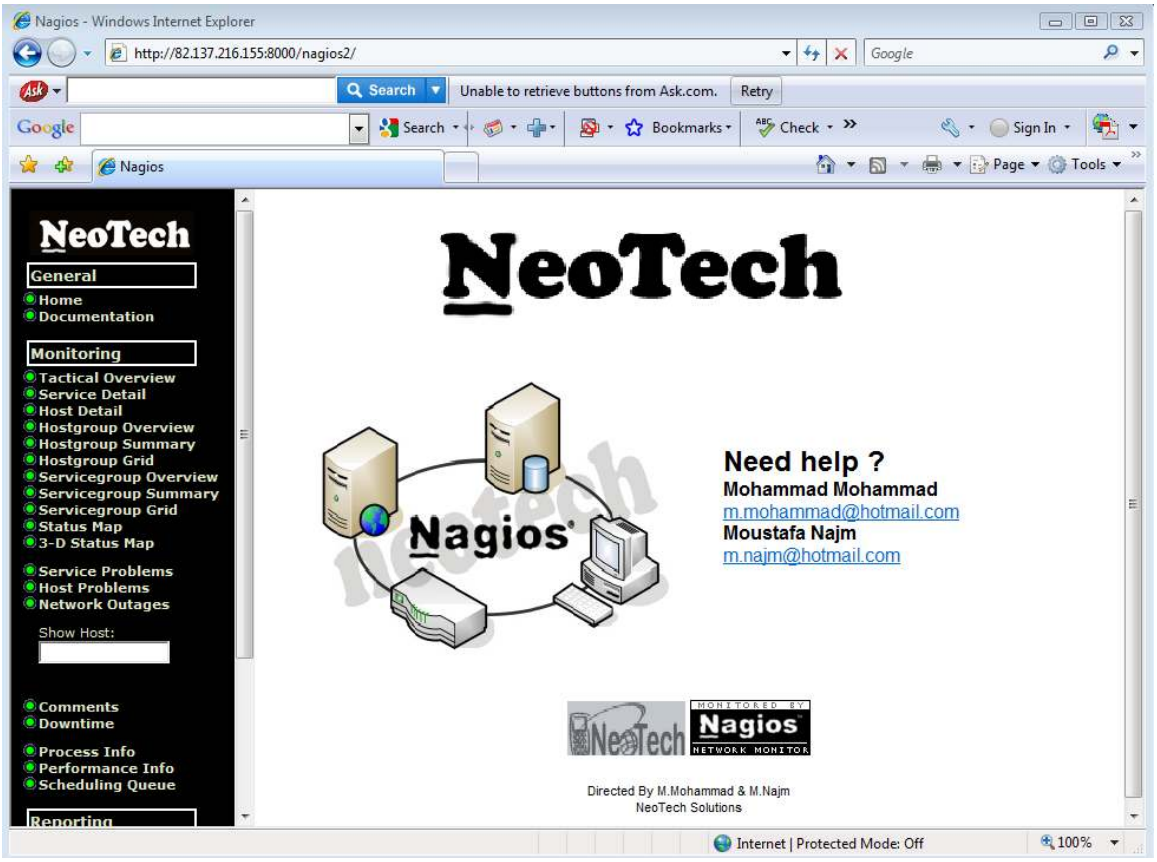
التحقيق و التنفيذ

8-1 شرح واجهات النظام :

في هذه المرحلة سيتم شرح جميع الواجهات الموجودة ضمن النظام و كيفية استخدام النظام :

- **الواجهة الرئيسية :**

و هي الواجهة التي تظهر لنا عند تنفيذ النظام.



الشكل 8-1 واجهة النظام الرئيسية

و هي تمثل الواجهة الرئيسية التي يمكن من خلالها الوصول إلى جميع الخدمات التي يحققها النظام من خلال الضغط على الروابط الموجودة في القائمة اليسارية :

Tactical overview	يعطي خلاصة عامة عن حالة المضيفين و الخدمات في الشبكة
Service Detail	**يوضح** بشكل تفصيلي حالة الخدمات في جميع المضيفين
Host Detail	يعطي معلومات عن المضيفين hosts الموجودة في الشبكة و حالة كل منها
HostgroupOverview	تظهر معلومات عن حالة المضيفين و ملخص عن حالة الخدمات ضمن كل مضيف

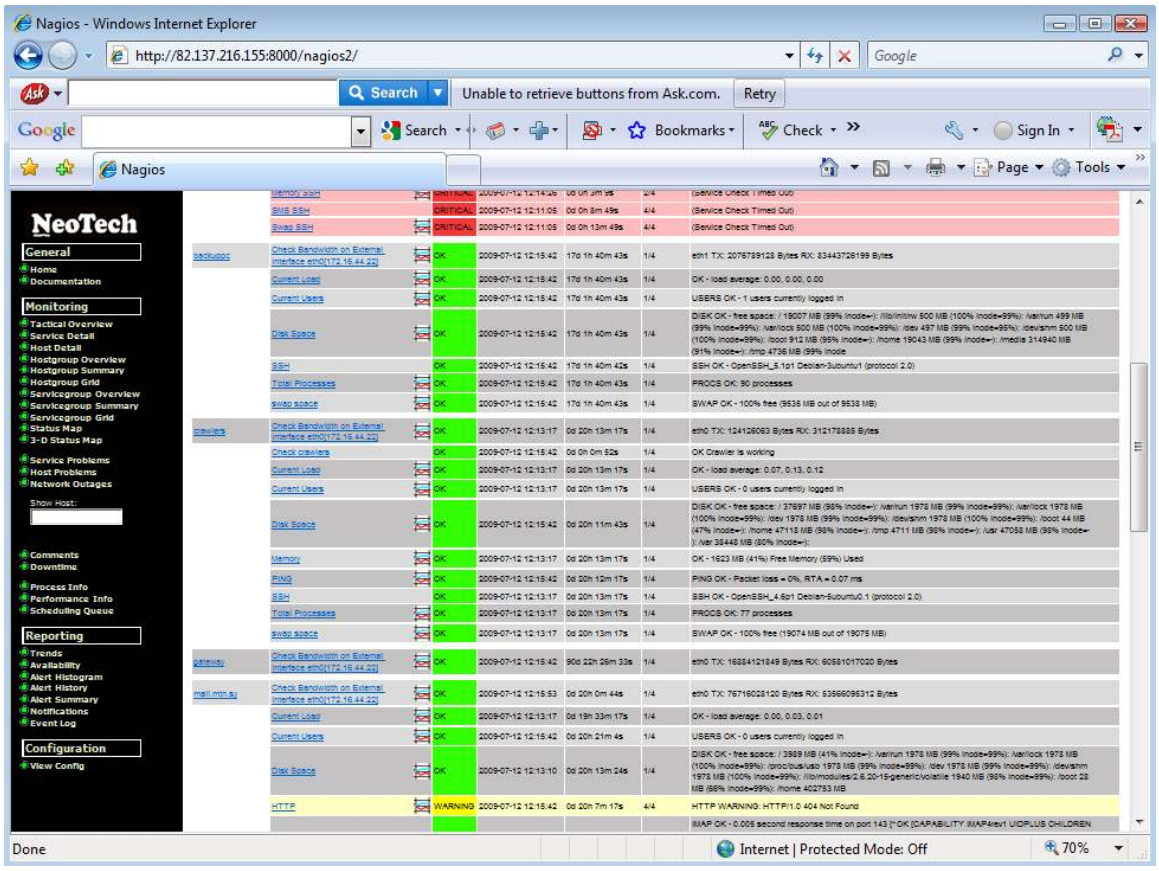
HostgroupSummary	تعطي ملخص عن مجموعة ما (مجموعة مضيفين) و عن الخدمات ضمن هذه المجموعة
HostGroup Grid	تظهر مجموعة المضيفين و الخدمات المعرفة ضمن كل منها (عرض فقط و ليس مراقبة)
Status map	خريطة توضح مكونات الشبكة الخاضعة للمراقبة
Service Problems	**تظهر** الخدمات التي تحوي مشاكل (حالة حرجة أو تنبيه أو غير معروفة) تظهر فائدة هذه الخدمة في حال كان عدد المضيفين كبير ،و بالتالي قد لا نستيطع تمييز الحالات التي تحوي مشاكل ،و للسهولة يمكن اختيار عرض الحالات التي تحوي مشاكل فقط
Process Info	**و** هي تعرض معلومات حول النظام ،و المهام المختلفة ضمنه. يظهر لدينا معلومات مختلفة ،مثلا :لحظة تشغيل النظام ،فترة عمل النظام (بشكل مستمر من آخر تشغيل و هي الفرق بين الزمن الحالي و زمن آخر تشغيل) ،و المهام الفعالة و المعطلة.
Performance Info	يظهر معلومات حول أداء النظام ،مثلا زمن تفحص الخدمة.
Scheduling Queue	يظهر حالة الخدمات المختلفة (فعالة أو معطلة) حيث يمكن تعطيل خدمة ،مثلا إذا كانت تستهلك قدر كبير من موارد النظام أو لا تهمنا مراقبتها حاليا
Alert Histogram	يعرض معلومات تاريخية عن مراقبة الخدمات المختلفة و المضيفين
Notifications	تعرض الحالات التي تم فيها إرسال تنبيه لمدير الشبكة (مثلا حالة توقف خدمة أو مضيف)
View Config	يظهر إعدادات المضيفين (يحصل عليها من ملف تعريف المضيفين و يعرضها)

ملاحظة :

نستفيد من تعريف المجموعة مثلا في حال كان لدينا مخدمات Linux و مخدمات Windows ،حيث نعرف مجموعة لكل منهما ،أو لتطبيق خدمة على مجموعة مخدمات (و ذلك بتطبيقها مرة واحدة على المجموعة و بالتالي يتم تطبيقها على كل مخدم ضمن المجموعة).

- **مراقبة خدمة :**

يمكن من خلال الواجهة التالية مراقبة الخدمات ،و يمكن الوصول إليها يتم عبر الرابط Service Detail.



الشكل 8-2 واجهة مراقبة خدمة

نلاحظ هنا مجموعة من الحقول ،و هي :اسم الخدمة ،حالة الخدمة ،زمن آخر عملية تفحص ،فترة التفحص ،و ناتج تنفيذ مراقبة الخدمة.

نميز عدة حالات للخدمة ،مثلا استخدام الذاكرة : أقل من 80 ٪ الحالة طبيعية OK ،بين 80٪- 90 ٪ حالة تنبيه Warning ،أعلى من 90٪ حالة حرجة Critical.

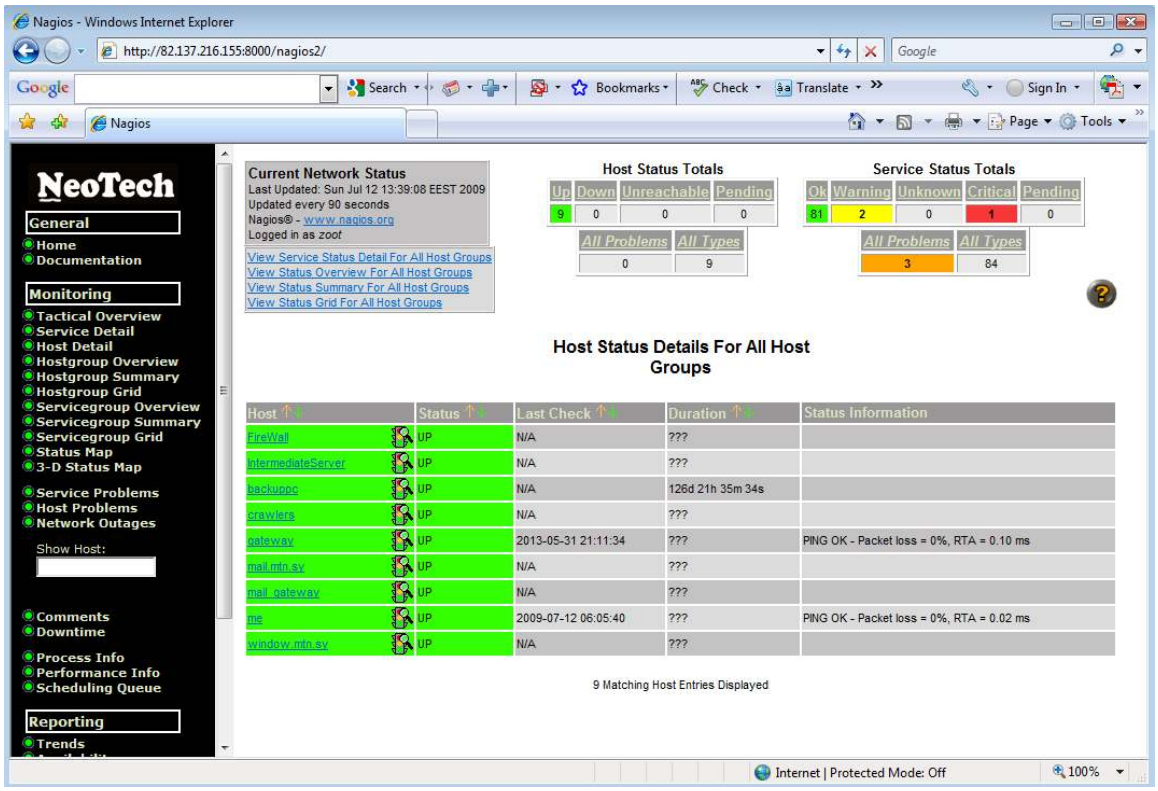
هناك حالة إضافية Unknown تدل على أن حالة الخدمة غير معروفة ،لعدم القدرة على تفحص الخدمة (نتيجة انقطاع الاتصال مثلا) أو عدم القدرة على تفسير نتيجة التفحص.

نميز حالة الخدمة بالألوان كمايلي :

OK	أخضر	Critical	أحمر
Warning	أصفر	Unknown	برتقالي

- **مراقبة مضيف:**

يمكن من خلالها مراقبة حالة المضيفين ،و يتم الوصول إليها عبر الرابط Host Detail.



الشكل 8-3 واجهة مراقبة مضيف

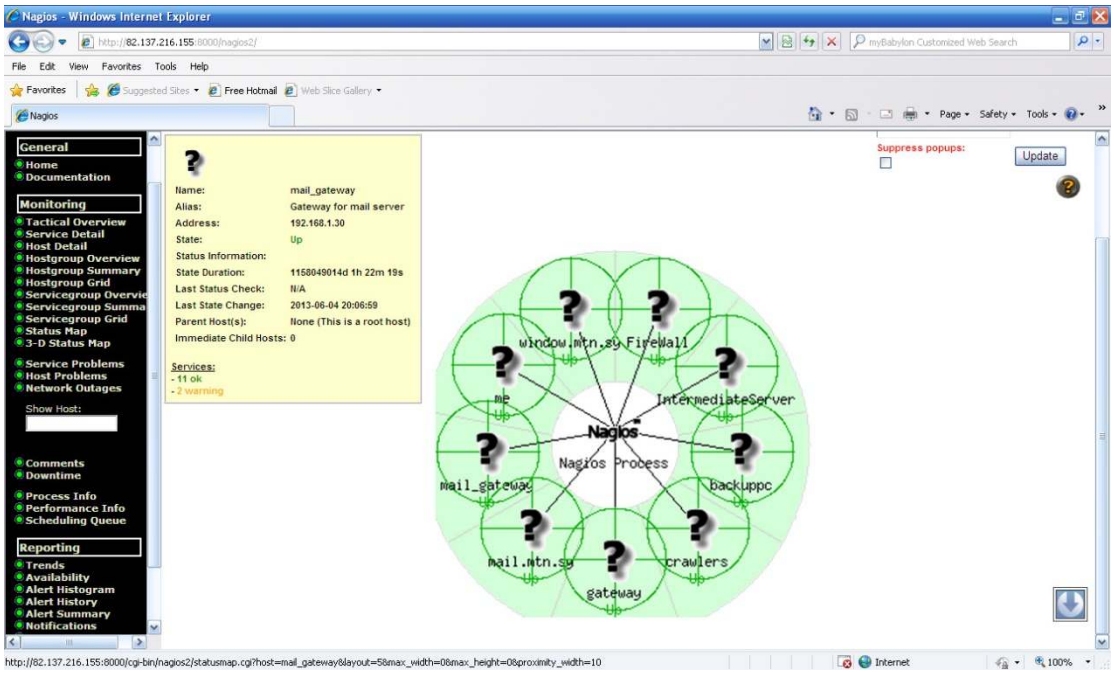
كذلك نلاحظ هنا تمييز حالة المضيف بالألوان (كما في حالة الخدمة).

كما نلاحظ يظهر في أعلى الصفحة ملخص للحالات : عدد المضيفين في كل حالة ،و عدد الخدمات في كل حالة ،و عدد المشاكل (و هي الحالات الحرجة و حالات التنبيه).

و يمكن تحديد مضيف معين :لمراقبة حالته أو مراقبة الخدمات ضمنه بإدخال اسم المضيف ضمن القائمة اليسارية.

- **خريطة الشبكة :**

توضح مكونات الشبكة الخاضعة للمراقبة ،و يتم الوصول إليها عبر الرابط Status map.



الشكل 8-4 واجهة خريطة الشبكة

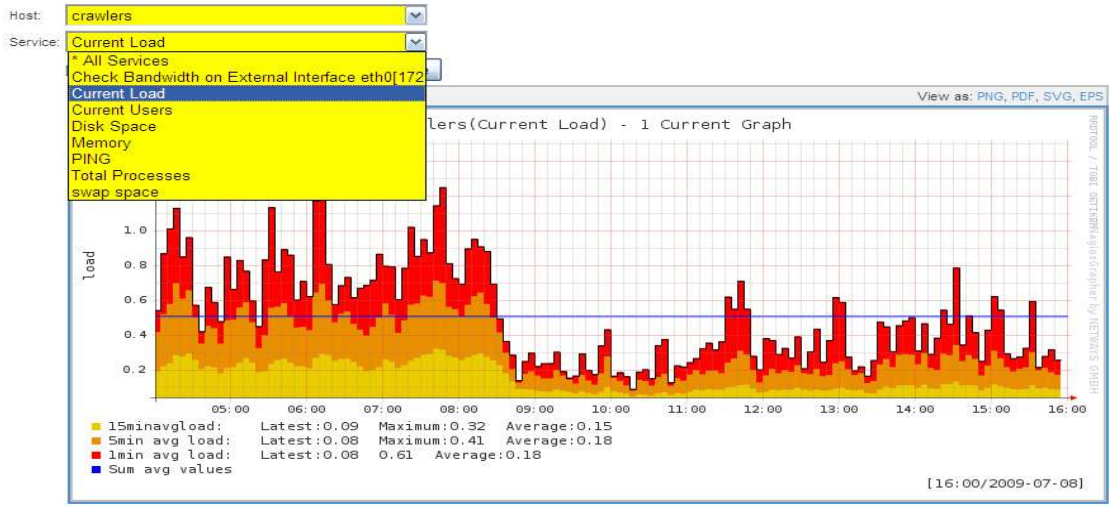
يمكن الحصول على معلومات كل مضيف بوضع المؤشر على هذا المضيف.

8-2 الرسوم البيانية :

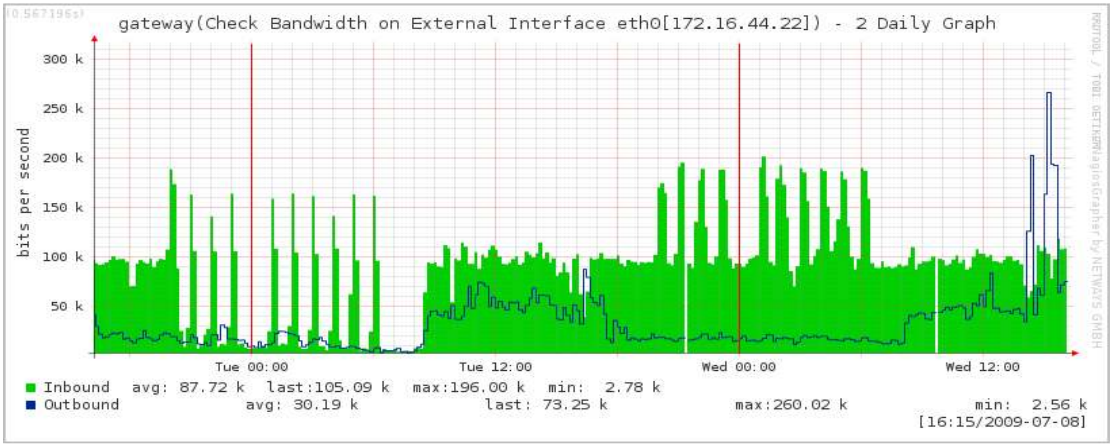
لاحظ عند مراقبة الخدمات أنه يظهر بجوار كل خدمة أيقونة صغيرة يمكن من خلال الضغط عليها الحصول على مخطط بياني لمراقبة الخدمة،يكن عرض مخططات بالوقت الحالي (خلال عشر دقائق) أو يومية أو أسبوعية أو سنوية.

يجب تحديد المضيف و الخدمة (ضمن المضيف) التي نريد رسم الخطط البياني لها (لاحظ ذلك في الشكل 8-5).
و يتم رسم المخطط البياني عن طريق أداة RRD Tool و Nagios Graph.
و يمكن من خلال تحليل هذه المخططات استنتاج العديد من المعلومات المفيدة مثل :وقت الذروة ،و فترات الضغط ،و نسبة تزايد الاقبال على خدمة ما .و بالتالي يمكن إلى حد ما التنبؤ بالمستقبل للحفاظ على جاهزية الشبكة و جودة الخدمة و ذلك باتخاذ الإجراءات المناسبة في الوقت المناسب.

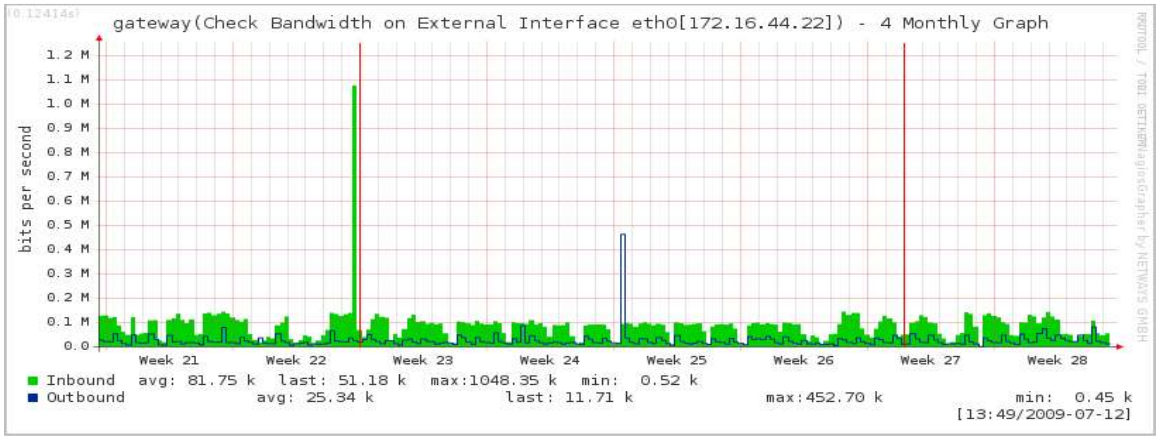
فيما يلي بعض المخططات البيانية لخدمات مختلفة :



الشكل 8-5 مخطط حالي لخدمة الحمل على مخدم الـ crawler



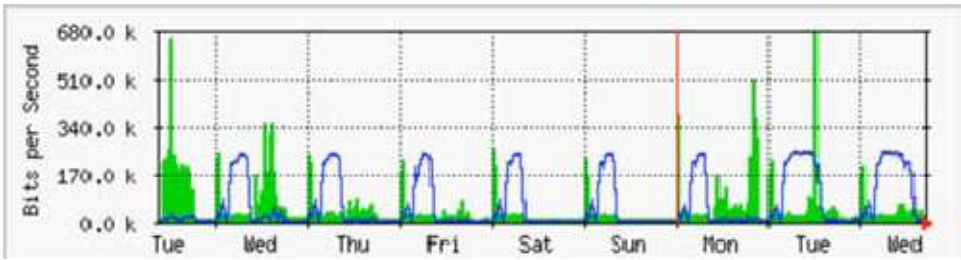
الشكل8-6 مخطط يومي لتدفق البيانات عبر على الواجهة الخارجية لـ getway



الشكل8-7 مخطط شهري لتدفق البيانات عبر الواجهة الخارجية لـ getway

8-2-1 كيفية تفسير الرسوم البيانية لتدفق البيانات عبر الشبكة:

تشير المنطقة الخضراء في الرسوم البيانية البسيطة لتدفق البيانات عبر الشبكة (كتلك التي يولدها برنامج NagiosGraph) إلى البيانات الواردة إلى الشبكة inbound traffic ،في حين يستدل باللون الأزرق على البيانات الصادرة من الشبكة outbound traffic. نعني هنا بالبيانات الواردة أية بيانات يقع مصدرها خارج الشبكة المعنية (عادة ما ترد هذه البيانات من شبكة الإنترنت) وتتجه إلى حاسوب يقع ضمن هذه الشبكة .أما البيانات الصادرة فترسل من داخل الشبكة إلى عناوين تقع ضمن شبكة الإنترنت .تعين الرسوم البيانية لتدفق البيانات عبر الشبكة على استيعاب الكيفية التي يتم وفقها استثمار هذه الشبكة .يمكن عبر مراقبة المخدمات مثلاً اكتشاف الكميات الفائضة من البيانات الصادرة أثناء استجابة هذه المخدمات للطلبات الواردة (كإرسال البريد الإلكتروني أو توفير صفحات الوب)، كما أن مراقبة حواسيب المستخدمين قد تساعد على كشف الكميات الفائضة من البيانات الواردة إلى هذه الحواسيب أثناء استقبالها من المخدمات.



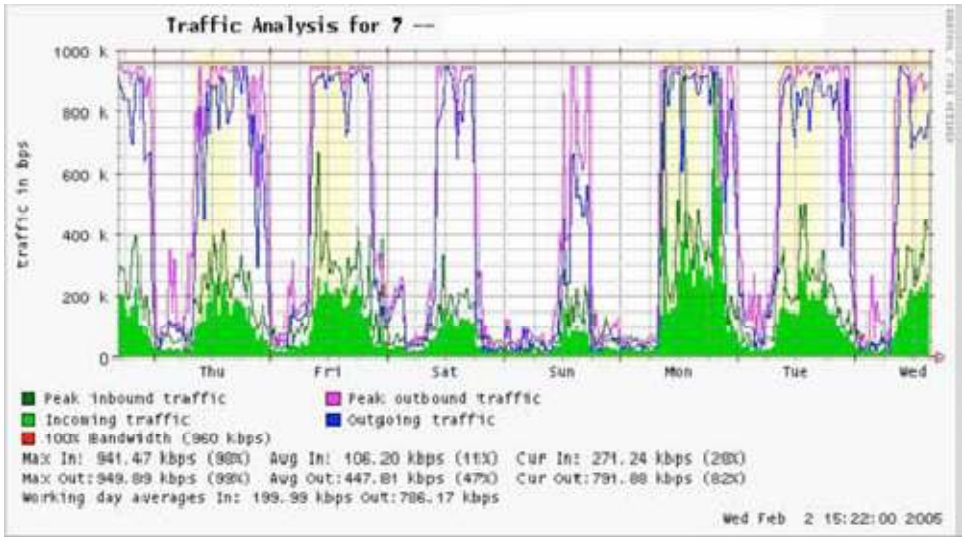
الشكل8-8 الرسم البياني التقليدي لتدفق البيانات ضمن الشبكة [3]

تمثل المنطقة القاتمة البيانات الواردة في حين يدل الخط على البيانات الصادرة .تبين الأقواس المتكررة في خط البيانات الصادرة الفترات التي تتم فيها عمليات النسخ الإحتياطي.

ستتغير أشكال تدفق البيانات عبر الشبكة تبعاً للجهاز الذي تتم مراقبته .سيظهر الموجه مثلاً كميات أكبر من البيانات الواردة مقارنة بتلك الصادرة أثناء قيام مستخدمي الشبكة بتحميل ملفات من شبكة الإنترنت .قد تشير الكميات الفائضة من البيانات الصادرة و التي لم تقم مخدمات الشبكة بإرسالها إلى وجود برنامج لتبادل الملفات peer-to-peer أو مخدم غير مخول أو حتى فيروس ضمن أحد الأجهزة .لا توجد مجموعة محددة من المعايير التي ستحدد الكيفية التي ينبغي أن تكون عليها البيانات الصادرة أو الواردة، لذلك ينبغي تحديد الحالة المرجعية للشبكةلنتمكن من استيعاب الشكل الطبيعي لحركة البيانات عبر الشبكة.

8-2-2 إكتشاف التحميل الزائد للشبكة

يظهر **الشكل8-9** حركة البيانات ضمن وصلة الإنترنت عند تحميلها بأكثر من طاقتها.



الشكل8-9 التحميل الزائد للشبكة [3]

تشير الرسوم البيانية ذات القمم المسطحة إلى أن الوصلة تعمل بكامل استطاعتها وبأن تحميل هذه الوصلة يفوق طاقتها في هذه الفترات.

تعتبر القمم المسطحة في الرسم البياني لكمية البيانات الصادرة أكثر المؤشرات وضوحاً على التحميل الزائد للشبكة كل يوم في منتصف النهار .تشير القمم المسطحة إلى التحميل الزائد للوصلة حتى لو كانت أقل من الإستطاعة النظرية القصوى للوصلة، وقد تدل في هذه الحالة على أن عرض الحزمة المتاح عملياً من قبل مزود الخدمة يقل عن المتوقع.

8-3 الاختبارات :

- اختبار التكامل :

تم التحقق من عمل التوافق بين أجزاء النظام ،و عمل النظام ككل بشكل صحيح .

- اختبار إقرار الصلاحية :

بعد الانتهاء من اختبار التكامل قمنا بالتأكد من أن التطبيق لم يغفل أي من الوظائف المطلوبة ،و الأهداف المرجوة من النظام.

- اختبار الأداء :

أكثر ما يهمنا في تطبيقات من هذا النوع هو إعطاء نتائج دقيقة قدر الإمكان و بأكبر سرعة ممكنة ،و عدم استهلاك قدرة الشبكة في عمليات المراقبة.

- الجودة :

حققنا من خلال مشروعنا بعضاً من عوامل الجودة التي نستعرضها فيما يلي :

1- الصحة :

أي تحقيق البرنامج للمواصفات المطلوبة .

حاولنا قدر الإمكان التأكد من صحة النتائج التي يعطيها نظامنا , و ملاءمتها فعلاً لما يطلبه الزبون

2 – الاستخدامية :

أي الجهد المطلوب لتعلم استخدام النظام.

تم تصميم النظام بشكل بسيط و واجهات رسومية واضحة User Friendly بحيث يكون سهل التعامل ،بالإضافة إلى تزويد المشروع بدليل المستخدم الذي يشرح كيفية استخدام النظام.

3 – تحمّل الخلل :

تمت من خلال رسائل الخطأ التي تعالج الأخطاء المختلفة (مثلا حالة انقطاع الاتصال أو عدم القدرة على تفسير نتائج المراقبة).

8-4 الجدوى الاقتصادية للمشروع :

لما كان تيار المنافع يتدفق خلال عدد من السنوات (عمر المشروع) و تيار التكاليف يتركز فى السنوات الأولى من المشروع و الجزء الأكبر منه ينفق قبل بدء تشغيل المشروع ،لذلك يجب أن نأخذ بعين الاعتبار عند حساب الجدوى المالية تكاليف وعوائد تتحقق بعد تنفيذ المشروع

التكاليف فى أي مشروع تنقسم إلى :

أ – تكاليف استثمارية :

وهى كافة ما ينفق على المشروع منذ بداية التفكير فى عملية الاستثمار حتى دورة التشغيل العادية الأولى . وتمثل هذه التكاليف إنفاق استثماري يستفيد منه المشروع لأكثر من سنة خلال عمر المشروع . وتشمل جميع تكاليف تأسيس وإنشاء المشروع بالإضافة إلى فوائد القروض طويلة الأجل.

ب- تكاليف جارية :

وتشمل جملة التكاليف قصيرة الأجل ، تكاليف مستلزمات التشغيل لدورة واحدة و تكاليف الأجور و المرتبات و الطاقة.

الخطة الزمنية للمشروع :

المرحلة	الفترة المخططة	الفترة الفعلية	عدد الساعات الفعلية
جمع المتطلبات	3	5	40
الدراسة التحليلية	7	8	64
تصميم النظام	7	6	48
دراسة وتشغيل أدوات العمل	8	12	96
تحقيق و تنفيذ النظام	25	32	256
التجارب	3	2	16
صيانة و تطوير النظام	7	9	72
التوثيق	6	8	64
الإجمالي			652 ساعة

بدأ العمل بالمشروع في 3\11\2008 و انتهى العمل في 27\5\2009.

المخطط السابق على اعتبار العمل 8 ساعات يوميا و على فترات متقطعة.

و بالتالي عدد ساعات العمل الكلي 652 و باعتبار أن الشهر 208 ساعات (26 يوم X 8 ساعات) و الراتب الشهري 24000 ل.س بالتالي فإن تكلفة الموظف الواحد :

التكلفة الكلية = 24000 * (652 / 208) = 75230 ل.س

	الكلفة الافرادية	العدد	الكلفة الكلية
المصادر البشرية	75230	2	150460
الآلات	20000	2	40000
الأدوات	0	0	OpenSource..!
الإجمالي			190460 ل.س

و لكن الجدوى الاقتصادية للمشروع لا تقاس بتكلفته فقط إنما بالعوائد أيضا ،حيث تظهر فائدة المشروع على المدى الطويل حيث يقي الشبكة من العديد من المشاكل التي كانت تحدث مسبقا (و هذا ما لمسناه فعلا) مما يوضح أهمية المشروع في عمل الشركة من حيث استمرارية الخدمة و جاهزية الشبكة و معرفة مكان العطل فور حدوثه أو إمكانية التنبؤ بالعطل قبل حدوثه ،و هذا ما كنا قد أشرنا إليه في بداية المشروع.

بالنسبة للتكاليف الجارية :هي تكاليف الطاقة الكهربائية اللازمة لتشغيل الجهاز الذي يعمل عليه النظام (حيث يجب أن يعمل بشكل مستمر).و لا يحتاج النظام إلا موظف واحد لمتابعته هو مدير الشبكة ،و بالتالي لن نحتاج إلى موارد بشرية إضافية.

بالمقارنة مع نظم إدارة الشبكات المغلقة و غير المجانية و التي نشتريها من بعض الشركات الكبرى (Cisco Works) فإن هذا النظام مجدي ،و ذلك لأنه أقل كلفة من جهة (قد تصل كلفة النظام المغلق إلى عشرة أضعاف) ،كما أنه قد لا يلائم الشبكة الخاصة بالشركة ،و لا يمكن إجراء أي تعديل عليه ،بالإضافة إلى كلفة التدريب عليه ،و قد يلزمه برمجيات خاصة مما يزيد الكلفة ..

يجب الموازنة دائما بين التكاليف و الاحتياجات ، أي لا نشتري نظام شامل يفوق احتياجاتنا ،و تكون كلفته عالية.

الخاتمة

تم إنجاز المشروع وفق منهجية عمل محددة ،تنطوي على دراسة شاملة للمشروع ،تبدأ بتحديد الأهداف ،ثم تحديد المبادئ التقنية ،يليها انتقاء الأدوات ،و أخيرا التصميم و التنفيذ ،بالإضافة إلى دراسة الجدوى الاقتصادية للمشروع.

و قد واجهتنا العديد من الصعوبات و التحديات التي حاولنا تخطيها و الاستفادة منها ،و لكن بالمقابل أدركنا واقع العمل ،و استطعنا توظيف المعلومات النظرية و العملية التي كنا قد تعلمناها خلال سنواتٍ خمس في بناء مشروع متكامل.

و بحكم عملنا بالعديد من الأدوات ،و على نظام لينكس ،فقد أتاح لنا ذلك اكتساب العديد من المهارات و الخبرة في مجال نظم التشغيل و الشبكات.

و نطمح مستقبلاً إلى تطوير مشروعنا ليتيح العديد من الخدمات الاضافية :

- إمكانية معالجة بعض حالات العطل التي تحصل في الشبكة من قبل النظام بشكل تلقائي.
- بناء واجهات تفاعلية للنظام ،تسمح للمستخدم بإضافة خدمات من خلال واجهة رسومية.
- تطوير النظام بحيث يصبح نظام موزع ،قادر على مراقبة العديد من الشبكات.

الملاحق

Practical Extraction Report Language

PERL

تعريف :

هي أداة خطاطّة قوية Powerful Scripting Tool يمكننا استخدامها لإدارة الملفات و إنشاء التقارير و تحرير النصوص و تأدية العديد من المهام عند استخدام نظام التشغيل Linux.

تستخدم أيضا لكتابة العديد من البرمجيات الخاصة بـ Linux و بالتالي لا يمكن لمدير نظام أن يتخيل إتمام مهمته بدون PERL.

تم تصميمها من قبل لاري وول Larry Wall عام 1987 و تابع تطويرها بنفسه بشكل مستمر حتى الآن.

ميزات PERL:

تمتلك PERL القوة و المرونة الموجودة في لغات البرمجة العالية المستوى مثل لغة c .

- كأي لغة من اللغات الخطّاطة فهي لا تحتاج مترجما Compiler خاصا أو رابطا خاصا Linker كي تعمل ،فقط اكتب البرنامج و أخبر PERL لتشغله ،لذا تعتبر PERL مثالية لإنتاج حلول سريعة لمسائل برمجية صغيرة.
- تزود بكافة الخصائص المتوفرة في اللغات الخطّاطة مثل awk & sed بالإضافة إلى العديد من الميزات التي لا تقدمها هاتين اللغتين.
- سهلة التعلم و لا تحتاج خبرة كبيرة في البرمجة .
- تمتلك قدرات كبيرة جدا في مجال التعابير المنتظمة و تمتلك تسهيلات كبيرة على مستوى التفحص.
- هناك مجتمع كامل على الانترنت يعمل في حقل تطوير مجتزئات Modules تعمل بالتكامل مع برامج PERL ،و يمكن أن نجد العديد من المجتزئات التي تلبي احتياجاتنا بشكل سريع و مختبر من قبل العديد من المطورين.

عادة تتواجد PERL في المسار التالي:

/usr/local/bin/perl

إذا :

تعتبر PERL الخيار الأقوى للعمل ضمن بيئة Linux خاصة عند التعمال مع الملفات و التقارير حيث تستطيع في ثلاثة أسطر برمجية فتح ملفين و نسخ أحدهما للآخر !

مثال:

```
#! /usr/bin/perl –w
Print “Hello World!”
```

في بداية كل ملف PERL يجب كتابة مسار الـBIN للبرنامج بالشكل التالي :

```
#! /usr/bin/perl –w
```

هذا التعليق يدل على أن هذا الملف هو ملف مكتوب بلغة PERL و هذا التعليق يؤخذ بعين الاعتبار من قبل مفسر PERL.

الخيار W– يخبر المفسر كي يصدر تحذيرات حول البرنامج المكتوب.

التعابير المنتظمة

Regular Expressions

تعريف :

التعابير المنتظمة و يشار إليها بالاختصار التالي regexp أو regex هي عبارة عن أدوات لتحديد القواعد المتبعة في تحرير النصوص . حيث يعتمد العديد من محركات البحث في معالجة محتوى النص على نموذج محدد من التعابير المنتظمة، إضافة إلى أن معظم لغات البرمجة و منها PERL تدعم التعابير المنتظمة لمعالجة السلاسل المحرفية، حيث تتضمن بنيتها محرك Engine قوي للتعامل مع التعابير المنتظمة.

المفاهيم الأساسية :

التعبير المنتظم يعتبر قالب بنائي لتراكيب بعض الجمل، حيث يستخدم للتحقق من توافق الجمل مع التركيب البنائي الذي تم تحديده للتعبير.

فمثلاً يتم استخدام التعبير المنتظم للتحقق من صحة بناء عنوان البريد الإلكتروني ، حيث لا يوجد بريد الكتروني إلا ويتكون من @ وجزء قبلها يمكن ان يكون احرف أو ارقام أو العلامات التالية _ و كذلك جزء آخر بعد العلامة يتكون من أحرف و أرقام وعلامات خاصة ثم نقطة يليها امتداد الموقع امّا com أو net أو غيرها من الامتدادات الحالية.

الرموز الخاصة :

تنقسم الرموز إلى مجموعتين تبعاً لمكان وجودها، المجموعة الأولى الرموز خارج الاقواس المربعة ، والثانية الرموز داخل الأقواس المربعة.

توضيح : الاقواس المربعة هي الاقواس [و] .

المجموعة الأولى – خارج الأقواس المربعة :

^

لتحديد بداية التعبير.

الرمز ^ أو كما يسميها البعض الثمانية، أو علامة الأس في البرمجة، توضح ان ما بعدها يعتبر هو بداية السطر أو الجملة وأن لا شيء يسبقه.

$

لتحديد نهاية التعبير.

علامة الدولار $ ، توضح انتهاء التعبير و أن لا شيء متوقع ان يكون بعد ذلك.

^devpedia$

التعبير السابق لن يتطابق إلا مع الكلمة devpedia ، حيث لن يتطابق مع أي كلمة أخرى مثل wdevpedia أو حتى devpediaw، لأن الأخيرتين يسبقها بحرف أو تزيد عليها حرف في آخرها ولإتاحة إمكانية أن تحتوي الكلمة أحرف سابقة أو لاحقة كل ما عليك هو الاستغناء عن رمزي التحديد أو أحدهما كما ترغب.

.

لتعيين مكان لرمز مجهول.

النقطة يمكن أن تعبر عن أي حرف أو رمز غير معلوم مسبقا، لنوضح ذلك عبر التعبير التالي:

^.at$

نلاحظ أن الخانة الأولى في التعبير كانت هي النقطة ، وهنا يمكن أن يطابق التعبير الكلمات التالية : cat, hat, fat و أي كلمات تتكون من ثلاثة أحرف الثاني والثالث هنا هو at ، أو حتى يمكن أن يكون الحرف الأول مسافة أو رمز فسوف يكون التعبير متطابق مع الكلمة.

كما أنه يمكن أيضاً وضع العديد من النقاط حسب الرغبة وحسب عدد الاحرف غير المعلومة في الكلمة ، حيث يمكن ان يكون التعبير السابق بالشكل التالي:

^..at$

وهي في هذه الحالة تحتمل جميع الكلمات التي تتكون من أربعة أحرف وتنتهي بـ at مثل الكلمة : heat. وهكذا...

[

لبداية تصنيف رموز جديد.

]

لإنهاء تصنيف الرموز.

الأقواس المربعة السابقة مهمة بالنسبة للتعابير المنتظمة ، و وظيفتها جمع عدد من الرموز التي يحتمل وجودها ضمن الجمل التي يتم مطابقتها معها.

مثلاً:

^[abcdef]$

هذا التعبير يستخدم للكشف عن حرف واحد ليتحقق من تواجده ضمن المجموعة السابقة أم لا ، أمّا عن كيفية الكشف عن أكثر من حرف (أي كلمة مثلاً) فعلينا تكرار القوس المربع بما يحويه لأكثر من مرة كما يلي:

^[abcdef][abcdef][abcdef][abcdef]$

حيث أن هذا يمثل كلمة تتكون من أربعة أحرف لا تخرج أحرفها عن a, b, c, d, e, f مع ملاحظة أنه يمكن تغيير القوس الأول بالإحتمالات الخاصة بالحرف الأول و القوس الثاني كذلك بما يخص الحرف الثاني ، وهكذا.

|

لوضع عدة اختيارات.

في بعض الأحيان تكون هناك عملية تخيير بين كلمتين يمكن أن تكون موجودة لا ثالث لهما ، في هذه الحالة يمكن استخدام رمز الخط العمودي | لهذه المهمة.

^com|net$

هذا التعبير سوف يطابق أي واحدة من الكلمتين com أو net .

(

لبداية نمط فرعي.

)

لإنهاء نمط فرعي.

و الأنماط الفرعية يتم وضعها للفصل بين بعض الأنماط المختلفة فتكون اختيارية لعملية الترتيب ، أو تكون إجبارية لعملية التحديد أو ازالة بعض المشاكل.

{a,b}

قوس التكرار : و هذا القوس يوضع بجوار القوس المربع أو القوس الدائري أو حتى الحروف والرموز و الأرقام ، وكذلك بجوار النقطة لتفادي المشكلة عندما لا نعلم مرات التكرار تحديداً.

حيث a هو أقل عدد مرات للظهور ، فيمكن أن يكون صفراً (0) حيث تكون احتمالية الظهور تبدأ من صفر إلى b وهو الحد الأعلى لإحتمالية الظهور ، فيمكن إزالته وتركه فارغاً لجعل الحد الأعلى غير محدود.

هناك اختصارات متعارف عليها بدلاً من كتابة كامل الاقواس و هي:

*** = {0,}**

النجمة، وتعني أن ما سبقها قد يكون غير موجود أو موجود بعدد مرات غير محدود.

+ = {1,}

إشارة الجمع، وتعني أن ما سبقها على الاقل يكون موجود مرّة واحدة أو اكثر.

? = {0,1}

علامة الاستفهام، وتعني أنه إنّ وجد ، فهو موجود لمرّة واحدة فقط.

\

علامة التجاهل.

بعض الأحيان ، نجبر على استخدام بعض الرموز الخاصة بالتعابير المنتظمة ليس لتأدي العمل المناط بها ، و إنما لتكون كـعنصر ثابت، كأستخدام علامة الدولار داخل النص في عملية التدقيق ان المبلغ بالدولار وينتهي برمز الدولار ، في هذه الحالة يجب أن تسبق علامة الدولار بالرمز \ حتى يتم تجاهل علامة الدولار من مهمتها واعتبارها جزء من النص.

المجموعة الثانية – داخل الاقواس المربعة:

\^-

والرموز الاخرى تعتبر كـ ثوابت ، أي كأنها احرف أو ارقام.

\

علامة التجاهل.

نفس وظيفة علامة التجاهل السابقة تماماً ، ولكن داخل الأقواس المربعة.

^

رمز النفي.

ويجب أن يكون مباشرة بعد قوس الابتداء [، وإلاّ اعتبر رمز ثابت مثل الحروف والأرقام.

وظيفته : يرفض النص الذي يحتوي على الرموز الموجودة داخل القوس المربع ، أي يقوم بعكس دوره.

-

رمز المدى.

يستخدم بدلاً من كتابة جميع الاحرف ، فيكتب على الشكل a-z ، وكذلك للأرقام فتكتب 0-9 .

تنصيب برنامج nagios :

بعض الأدوات التي يمكن تحميلها من شبكة ال Internet :

- الملف nagios-3.0.2.tar.gz
- الملف nagios-plugins-1.4.6.tar
- الملف NSClient++-Win32-0.3.5
- NRPE Addon

سنقوم بشرح إعدادات بعض الأدوات التي تمكننا من إعداد nagios و إعداد بعض المكتبات التي تمكننا من مراقبة بعض الخدمات

إعداد nagios في بيئة Linux open Suse:

في البداية نحتاج إلى وجود بعض ال packages مثل

- Apache2
- C/C++ development Libraries

1- إنشاء حساب:

Become the root user
Su –l

Create a new *nagios* user account and give it a password

/usr/sbin/useradd -m nagios
passwd nagios

Create a new *nagios* group. Add the nagios user to the group.

/usr/sbin/groupadd nagios
/usr/sbin/usermod -G nagios nagios

Create a new *nagcmd* group for allowing external commands to be submitted through the web interface.
Add both the nagios user and the apache user to the group

/usr/sbin/groupadd nagcmd
/usr/sbin/usermod -G nagcmd nagios
/usr/sbin/usermod -G nagcmd wwwrun

2- ترجمة وتركيب nagios (Compile and Install nagios)

mkdir ~/downloads
cd ~/downloads

Extract the Nagios source code tarball.
tar xzf nagios-3.0.2.tar.gz
cd nagios-3.0.2

Run the Nagios configure script, passing the name of the group you created earlier like so:
./configure --with-command-group=nagcmd

Compile the Nagios source code.
make all

Install binaries, init script, sample config files and set permissions on the external command directory:
make install
make install-init
make install-config
make install-commandmode

Don't start Nagios yet - there's still more that needs to be done...

3- تعديل الإعدادات (Customize configuration)

ملفات الإعدادات تنصب تحت المسار التالي

/usr/local/nagios/etc

نحن بحاجة لإجراء تعديل بسيط قبل المتابعة حيث نحرر الملف contacts.cfg الموجود في المسار

/usr/local/nagios/etc/objects/contacts.cfg

ونقوم بتغيير الإيميل ووضع الإيميل الذي سنتلقى عليه التنبيهات

vi /usr/local/nagios/etc/objects/contacts.cfg

4- تكوين واجهة الويب (configure Web Interface)

Install the Nagios web config file in the Apache conf.d directory.
make install-webconf

Create a *nagiosadmin* account for logging into the Nagios web interface. Remember the password you assign to this account - you'll need it later.
htpasswd2 -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

Restart Apache to make the new settings take effect.
service apache2 restart

5- ترجمة وتنصيب Nagios plugins :

Extract the Nagios plugins source code tarball.
cd ~/downloads
tar xzf nagios-plugins-1.4.11.tar.gz
cd nagios-plugins-1.4.11

Compile and install the plugins.
./configure --with-nagios-user=nagios --with-nagios-group=navies

make
make install

6- Start Nagios

Add Nagios to the list of system services and have it automatically start when the system boots.
chkconfig --add navies
chkconfig nagios on

Verify the sample Nagios configuration files.
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

If there are no errors, start Nagio
service nagios start

7- Login to the Web Interface

You should now be able to access the Nagios web interface at the URL below.
You'll be prompted for the username (*nagiosadmin*) and password you specified earlier.
http://localhost/nagios/

يمكن الأن الضغط على Service Detail لمشاهدة الأشياء المراقبة على جهازك المحلي.

تنصيب NRPE :

يجب تنصيب الرزمة nagios-plugins-1.4.6.tar.gz ونتع الخطوات التالية

1- إنشاء حساب:

Become the root user. You may have to use sudo -s on Ubuntu and other distros.
su –l

Create a new nagios user account and give it a password.
/usr/sbin/useradd nagios
passwd navies

2- تنصيب برامج nagios :

Create a directory for storing the downloads.
mkdir ~/downloads
cd ~/downloads

Extract the Nagios plugins source code tarball.
tar xzf nagios-plugins-1.4.6.tar.gz
cd nagios-plugins-1.4.6
Compile and install the plugins.
./configure
make
make install

The permissions on the plugin directory and the plugins will need to be fixed at this point, so run the following
commands.
chown nagios.nagios /usr/local/nagios
chown -R nagios.nagios /usr/local/nagios/libexec

3- تنصيب NRPE daemon :

```
cd ~/downloads
```

Extract the NRPE source code tarball.
tar xzf nrpe-2.8.tar.gz
cd nrpe-2.8
Compile the NRPE addon.
./configure
make all
Install the NRPE plugin (for testing), daemon, and sample daemon config file.
make install-plugin
make install-daemon
make install-daemon-config
Install the NRPE daemon as a service under xinetd.

```
make install-xinetd
```

Edit the */etc/xinetd.d/nrpe* file and add the IP address of the monitoring server to the *only_from* directive.

only_from = 127.0.0.1 <nagios_ip_address>
Add the following entry for the NRPE daemon to the */etc/services* file.
nrpe 5666/tcp # NRPE

Restart the xinetd service.
service xinetd restart

في هذا الملحق نورد أمثلة عن تحقيق الأغراض التي تم شرحها في فصل تصميم النظام:

Host:

```
define host{
host_name                       bogus-router
alias                            Bogus Router #1
address                         192.168.1.254
parents                         server-backbone
check_command                   check-host-alive
check_interval                  5
retry_interval                  1
max_check_attempts              5
check_period                    24x7
process_perf_data               0
retain_nonstatus_information    0
contact_groups                  router-admins
notification_interval           30
notification_period             24x7
notification_options            d,u,r
}
```

HostGroup:

```
define hostgroup{
hostgroup_name                  novell-servers
alias                           Novell Servers
members                         netware1,netware2,netware3,netware4
}
```

Service:

```
define service{
host_name                       linux-server
service_description             check-disk-sda1
check_command                   check-disk!/dev/sda1
max_check_attempts              5
check_interval                  5
retry_interval                  3
check_period                    24x7
notification_interval           30
```

notification_period 24x7
notification_options w,c,r
contact_groups linux-admins
}

Servicegroup:

define servicegroup{
servicegroup_name dbservices
alias Database Services
members ms1,SQL Server,ms1,SQL Server Agent,ms1,SQL DTC
}

Contact:

define contact{
contact_name M.Mohammad
alias Moustafa Najm
host_notifications_enabled 1
service_notifications_enabled 1
service_notification_period 24x7
host_notification_period 24x7
service_notification_options w,u,c,r
host_notification_options d,u,r
service_notification_commands notify-by-email
host_notification_commands host-notify-by-email
email Moustafa-MN@localhost.
address1 xxxxx.xyyy@neotech.com
address2 555-555-5555
can_submit_commands 1
}

ContactGroup:

define contactgroup{
contactgroup_name novell-admins
alias Novell Administrators
members Moustafa,Mohamad
}

Timeperiod:

```
define timeperiod{
timeperiod_name          misc-single-days
alias                      Misc Single Days
2008-01-28               00:00-24:00 ;   January 28th, 1999
monday  3                00:00-24:00 ;   3rd Monday of every month
day 2                    00:00-24:00 ;   2nd day of every month
february 10              00:00-24:00 ;   February 10th of every year
february -1              00:00-24:00 ;   Last day in February of every year
friday -2                00:00-24:00 ;   2nd to last Friday of every month
thursday -1 november   00:00-24:00 ;     Last Thursday in November of every year
}
```

Command:

```
define command{
command_name     check_pop
command_line                    /usr/local/nagios/libexec/check_pop   -H
$HOSTADDRESS$
}
```

Servicedependency:

```
define servicedependency{
host_name                       WWW1
service_description              Apache Web Server
dependent_host_name             WWW1
dependent_service_description    Main Web Site
execution_failure_criteria        n
notification_failure_criteria     w,u,c
}
```

Serviceescalation:

```
define serviceescalation{
host_name                       nt-3
service_description              Processor Load
first_notification              4
last_notification               0
notification_interval            30
contact_groups                   all-nt-admins,themanagers
}
```

Hostdependency:

```
define hostdependency{
host_name                       WWW1
dependent_host_name             DBASE1
notification_failure_criteria    d,u
}
```

Hostescalation:

```
define hostescalation{
host_name                   router-34
first_notification          5
last_notification           8
notification_interval       60
contact_groups              all-router-admins
}
```

Hostextinfo:

```
define hostextinfo{
host_name          netware1
notes              This is the primary Netware file server
notes_url          http://webserver.localhost.localdomain/hostinfo.pl?host=netware1
icon_image         novell40.png
icon_image_alt     IntranetWare 4.11
vrml_image         novell40.png
statusmap_image    novell40.gd2
2d_coords          100,250
3d_coords          100.0,50.0,75.0
}
```

Serviceextinfo:

```
define serviceextinfo{
host_name            linux2
service_description   Log Anomalies
notes                Security-related log anomalies on secondary Linux server
notes_url  http://webserver.localhost.localdomain/serviceinfo.pl?host=linux2&service=Log+Anomalies
icon_image           security.png
icon_image_alt       Security-Related Alerts
}
```

المراجع

1. **Network Management Principles and Practice - Mani Subramanian**
2. **Simple Network Management Protocol, tutorials by Dr. Andreas Steffen**
3. *الشبكات في الدول النامية : ترجمه إلى العربية أنس طويلة*

4. **http://www.adsh2007.com/vb/Arabic_CCNA/CCNA_ARABIC_4/**
5. **http://wndw.net/**
6. **http://www.nagios.org**
7. **http://www.nagiosexchange.org**
8. **http://nagioswiki.org/wiki/Addon:NagiosGrapher**
9. **http://sourceforge.net/project**
10. **http://nagios.demo.netways.de/**
11. **http://www.novell.com/coolsolutions/feature/19843.html**
12. **http://nsclient.org/nscp/**
13. **http://www.linux-ar.org/forum/**
14. **http://www.tech-faq.com/firewall.shtml**
15. **http://en.wikipedia.org/wiki/**
16. **http://www.nagioscommunity.org/wiki/**
17. **http://nrpe.org**
18. **www.itrainonline.org/itrainonline/mmtk**
19. **http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems**