بيئات الإدارة العامة

هناك عدد من التنظيمات مهتمة بمشكلة إدارة الشبكة و الخدمة، و هي غير محددة ، و لكن من المهم تقديم تلك التي لها أهمية أكبر بهذا المجال.

فيما يلي الجدول التالي البيئات الأساسية للإدارة الموجودة بالأسواق:

Environnements de gestion	Organismes et consortiums initiateurs
SNMP v1,v2,v3	IETF (Internet engineering task force)
TMN/CMIP	UIT-T et l'ISO
DMI/WEBM/CIM/DEN	DMTF (Distributed management task force) et DEN (Directory enabled networking)
Corba/OMA	OMG (Object management group) et TMF (Telecommunication management forum)
JMX	Consortium Java
DCE/DME	OSF (Open software fundation)

الهيئات و الاتحادات العالمية و ضعوا العديد من الحلول و سنذكر منها الأكثر انتشاراً:

- **SNMP** (Simple Network Management Protocol) :وضع من قبل IETF عام 1988 من أجل إدارة بيئات TCP/IP . هذه البيئة حالياً أصبحت الأكثر انتشاراً و استخداماً.
- **TMN/CMIP** وضعت على التوالي من قبل UIT-T و ISO . بنية TMN (Telecommunjcation Management Network) و بروتوكول CMIP (Common Management Information Protocol) .هذه البيئة مبنية لمجال إدارة شبكة الاتصالات.
  إن CMIP تقدم نسخة محسنة ل SNMP بينما TMN أدخلت إطار عمل ل:تخطيط – تنصيب (تركيب) – صيانة – استخدام – إدارة شبكة الاتصالات و الخدمات المشاركة.

إن التعقيد في هاتين TMN/CMIP كان الكابح لامتدادهم في الشبكات الصغيرة، و هم بالمقابل يستخدموا تقريباً في الشبكات الكبيرة الآلية (Operators-Operateurs).

- **WEBM/DMI/CIM** وضعت بواسطة صانعي مواقع العمل و المخدمات المجمعة في اتحاد DMTF (Desktop management task force) و المسماة حالياً (Distributed management task force) . هدفها هو دفع عملية الإدارة حتى موقع العمل و المخدمات الحاوية لكل عناصر نظام المعلومات للشركة. العديد من البيئات طرحت لذلك و منها:
  - **DMI** (Desktop management Interface)
  - **CIM** (Common information model)
  - **WBEM** (Web based management)

- (Directorie enabled network) **DEN**

هذه البيئات تقدم مجموعات مختلفة، و هي في طور أن تكون متكاملة في نفس الهيكلية.

- DME (Distributed Management Environnement) وضعت بواسطة صانعي البرامج المجمعة في OSF (Open Softwarw Fundation) ،هذه الهيئة وجهت باتجاه إدارة مواقع UNIX
- OMA (Object management architecture) وضعت من قبل اتحاد OMG (Object management group) ، هذه الهيئة للإدارة مرتكزة على الهيكلية المسماة Cobra (Common objet request broker architecture) و تعتزم وضع حل لإدارة تشتمل على مختلف الشركات المتقاربة.
- JMX (Java™ management extensions) وضعت بواسطة اتحاد Java ، و هي أيضاً تعتزم وضع حل أوحد بالمقارنة مع حلول SNMP/TMN/WEBM

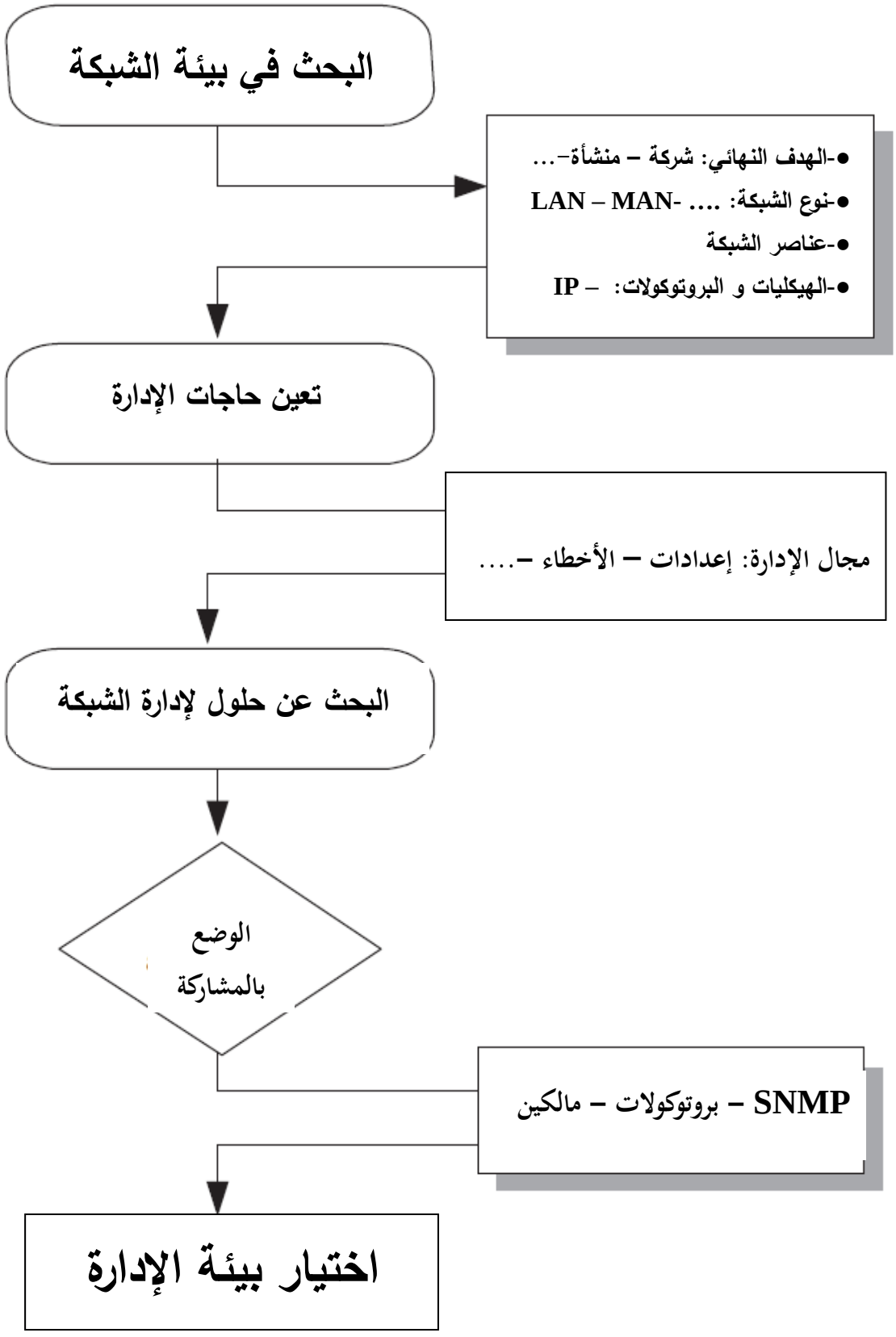
إدراك بيئة إدارة

إدراك أو فهم بيئة إدارة هي العملية التي تسمح بالوصول لحل هيكلي و تقني لنظام الإدارة. هذا يفرض بشكل إجباري دقة كبيرة في اختيار من يشرف على تنفيذ البيئة و الذي يضمن عدم السقوط و الفشل في تحقيق الأهداف و الأسعار. لذلك هذا مهم جداً تحديد الخطوات التي من خلالها مدراء الشبكة يستطيعون الاستناد عليها للحصول على اختيار جيد للهيكليات و التقنيات، و التي بدورها تؤمن حاجات المنشأة.

الخطوة المفترضة تمر عبر: التعريف المسبق للحاجات، و من ثم تحديدها و الانتقاء للخدمات الضرورية، و كذلك اختيار تقني دقيق، و في النهاية وضع صيغة للاستثمار.

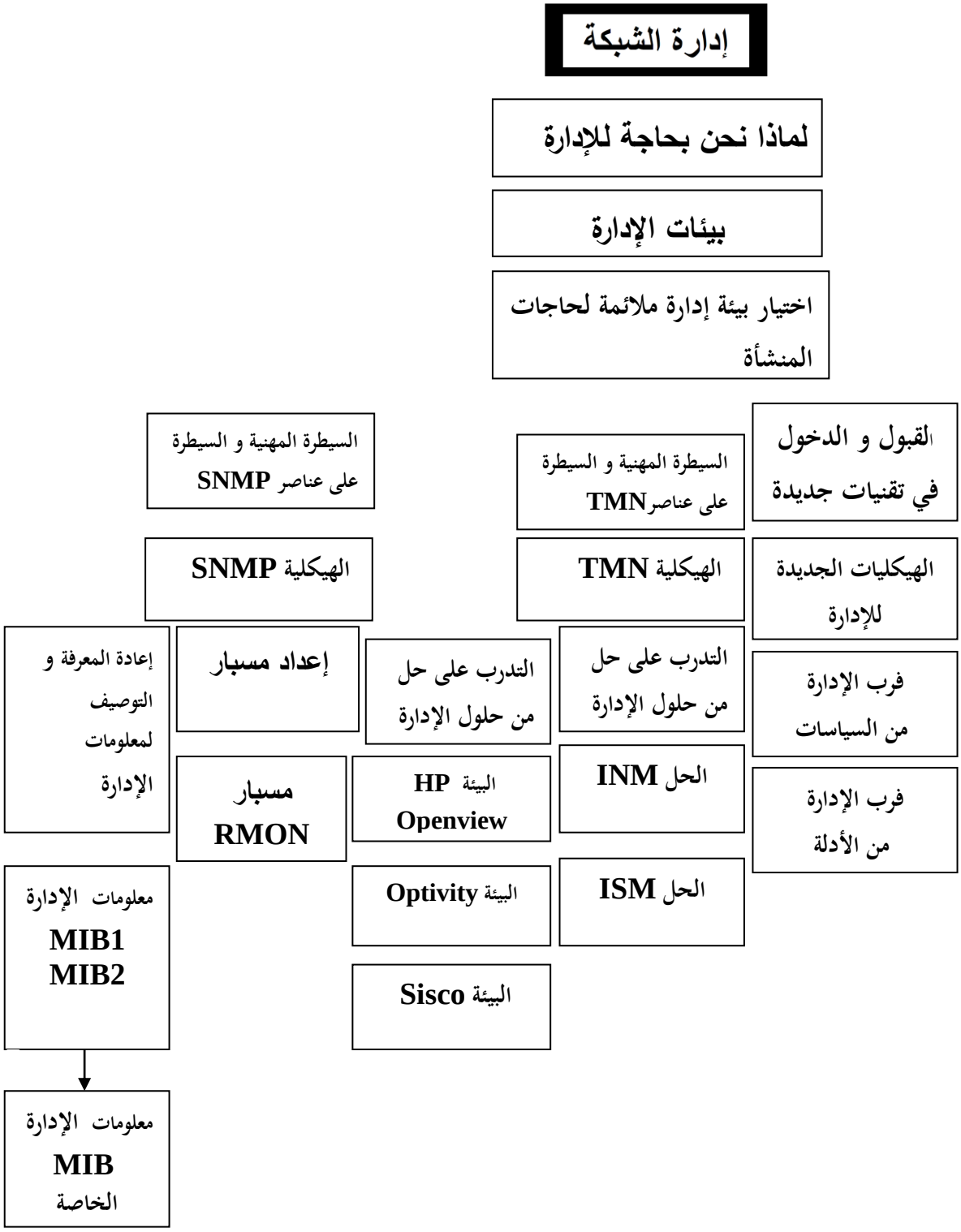
هذه العملية تشتمل على خمس مراحل كما هو مبين بالشكل أدناه.

من أجل إمكانية تنفيذ المراحل المختلفة، فإن مدير الشبكة يتوجب عليه أن يمتلك المعرفة و الإلمام الجيد للعمل، و الذي يسمح له بالسيطرة التكنولوجية و بمعرفة أية حالات تكون ملائمة للمستخدم، و في الختام من أجل أن يكون هو نفسه أن يصنع الخيارات المثالية و ذلك بهدف وضع حلوله في الموقع.



شكل : مراحل إدراك و فهم بيئة الإدارة للشبكة

من أجل ذلك نحن نعرض لمنهجية تعلم التي تسمح للقارئ بتحديد العلوم الأساسية للإجابة عن حاجات الإدارة لبيئة شبكته. و هذه المنهجية يمكن توصيفها وفق الشكل التالي:



شكل: منهجية التعلم في مجال إدارة الشبكة

عناصر الشبكة و بيئات الإدارة

كما نعرف فإن إدارة الشبكة تتضمن القيادة عن بعد لعناصر الشبكة، من أجل ذلك فإنه يجب الضم لعناصر الشبكة بيئة الإدارة القادرة على القيادة عن بعد. على سبيل المثال المركزات شبكة Ethernet و الراوترات يمكن أن يكونوا مقادين بواسطة بيئة الإدارة SNMP .

نفس الشيء بالنسبة للتجهيزات الوسيطية للشبكة، فإنه من الممكن قيادة المخدمات، قواعد البيانات أو التطبيقات. عملياً فإن بيئة الإدارة SNMP يمكن أن تقود كل التجهيزات الموصولة بالشبكة التي تنظم تتابعية عمل ما يسمى SNMP و التي تكون قادرة على إطلاق عمليات المراقبة.

أغلب التجهيزات الموصولة بالشبكة تدعم و تتحمل SNMP و يمكن أن تكون خاضعة للإدارة عن بعد. هذه التجهيزات يكونون موصفين بمتحولات أو بمتغيرات توصف حالتهم و كذلك بارامترات إعداداتهم.

مع ذلك بعض التجهيزات ليس من الضروري أن تنظم بشكل حتمي بSNMP و لكن يمكن أن تكون مخصصة بواسطة نوع آخر، و بالتالي بهذه الحالة ليس من السهل قيادة هذه التجهيزات، و مثال ذلك الأغلبية الكبرى للمركزات الغير فعالة (Hubsالغير الفعالة) لا يمكن أن تكون مقادة عن بعد.

لذلك في البداية سيكون إجباريا على مدير الشبكة أن يستطيع تحديد هوية تجهيزاته التي يمكن أن تقاد أم لا. سنقدم أدناه العناصر البرمجية و العتاد التي يمكن أن تكون مقادة أم لا .

أصناف التجهيزات و التطبيقات الممكن قيادتها:

- المورديمات لا تكون إلا قليلاً منظمة بSNMP
- المركزات (Hubs) الغير فعالة لا تكون بشكل عام منظمة بSNMP
- المبدلات و المركزات الفعالة تكون غالباً منظمة بSMNP
- الجسور تكون غالباً منظمة بSMNP
- الراوترات تكون بأغلبيتها مجهزة بمنظمتها
- المضاعفات لا تكون إلا قليلاً جداً منظمة بSMNP
- العبارات (gateways) تكون مجهزة أغلب نماذج SNMP و واقية النار تستخدم موديل المعلومات DEN
- المبدلات الأوتوماتيكية التلفونية تكون مجهزة بمنظمات إدارتها TMN و بيئات الإدارة سيكونون بيئات خاصة
- المبدلات الضوئية تكون مجهزة بمنظمات و بيئات إدارة التي ستكون بيئات خاصة
- المخدمات تكون غالباً منظمة بSMNP و لكن نحن نقودها بشكل أساسي بواسطة بيئة OSF بحالة UNIX
- بعض التطبيقات مثل قواعد المعطيات التي لها SNMP الخاص بها

حالما تم تحديد و تعريف التجهيزات ، فإنه سيكون ضرورياً عمل مشاركة لنماذج التجهيز و بيئات الإدارة التي يمكن قيادتها.

Environnements de gestion	SNMP	TMN/CMIP	WBEM/CIM
Les modems	×		
Les commutateurs	×		
Les ponts (bridge)	×		
Les routeurs	×		
Les multiplexeurs	×		
Les passerelles (gateways)	×		×
Les autocommutateurs téléphoniques		×	
Les commutateurs optiques		×	
Les serveurs			×
Les applications	×		×
Les postes de travail			×

الهيكليات التقنية و بيئات الإدارة

قبل اختيار بيئة الإدارة فإنه يتوجب علينا أن نكون قادرين على معرفة الهيكليات التقنية للشبكة التي نريد إدارتها.

مع الملاحظة أن كل بيئات الإدارة لا يمكنها إدارة كل أصناف الهيكليات التقنية . لذلك يجب أن نشرك بيئات الإدارة بالهيكليات التقنية.

المشاركات

الجدول التالي يظهر مختلف المشاركات بين بيئات الإدارة و الهيكليات التقنية:

Environnements de gestion	SNMP	TMN/CMIP	Propriétaires
Architecture technologique IP	×		×
Architecture technologique ATM	×	×	×
Architecture technologique Relais de trames	×		×
Architecture technologique X25		×	×
Architecture technologique Sonet		×	×
Réseau téléphonique		×	×
Architecture technologique IPX	×		×

- بيئة الإدارة SNMP مستخدمة في أغلب الحالات مع الهيكلية التقنية IP ، و بسبب شعبية البروتوكول IP .
- بيئة الإدارة TMN غالباً مستخدمة مع: الهيكلية SONET – شبكة النقل – شبكة الصوت PSTN (Public Service Telephony Network) – كذلك أيضاً الهيكلية ATM .
- بعض الهيكليات التقنية تستخدم بشكل أساسي بيئات مطلقة مثل : الهيكليات ATM, SONET, PSTN تكون مقادة بواسطة بيئات مطلقة.

المنهجية المعتمدة على الأهداف لإدارة و مراقبة الشبكة

بمفهوم آخر، يتطلّب ضمان توفير خدمةٍ معيّنةٍ ضمن الشبكة القيام باستمرارٍ بمراقبة و إدارة العديد من جوانب نظام الاتصالات. **تعتبر القدرة على تمييز المعلومات القيّمة والحصول على البيانات من النظام شرطين أساسيين للتمكّن من اتخاذ القرارات الصحيحة.**

لسوء الحظ، لن تتمكّن البيانات وحدها من حل المسألة، فالبيانات ليست بالضرورة معلومات، والحصول على المعلومات لا يعني بالضرورة أيضاً حصولك على المعرفة.

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

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

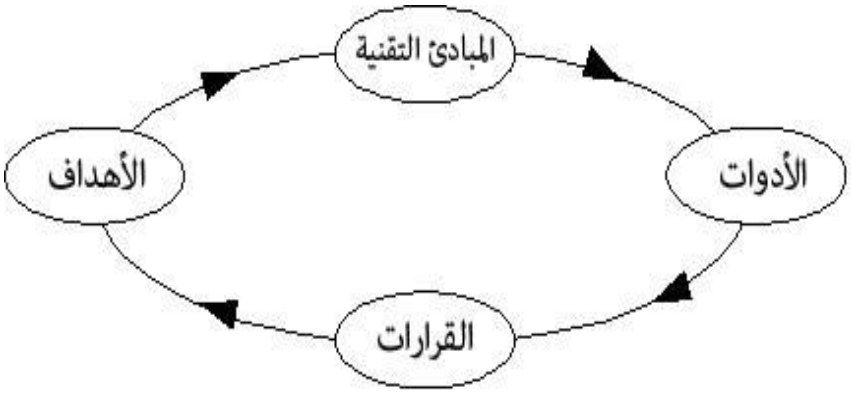
من الأخطاء الشائعة في عالم مزوّدي خدمات الإنترنت ISPs تبنّي أسلوبٍ يعتمد على الأدوات tool-centric في اتخاذ القرار. على سبيل المثال، عند تركيب أداة إدارةٍ معيّنةٍ في نظامٍ لإدارة الشبكة يتم اتخّاذ جميع القرارات بناء على إمكانيّات هذه الأداة عوضاً عن أهداف وأولويّات مزوّد الخدمة. لذلك هنا سنعتمد أسلوباً مبنيّاً على الأهداف goal-centric في إدارة الشبكة. تقدّم هذه الوحدة (بعكس الأسلوب المعتمد على الأدوات) منهجيّةً لإدارة الشبكة تبدأ بتحديد أهدافٍ واضحةٍ لإيجاد الأدوات الصحيحة.

الأهداف في مقابل مراقبة البيانات

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

يعتبر تحديد:

(١) **الهدف** أمراً أساسيّاً للتفكير (٢)**بالمبادئ التقنيّة** المطلوبة للحصول على المعلومات الضروريّة من النظام. يمكّننا تحديد المبادئ التقنيّة من اختيار تصميم وتركيب (٣) **الأدوات** اللازمة. توفّر المعلومات التي ستقدّمها هذه الأدوات معرفةً إضافيّةً لإتخاذ (٤) **القرارات** الصائبة و المناسبة. و الشكل التالي يبين الترابط بين البارامترات الأربعة المبينة أعلاه:



شكل: يظهر المنهجيّة المعتمدة على الأهداف لمراقبة (إدارة) الشبكة

I-مراقبة أهداف الخدمة Monitoring Service Goals

سنحاول في سبيل استعراض هذا الأسلوب المنهجي لمراقبة و لإدارة الشبكة تحديد ثلاثة أهدافٍ مختلفةٍ شائعةٍ في أيّة شبكةٍ و خصوصاً اللاسلكيةٍ:

١. توفير النفقات عبر تخفيض استخدام عرض الحزمة الدولي
٢. توفير جودة أفضل لخدمات نقل الصوت عبر بروتوكول الإنترنت VoIP
٣. إدارة الخدمة وتوسّع الشبكة

تؤثّر الأهداف في الشبكات اللاسلكية (تماماً كما هي الحال في أيّ نظام اتصالات آخر) على جميع طبقات نموذج OSI المعياري. لذلك يتوجّب علينا لضمان جودة الخدمة أن نستوعب جميع جوانب شبكة الاتصالات وليس تلك المتعلّقة بالشبكة اللاسلكية وحسب.
تظهر الجداول التالية كيفيّة استخدام هذه الأهداف للمبادئ التقنيّة الأساسيّة وكيف يتطلّب كلٌ من هذه الأهداف تجميّع المعلومات من جميع طبقات نموذج OSI المعياري لنظام الاتصالات.

١. توفير نفقات عرض الحزمة الدولي

الطبقة	المبدأ التقني
التطبيقات Application	التخزين المؤقت Caching، كشف / إيقاف الرسائل غير الموجّهة Spam والفيروسات (المصافي الديكارتيّة Bayesian Filters)
النقل Transport	تشذيب سيل البيانات Traffic Shaping (مبادئ الإصطفاف Queuing Principles) محاسبة حركة البيانات Traffic Accounting (SNMP، Promisc)
الشبكة Network	التحكّم بالوصول إلى الشبكة Network Access Control (جدار النار Firewalling) تشذيب سيل البيانات محاسبة حركة البيانات Traffic Accounting (SNMP، Promisc)
التحكّم بالوصول إلى الميديا Media Access Control	التحكّم بالوصول إلى الشبكة اللاسلكية Wireless Access Control تجميع بيانات الطبقة الثانية اللاسلكية (SNMP)

جدول ١: المبادئ التقنيّة (وطبقات نموذج OSI الموافقة) التي يمكن استخدامها لتوفير عرض الحزمة الدولي

٢. توفير جودة أفضل لخدمة نقل الصوت عبر بروتوكول الإنترنت VoIP

الطبقة	المبدأ التقني
التطبيقات Application	
النقل Transport	تشذيب سيل البيانات Traffic Shaping (مبادئ الإصطفاف Queuing Principles) محاسبة حركة البيانات Traffic Accounting (SNMP، Promisc)
الشبكة Network	تشذيب سيل البيانات Traffic Shaping (مبادئ الإصطفاف Queuing Principles) محاسبة حركة البيانات Traffic Accounting (SNMP، Promisc)
التحكّم بالوصول إلى الميديا Media Access Control	تجميع بيانات الطبقة الثانية (SNMP) تخفيض التأخير اللاسلكي Wireless Latency

جدول 2: المبادئ التقنيّة (وطبقات نموذج OSI الموافقة) التي يمكن استخدامها لتوفير جودةٍ أفضل لخدمة VoIP

٣. إدارة الخدمة وتوسّع الشبكة

الطبقة	المبدأ التقني
التطبيقات Application	Virus/Spam, SQL (موازنة الخدمات Service Balancing)
النقل Transport	تجميع إحصاءات بروتوكولات TCP/UDP موازنة استخدام الجدران الناريّة Firewall Balancing
الشبكة Network	تجميع إحصاءات طبقة بروتوكول الإنترنت IP مبادئ التوجيه Routing Principles
التحكّم بالوصول إلى الميديا Media Access Control	تجميع بيانات الطبقة الثانية (SNMP)

جدول 3: المبادئ التقنيّة (وطبقات نموذج OSI الموافقة) التي يمكن استخدامها لإدارة الخدمة وتوسّع الشبكة

يؤدّي الإخفاق في إعداد أيٍّ من الطبقات بالشكلِ الأمثل إلى التأثير على أداء الخدمة بأكملها. فعلى سبيل المثال: تؤثّر المستويات المرتفعة من الحزم المعطوبة في الشبكة اللاسلكية على أداء بروتوكول TCP بأكمله مما يؤدّي إلى تأخّرٍ ملحوظٍ في تخديم مستخدمي تطبيقات الزمن الحقيقي Real-time.

لا تتجلى الصعوبة في استيعاب جميع طبقات الاتصال المتعلقّة بالنظام وحسب، بل من ضرورة الإلمام بالتداخلات والتفاعلات المختلفة بين هذه الطبقات أيضاً.

تماماً كما في جميع أنظمة الاتصالات، يمكننا بناء شبكةٍ لاسلكيةٍ بسهولة، أما بناء شبكةٍ لاسلكيةٍ ذات أداءٍ جيّدٍ فيتطلّب منا الكثير من الوقت والخبرة. هذا هو المبدأ الذي بني عليه نجاح الإنترنت بأكملها!

II- المبادئ التقنيّة Technical Principles

سنقوم بشرح المبادئ التقنيّة التي تعتمد عليها أدوات مراقبة (إدارة) الشبكة، و لكن قبل مناقشة هذه الأدوات. يمكن تطبيق بعض هذه المبادئ بأشكالٍ عدّةٍ لتحقيق أهدافٍ مختلفةٍ. تستخدم الأدوات عادةً مجموعة جزئيّةً من إمكانيّات مبدأٍ تقنيٍّ.

حيث أنه سيساعدنا استيعاب المبادئ التقنية بالإضافة إلى اختيار الأدوات الصحيحة على تصميم أداةٍ جديدةٍ في حال عدم توفّر أداةٍ جاهزةٍ تلبّي كل متطلباتك.

II-١ – . بروتوكول إدارة الشبكة البسيط SNMP

بروتوكول إدارة الشبكة البسيط Simple Network Management Protocol (SNMP) هو بروتوكولٌ للإدارة والصيانة صمّم خصيصاً للشبكات الحاسوبيّة وتجهيزات الشبكة الإفراديّة.صمم بنهاية الثمانينات من القرن الماضي، وتم وضعه بشكل قياسي خلال التسعينات من القرن الماضي. و هو يقدم ميزات كثيرة بالنسبة للبروتوكولات الأخرى، و هو يقدم واجهة تعامل لكل المواد أو التجهيزات للشبكة، و بالتالي هو الأكثر ملاءمةً . لذلك أصبح المرجع فيما يخص إدارة الشبكات. فهمه و استيعابه يسمح بحل و إدارة كل المعوقات السابقة، و لكن النسخة الأولى من بروتوكول SNMP(SNMPv1) كانت تعاني من بعض الثغرات: فقدان التسلسلية– الأداء– ألسرية–... .

كل هذه المشاكل أجبرت الباحثين على إنتاج أجيال متطورة عن الجيل الأول ، حيث طورّت من قبل فريق عمل هندسة الإنترنت IETF و التي سميت SNMPV2 و ذلك في عام 1993 ، و حيث أن العديد من المؤلفين قد وضعوا العديد من الأشكال لهذا الجيل مثل: **SNMPv2* - SNMPv2u - SNMPv2c - SNMPv2p**

النسخة الأكثر استخداماً هي **SNMPv2c** ، و لكن الميل و الإتجاه ينعكس وذلك مع دخول العام 1997، حيث تم إنتاج الجيل SNMPv3. هذا الجيل أو هذه النسخة تضيف على السابقة سرية أفضل

بكثير، و كذلك إدارة تراتبية أفضل بكثير، و لكن تعقيداتها أدخلت العديد من المشاكل و خصوصاً أن الاستخدام يلزمه دقة أكثر من النسخ السابقة.

تقديم مبسط لهذا البروتوكول

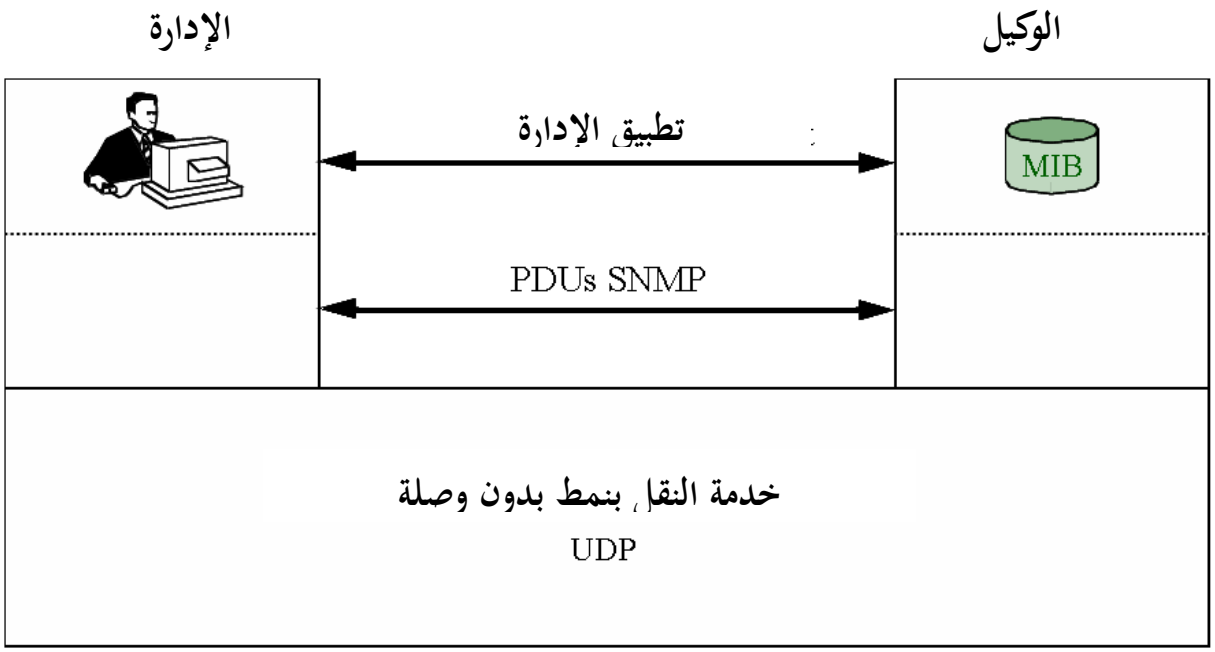
SNMP وهو من عائلة (Internet protocol) TCP/IP ، لذلك يمكن استخدامه في كل الشبكات من نوع Internet ، و هو يستثمر طاقة بروتوكول النقل UDP ☹الحيز له عنوان المنبع و التوزيع – يعمل بنمط بدون و صلة – ....

هناك منفذين أو بابين مخصصان للبروتوكول SNMP :

- باب أو منفذ لطلبات وكيل SNMP
- باب أو منفذ لسماع الإنذارات المخصصة لمحة الإدارة.

مبدأ العمل

بروتوكول SNMP مرتكز على وجود محطة إدارة ، والمدير له دور التحكم بالإتصال بواسطة هذا البروتوكول مع الوكيل أو الزبون. الوكيل يكون بطريقة عامة واجهة SNMP مركبة على العتاد المخصص ليكون مقاد عن بعد(كما هو مبين بالشكل التالي).

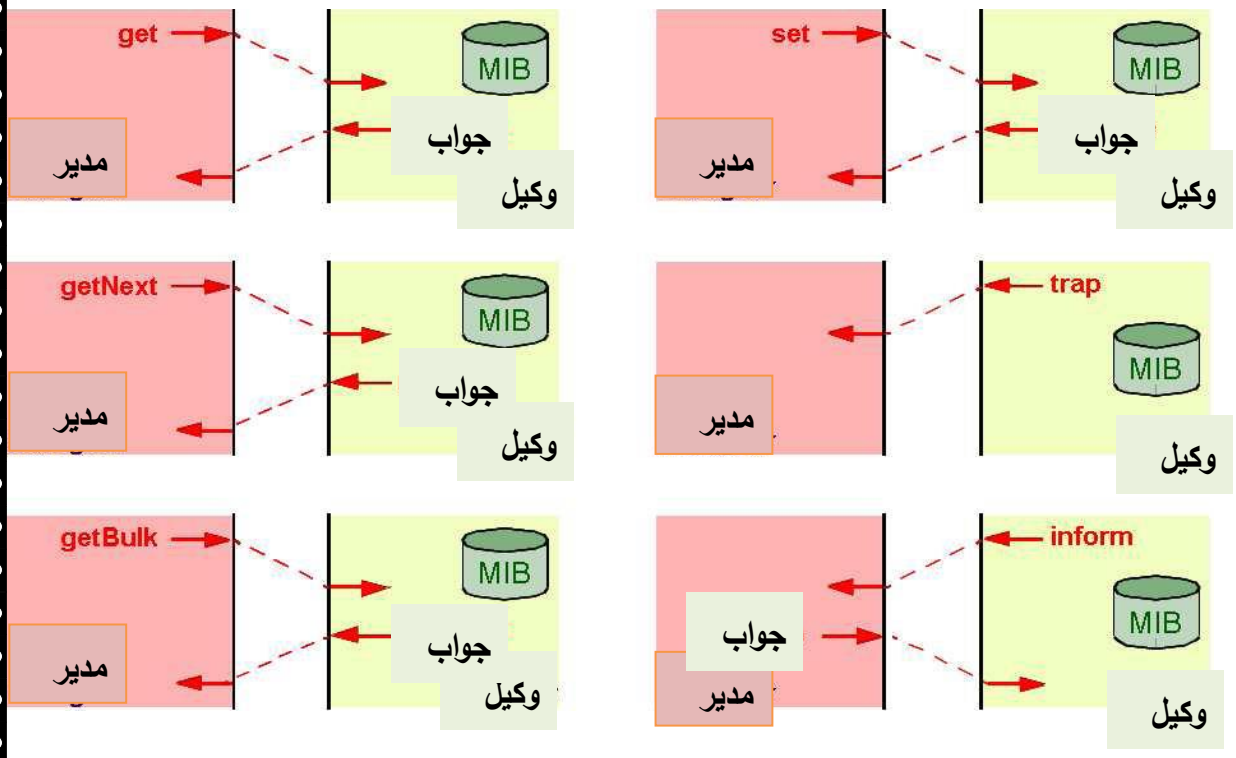


شكل: عمل SNMP

البروتوكول SNMP مكون من العديد من الأوامر المختلفة:

- Get : هذا الأمر يرسل من قبل المدير باتجاه الوكيل بهدف طلب معلومات من الوكيل، هذا يكون في حالة أن سماحية الطلب مثبتة أو مؤكدة، عندها ترسل إلى المدير القيمة المطابقة للمعلومة المطلوبة.

- Getnext : هذا الأمر مرسل من المدير إلى الوكيل بهدف طلب المعلومات التالية من الوكيل (الحصول على قائمة كل متغيرات أو متحولات الوكيل). إذاً نستخدم هذا الأمر بعد الطلب Get .
- Getbulk : هذا الأمر مرسل من قبل المدير للوكيل، من أجل معرفة كثير من المتغيرات: هذه تتجنب تنفيذ العديد من طلبات Get على التوالي، و هذا مل يحسن الأداء.
- Set : هذا الأمر مرسل من المدير إلى الوكيل بهدف تحديد قيمة متحول واحد لوكيل خاضع للإدارة. هذه تسمح بتنفيذ التعديلات على العتاد.
- Trap : بما أن حادثة خاصة تصل إلى العميل (توصيل– تعديل قيمة متحول – ...)، هذه تكون حساسة لإرسال ما نسميه : Trap ، بما أن الرسالة موجهه لمحطة الإدارة ، فإنه باستطاعتها معالجتها و احتمال التصرف نتيجة ذلك.
- Inform : في بعض الحالات ممكن أن يكون مفيداً للوكيل الحصول على جواب على Trap التي أرسلها و ذلك للحصول على تأكيد على أن التي أرسلها تم استلامها و حللت



شكل: ملخص لأوامر البروتوكول SNMPV2

و بالتالي يعتمد تجميع المعلومات على بنيّة المخدّم / الزبون حيث يقوم برنامجٌ زبون بطلب المعلومات الإحصائيّة والبيانات الخاصّة من تجهيزات الشبكة البعيدة. SNMP هو بروتوكول طبقة التطبيقات Application Layer المستخدم لتبادل المعلومات.

يحتوي كل جهازٍ يدعم بروتوكول SNMP على قاعدة بياناتٍ تدعى MIB (قاعدة معلومات الإدارة Management Information Base). تحتوي قاعدة البيانات هذه على المعلومات التي يتم تجميعها أثناء عمل الجهاز. يمكن القول بأنّ بروتوكول SNMP يشكّل آليّة إرسال الطلبات واستقبال الردود عن معلومات الإدارة من العناصر الفعّالة في الشبكة.

تكمن أهمّ نقاط القوّة في بروتوكول SNMP والتي يعود إليها الفضل الرئيسي في شعبية وانتشار هذا البروتوكول في دعمه للتفاعل بين تجهيزات الشبكة المختلفة Interoperability. تتفاوت تجهيزات الشبكة التي تدعم وكلاء SNMP Agents من الموجّهات، الحواسب والجسور إلى المودمات والطابعات.

كما تتيح مرونة بروتوكول SNMP إمكانيّة توسيعه ليتضمنّ بياناتٍ خاصةٍ بكل جهاز. يقوم معظم منتجو التجهيزات اللاسلكية بتضمين مجموعةٍ خاصّةٍ Proprietary من معلومات الشبكة اللاسلكية في قواعد معلومات الإدارة MIB ضمن منتجاتهم، قد يعني ذلك ولسوء الحظ أنّه وعلى الرغم من قيام جميع المنتجين بتضمين دعم البروتوكول SNMP فإنّ آليّات تجميع بعض أنواع معلومات الشبكة اللاسلكية قد تختلف فيما بينها.

يوفّر منتجو تجهيزات الشبكة اللاسلكية لزبائنهم عادةً "أدوات إدارةٍ" خاصّةٍ بهم تستخدم بروتوكول SNMP للتواصل مع التجهيزات التي ينتجونها. يعتبر تركيب أدوات الإدارة المختلفة من عدة منتجين أمراً معقدّاً جدّاً لأنّ هذه الأدوات نادراً ما تكون مفتوحة المصدر. قد يتمثّل الخيار الأفضل بقيامك بكتابة نظام إدارة الشبكة اللاسلكية الخاص بك.

يحتوي بروتوكول SNMP أيضاً على نقاط ضعفٍ عدّةٍ. لا يسهل استخدام هذا البروتوكول على المبرمجين نظراً لقواعد الترميز المعقّدة التي يستخدمها كما يؤخذ عليه قلّة فاعليته وإضاعته لعرض حزمة الشبكة. تتضمّن كلّ حزمة SNMP العديد من حقول البيانات عديمة الأهميّة كما يتم ترميز متغيرات SNMP بأساليب تجعل حجم حزمة البيانات كبيراً بشكلٍ غير مبرر.

علينا الإنتباه إلى النقاط التالية عند تركيب أي نظام مراقبةٍ يعتمد على بروتوكول SNMP:

١. يؤدّي استخدام بروتوكول SNMP إلى زيادة الضغط على الشبكة. حاول تخفيض هذا الضغط باتخاذ القرارات الصائبة.

٢. لا يدعم بروتوكول SNMPv1 تشفير مرحلة التحقق من الهويّة، إنتبه لكلمات السر الخاصّة بك.
٣. يستهلك بروتوكول SNMP جزءاً من قدرة المعالج CPU ضمن تجهيزات الشبكة.

II-٢ – محاسبة حركة البيانات Traffic Accounting

يستخدم مبدأ محاسبة حركة البيانات لمراقبة إحصاءات سير البيانات ضمن الشبكات الحاسوبيّة. تعتبر المعلومات التي يتم تجميعها من خلال محاسبة حركة البيانات ذات أهميّةٍ فائقةٍ عند اتخاذ القرارات المتعلّقة بتنظيم الشبكة، كشف الأعطال ومراقبة نشاطات الحواسب المختلفة.

من المعلومات الشائعة التي تقوم محاسبة حركة البيانات بتجميعها:

- عدد الحزم والبايتات Bytes.
- إحصاءات توزّع البروتوكولات (النوع، الأوقات، %).
- أخطاء بروتوكول الإنترنت IP Checksum Errors.
- إكتشاف الأجهزة النشطة.
- حركة البيانات بين الأجهزة.

يمكن تجميع المعلومات المتعلّقة بحركة البيانات ضمن الشبكة بطرقٍ عدّةٍ. من أكثر هذه الأساليب شيوعاً تشغيل بروتوكول SNMP في جميع موجهّات وجسور الشبكة. يستخدم بروتوكول SNMP لتجميع المعلومات المتعلّقة بالشبكة بشكلٍ **نشط Active**، لأنّ الحصول على هذه المعلومات يتطلّب تبادل حزم SNMP فيما بين الموجّهات والجسور.

يمكن أيضاً الحصول على المعلومات المتعلّقة بحركة البيانات عبر الشبكة دون الحاجة إلى زيادة الضغط على الشبكة عبر إباحة التنصّت على البيانات المنتقلة ضمن الشبكة. يعتبر التنصّت على الشبكة آليةً **خاملةً Passive** لا تتطلّب استخدام بروتوكول SNMP على الإطلاق. إلا أنّ استخدام هذا الأسلوب محدودٌ لسببين: ينبغي أن تكون قادراً على الوصول المباشر إلى البيانات المنتقلة عبر الشبكة إضافةً إلى استهلاك الكثير من قدرة المعالج CPU لتجميع واستيعاب حجم المعلومات المارّة عبر قناة الإتصال.

II-٣ – تشذيب سيل البيانات Traffic Shaping

وهو أسلوبٌ يستخدم للتحكّم بسير البيانات ضمن الشبكة بغية ضمان مستوىً محدد من الأداء. ينتج تشذيب سيل البيانات عن تفعيل قواعد ضبط طوابير البيانات في الموجّهات. يمكنك عبر إدارة هذه القواعد بحكمة تغيير أداء الشبكة فيما يتعلّق بـ :

١. التأخير وإدارة الإزدحام Latency and Congestion Management
٢. إدارة عرض الحزمة Bandwidth والعدالة Fairness.

يعمل تشذيب سيل البيانات عادةً في طبقة بروتوكول الإنترنت IP Layer عبر تغيير أساليب إصطفاف وتوصيل الحزم في الموجّهات. يؤثّر تشذيب البيانات ضمن طبقة بروتوكول الإنترنت على توزيع الموارد في الوصلة اللاسلكية.

من الجدير بالذكر أنّ بعض منتجي تجهيزات الشبكة اللاسلكية المعتمدة على معايير IEEE 802.11 قد حاولوا تطبيق آليّاتٍ مشابهةٍ في جسور الشبكات اللاسلكية عبر تعديل طريقة أداء طبقة IEEE 802.11 MAC التقليديّة، إلا أنّ غالبيّة هذه الحلول ظلّت خاصّةً بالمنتج مما لا يضمن توافقيّة هذه التجهيزات مع تلك المنتجة من قبل الآخرين.

قامت شركة Proxim على سبيل المثال بتطبيق آليّة تصويتٍ خاصّةٍ تدعى (WORP) لدعم اختناق عرض الحزمة غير المتناظر Asymmetric Bandwidth Throttling والذي يتيح تعديل سرعة استقبال أو إرسال البيانات من قبل المستخدم. تقوم آليّة WORP بتوزيع استطاعة الشبكة عبر تخصيص منافذ زمنيّةٍ وجيزةٍ لجميع المستخدمين الراغبين بإرسال أو استقبال البيانات وتعطي كلاً منهم دوراً لاستخدام عرض الحزمة.

II-٣ – ١: ضبط طوابير البيانات والتأخير Queuing disciplines and latency

إذا أردت الحفاظ على توافقيّة التجهيزات بين المنتجين المختلفين ولم ترغب بتطبيق آليةٍ خاصّةٍ بمنتجٍ ما ضمن شبكتك يتوجّب عليك حينها تطبيق تشذيب سيل البيانات على مستوى بروتوكول الإنترنت IP.

يتم تشذيب سيل البيانات عبر التأثير على طريقة ترتيب الحزم ضمن طوابير وتوصيل هذه الحزم عبر العناصر الفعّالة في الشبكة. تطبّق قواعد ضبط طوابير البيانات على الحزم أثناء عمليّة نقل هذه الحزم. تختلف قواعد ضبط طوابير البيانات تبعاً لأولويّة حزمة البيانات، مرسل هذه الحزمة أو وضعية الطابور في تلك اللحظة.

تعتبر قواعد ضبط طوابير البيانات المطبّقة على البيانات الخارجة من الشبكة أكثر أهميّةً من تلك المطبّقة على البيانات الواردة. يتوجّب إيلاء هذه القواعد عنايةً خاصّةً لأنّ عنق الزجاجة Bottleneck (أو النقطة الأكثر ضيقاً في الشبكة) تقع غالباً عند الوصلة الخارجيّة Uplink (أو الوصلة التي تربط الشبكة بالإنترنت)، حيث يتم ضغط سيل البيانات المنتقلة ضمن الشبكة المحليّة ضمن أنبوبٍ واحدٍ.

يتألّف طابور الحزم من حاجزٍ Buffer يقوم بحفظ حزم البيانات حتى يتجاوز حجم البيانات المستقبلة في الموجّه قدرته على الإرسال. ينبغي على الموجّه إهمال الحزم التي سترد بعد امتلاء الحاجز لعدم توفّر مساحةٍ في الذاكرة تكفي لتخزينها، مما قد يؤدّي إلى إعادة إرسال هذه الحزم من حاسب المستخدم.

إذا علقت حزمةٌ ما على الحاجز لفترةٍ طويلةٍ جدّاً فإنّ صلاحيتها ستنتهي مما يستدعي المرسل إلى إعادة إرسال هذه الحزمة، وبالتالي زيادة الحمل على الموجّه المضغوط أساساً.

يؤدّي الضغط الشديد على الحواجز إلى ظهور تأخيرٍ شديدٍ في الشبكة عند ازدحام الوصلة الخارجيّة. تتسبب محاولات إعادة الإرسال الناتجة عن إنتهاء صلاحيّة الحزم في جعل المشكلة أكثر سوءاً.

يكمن أحد حلول مشكلة التأخير في منح بعض الحزم أولويةً أعلى من غيرها. تحصل الحزم التي تتطلب التفاعل مع المستخدم (كتطبيقات Remote Console، الألعاب والدردشة على الإنترنت ونقل الصوت عبر بروتوكول الإنترنت VoIP إلخ) على أولويةٍ أعلى من تطبيقاتٍ مثل HTTP، FTP أو SMTP والتي تعمل تفضّل الحصول على عرض حزمةٍ أوسع عن حصولها على تأخيرٍ أقل. يمكن تطبيق هذه السياسة في منح الأولويات عبر استخدام قواعد تعتمد على نوع الخدمة (ما هي بوابة TCP التي تستخدمها الحزمة).

في الحالات التي تستخدم فيها عدّة بروتوكولاتٍ نفس بوابة TCP بشكلٍ إفتراضيٍّ (مثل بروتوكولي SSH و SCP) ينبغي تطبيق سياسةٍ أخرة لتنظيم الطوابير. يستخدم كلٌّ من بروتوكولي SSH و SCP البوابة ٢٢ بشكلٍ إفتراضيٍّ. يعتبر حجم حزم البيانات في بروتوكول SSH صغيراً جدّاً (يحتوي كلٌّ منها على بضعة أحرفٍ فقط) في حين يستخدم بروتوكول SCP حزماً ذات حجمٍ أكبر بكثير. يتطلب بروتوكول SSH (بعكس نظيره SCP) التفاعل مع المستخدم، مما قد يدعوك إلى تطبيق سياساتٍ مختلفةً لكلٍّ منهما. يمكن التأثير على الخدمات المختلفة التي تستخدم نفس البوابة عبر آليةٍ تقوم بتحديد الأولويّة بناءً على حجم الحزمة.

II-٣ – ٢ : إدارة عرض الحزمة عبر التحكّم باصطفاف الحزم Bandwidth Management by Packet Queuing

قد تمكنّك إدارة عرض الحزمة عبر التحكّم باصطفاف الحزم من ضمان جودة الخدمة Quality of Service (QoS) في شبكتك. تعني إدارة عرض الحزمة تحديد عرض الحزمة التي يمكن استخدامها من قبل حاسبٍ معينٍ أو لشبكةٍ فرعيّةٍ معينةٍ أو تحديد السرعة المتوفّرة لنوع محددٍ من الخدمات.

يمكن تطبيق إدارة عرض الحزمة لأسبابٍ متعددة. فقد ترغب في منع عملية نقل ملفٍ كبيرٍ من التأثير على جودة الخدمة المتوفّرة لبعض الحواسب ضمن الشبكة والتي تتطلّب عرض حزمةٍ أقل. قد ترغب أيضاً في توزيع موارد شبكتك بشكلٍ عادلٍ بحيث يحصل جميع المستخدمين على عرض حزمةٍ ملائمٍ تبعاً للثمن الذي دفعه كلٌ منهم للحصول على هذه الخدمة.

للقيام بذلك يمكن تطبيق قواعد ضبط طوابير البيانات الفئوي Classful Queuing أو غير الفئوي Classless Queuing في الموجّهات.

يمتلك ضبط طوابير البيانات الفئوي هيكليّةٍ هرميّةٍ تحتوي على علاقات أبويّةٍ Parent / Child (تعتمد على الفئات) وميراثٌ من الخصائص. ينتمي كل مضيفٍ Host إلى فئةٍ معينةٍ يتم ضمنها تحديد الخصائص مثل عرض الحزمة الأقصى Maximum Bandwidth، خوارزمية الإصطفاف Queuing Algorithm، سقف الحد Ceiling Limit (لاستعارة عرض الحزمة) وأرقام البوابات.

يمكن باستخدام إدارة عرض الحزمة وضبط طوابير البيانات الفئوي تخصيص عرض حزمةٍ محددٍ لبروتوكولٍ ما بناءً على نوع هذا البروتوكول (بوابة TCP المستخدمة). يمكن أيضاً تخصيص عرض حزمةٍ محددٍ لعددٍ من المضيفين (بناءً على الفئة التي ينتمون إليها) لضمان عدالة توزيع موارد الشبكة.

تعتبر آليّة دلو البطاقات الهرميّة Hierarchical Token Bucket (HTB) من أكثر أساليب ضبط طوابير البيانات الفئوي شيوعاً. تستخدم هذه الآليّة لتوزيع حزم البيانات على فروعٍ مختلفةٍ لنموذج الشجرة الهرميّة تبعاً للأولويّة ولعرض الحزمة. يمكن إنشاء فئاتٍ فرعيّةٍ لإتاحة تشارك عرض الحزمة غير المستخدم بين أعضاء الفئة الواحدة (أبناء نفس هذه الفئة الفرعيّة). تستخدم هذه الآليّة أيضاً للتحكّم بعرض الحزمة الصادر ضمن وصلةٍ خارجيّةٍ. تقوم هذه الآليّة عند تطبيق قواعد ضبط الطوابير على كلّ حزمةٍ واردةٍ باستخدام وصلةٍ فيزيائيّةٍ واحدةٍ لتمثيل عدّة وصلاتٍ أبطأ وبالتالي إرسال الأنواع المختلفة من الحزم عبر وصلاتٍ إفتراضيّةٍ مختلفةٍ.

تقوم قواعد ضبط طوابير البيانات غير الفئويّة (على عكس نظيرتها الفئويّة) بمجرّد إعادة جدولة حزم البيانات، تأخيرها أو رميها.

من الآليّات الشائعة لضبط طوابير البيانات غير الفئويّة طابور العدالة العشوائيّة Stochastic Fairness Queue (SFQ) والتي تستخدم عند امتلاء الوصلة الخارجيّة. لا تقوم هذه الآليّة بأيّ تشذيبٍ لسيل البيانات بل يقتصر عملها على جدولة إرسال الحزم بحيث تحصل جميع الوصلات على حصةٍ متساويةٍ من عرض الحزمة. لا تؤثّر هذه الآليّة على حركة البيانات عندما لا تكون الوصلة ممتلئةً.

تحاول آلية طابور العدالة العشوائيّة SFQ توزيع فرص إرسال البيانات إلى الشبكة بشكلٍ عادلٍ فيما بين عددٍ إعتباطيٍّ من سيول البيانات.

II-٤ – المصافي الديكارتيّة[١] Bayesian Filters

من المبادئ التقنيّة الأخرى التي يمكنك استخدامها لتحسين أداء شبكتك "المصافي الديكارتيّة Bayesian Filters". تستخدم المصافي الديكارتيّة لتطبيق أنظمة مكافحة الرسائل التجاريّة المرسلة عشوائيّاً Spam والتي تقوم بحساب إحتمال كون الرسالة مرسلةٍ عشوائيّاً بناءً على محتوياتها.

تعتمد تقنيّة المصافي الديكارتيّة على فكرة أنّ تصفية الرسائل العشوائيّة ممكنٌ بناءً على احتمال وجود كلماتٍ معيّنةٍ أو مجموعاتٍ من الكلمات التي تشير إلى أنّ هذه الرسالة مرسلةٌ عشوائيّاً في حين تشير كلماتٌ أخرى إلى أنّ هذه الرسالة طبيعيّة.
المصافي الديكارتيّة قادرةٌ على التكيّف، أي أنّها قادرةٌ على التعلّم من خبرتها للتمييز بين محتوى الرسائل الجيّد والسيء مما يؤدّي إلى زيادة ذكائها ووثوقيتها مع مرور الوقت.

تعتمد المصافي الديكارتيّة (شأنها شأن غالبيّة أنظمة تصفية الرسائل المرسلة عشوائيّاً) على المحتوى. تستبدل هذه المصافي القائمة اليدويّة المستخدمة لتحديد خصائص الرسائل المرسلة عشوائيّاً Spam (وهي إحدى أهم نقاط الضعف في الأنظمة الأخرى) بقائمةٍ من الكلمات التي تقوم المصفاة بنفسها ببنائها عبر تحليل المحتوى شائع الإستخدام. يتم بناء القائمة الأوليّة عبر تحليل مجموعة من الرسائل المعروفة المرسلة عشوائيّاً ومجموعةٍ من الرسائل المعروفة الطبيعيّة للحصول على تصنيفٍ أوليٍّ للتمييز بين المحتوى الجيّد والسيء.

[١] تأتي تسميّة "المصافي الديكارتيّة" نسبةً إلى عالم الرياضيّات الإنكليزي توماس ديكارت Thomas Bayes

لا يقل تصنيف المحتوى الجيّد أهميّةً عن تصنيف المحتوى السيء. كلما تكيّفت المصافي مع طبيعة مستخدمٍ ما كلّما صعب على مرسلي الرسائل العشوائيّة تخطّي هذه المصافي.

يزداد حجم القائمة الأوليّة بعد بنائها كلما استخدمت المصفاة بشكلٍ أكبر. ستتكيّف هذه المصافي بشكلٍ شخصيٍّ مع المستخدم لأنّها ستتعلّم من خلال تعليمات هذا المستخدم لدى حدوث خطأ في تصفيّة الرسائل الواردة.

تقوم المصافي الديكارتيّة (بعكس الأنواع الأخرى من المصافي المعتمدة على المحتوى) بتفحّص محتوى الرسالة بأكملها في حين تقوم المصافي الأخرى بتفحّص ترويسة الرسالة وحقل الموصوع فقط. تتفحّص المصافي الديكارتيّة (بالإضافة إلى نص الرسالة) أجزاءً أخرى مثل:

- الترويسة (المرسل ومسار الرسالة)
- نصوص HTML المضمّنة (كالألوان وغيرها)
- أزواج الكلمات والتعابير
- المعلومات التوصيفيّة Meta Information.

ننصح بالتفكير بتركيب أنظمة تصفيّة الرسائل التجاريّة المرسلة عشوائيّاً قبل بدء نقل رسائل البريد الإلكتروني عبر شبكتكم اللاسلكية. سيوفّر عليكم تركيب وكلاء تحويل البريد Mail Rely Agents ومصافي الرسائل المرسلة عشوائيّاً Spam عند نقطة الإتصال بالوصلة الخارجيّة ما قد يصل حتى ١٠ – ٢٠ % من تكاليف عرض الحزمة الدوليّة.

II-٥ – بصمات الفيروسات Viruses Fingerprints

يمكن لبرمجيّات مكافحة الفيروسات كشف الفيروسات وغيرها من البرمجيّات الضارّة وإزالتها. يتم اكتشاف هذه الفيروسات عبر تفحّص البرمجيّات التنفيذيّة والمستندات بحثاً عن تعليماتٍ حاسوبيّةٍ خاصةٍ تستخدمها الفيروسات المعروفة.

تسمّى هذه التعليمات الحاسوبيّة أو بعض مشتقاتها بـ "بصمة" أو "توقيع" الفيروس. يعتبر استخدام البصمات أحد المبادئ التقنيّة التي تتيح لبرمجيّات مكافحة الفيروسات البحث عن تعليماتٍ محددةٍ في البرمجيّات المشبوهة.

يتطلب نجاح برنامج مكافحة الفيروسات توفّر قاعدة بياناتٍ تحتوي على بصمات الفيروسات المعروفة وتحديثها على الدوام.

لكنّ اكتشاف البرمجيّات الضارّة ليس بالأمر السهل، فبرمجيّات الفيروسات غالباً ما تتحوّل وتعدّل نفسها لتغيير بصماتها. لذلك تستخدم خوارزميات المسح الإرشادي Heuristic Scanning Algorithms والتي تقوم بتجربة مجموعة من التحويلات على بصمات الفيروسات المعروفة للتنبأ وتحليل احتمالات تحوّل الفيروس وكشفه قبل إنتشاره على نطاق أوسع.

حاذر من التقليل من أهميّة تأثير البرمجيّات الضارّة على أداء شبكتك اللاسلكية. لا تقل أهميّة القدرة على اكتشاف وإزالة الفيروسات من رسائل البريد الإلكتروني الواردة أو منع الإتصال من الحواسب المصابة عن أهميّة الحصول على نسبةٍ جيّدةٍ للإشارة إلى الضجيج SNR في وصلاتك اللاسلكية.

III – الأدوات Tools

يقدّم هذا الجزء نظرةً أكثر قرباً إلى بعض الأدوات البرمجيّة الحرّة ومفتوحة المصدر التي يمكن استخدامها لمراقبة الشبكة. تتضمّن بعض هذه الأدوات آليّاتٍ قادرةٍ على اتخاذ إجراءاتٍ مباشرةٍ عند حدوث أيّ مشكل.

من الأدوات التي سنقوم باستعراضها: أدوات مراقبة الشبكة (ntop, MRTG)، مصافي الرسائل المرسلة عشوائيّاً (SpamAssassin) وبرمجيّات مكافحة الفيروسات (CLAM AV).

III– 1: مراقبة الشبكة اللاسلكية

يقوم منتجو تجهيزات الشبكات اللاسلكية عادةً بتوفير أداةٍ لمراقبة التجهيزات التي ينتجونها. يتم إعداد ومراقبة التجهيزات باستخدام برنامجٍ معيّنٍ يعمل ضمن نظام تشغيلٍ محدد.

ستجد عند بناء وتشغيل الشبكات اللاسلكية الكبيرة بأنّ هذه الأدوات محدودةٌ جدّاً. لا يمكنك تشغيل الأدوات المرفقة مع التجهيزات اللاسلكية ضمن نظام إدارة الشبكة الخاص بك، وعندما تستخدم تجهيزاتٍ مختلفةٍ عند بناء الشبكة سينتهي بك المطاف مع عددٍ من الأدوات التي ستعمل على سطح المكتب سويّةً لكي تمكّنك من استيعاب ما يجري ضمن شبكتك اللاسلكية.

يمكنك تشغيل أدوات الإدارة المختلفة مع بعضها البعض وتجميعها ضمن واجهةٍ رسوميّةٍ واحدةٍ عبر محاولة الحصول على المعلومات باستخدام قواعد بيانات SNMP MIB في كلٍّ من التجهيزات المستخدمة وإظهار جميع هذه المعلومات معاً باستخدام أداةٍ إضافيّةٍ مثل MRTG.

III –٢ : أداة MRTG

ممثّل حركة الموجّهات المتعددة Multi Router Traffic Grapher (MRTG) هي أداةٌ لإدارة الشبكة ذات واجهةٍ تعتمد على الوب قادرةٌ على مراقبة وعرض المتغيرات المتبدّلة أثناء عمل الشبكة. تستخدم أداة MRTG بروتوكول إدارة الشبكة البسيط SNMP لتجميع البيانات من موجّهاتٍ مختلفةٍ تدعم هذا البروتوكول بالإضافة إلى مجموعةٍ من المكتبات الرسوميّة لإظهار المعلومات بشكلٍ بياني.
لقد تم تصميم أداة MRTG بالأساس لإظهار رسوماتٍ بيانيّة توضّح ضغط حركة البيانات واستثمار عرض الحزمة إلا أنّها طوّرت لتتمكّن من تمثيل أي متغيّر ضمن الشبكة يتبدّل مع مرور الوقت.

III –٣ : مراقبة متغيرات الشبكة اللاسلكية باستخدام أداة MRTG

سنشرح في المثال التالي المبادئ الأساسية لبناء نظام مراقبة الشبكة الخاص بك باستخدام بروتوكول SNMP وأداة MRTG. يعتمد هذا المثال على عائلة منتجات Orinoco لكّن المنهجيّة المستخدمة قابلةٌ للتطبيق على أيّ جهازٍ لاسلكيٍّ آخر.

لنفترض أنّ لدينا وصلةً لاسلكيةً بين نقطتي PtP ونرغب بمراقبة مدى استثمار عرض الحزمة الكلّي (الطبقة الثالثة Layer 3) ووضعيّة الوصلة اللاسلكية (الطبقة الثانية Layer 2).

تعتبر مراقبة جسر الشبكة اللاسلكية للحصول على مدى استخدام عرض الحزمة بسيطاً كبساطة مراقبة استخدام عرض الحزمة في أيّ جهازٍ يدعم بروتوكول SNMP (موجّه، مبدّل إلخ).

يمكن تلخيص خطوات إعداد MRTG بما يلي:

١. تأكّد من حصولك على جميع المتطلّبات الضرورية: مخدّم للوب، أداة MRTG، عنوان الإنترنت IP وكلمات السر لبروتوكول SNMP للجهاز الذي ترغب بمراقبته.
٢. قم بكتابة ملفٍ لإعدادات MRTG. يمكن القيام بهذه الخطوة يدوياً أو باستخدام أدواتٍ إضافيّةٍ مثل cfgmaker.
٣. قم بإعداد مهمّة Cron ضمن نظام التشغيل لينكس لتشغيل أداة MRTG باستخدام ملف الإعدادات المحدد بشكلٍ دوريٍّ.

III –٤ : أداة Ntop

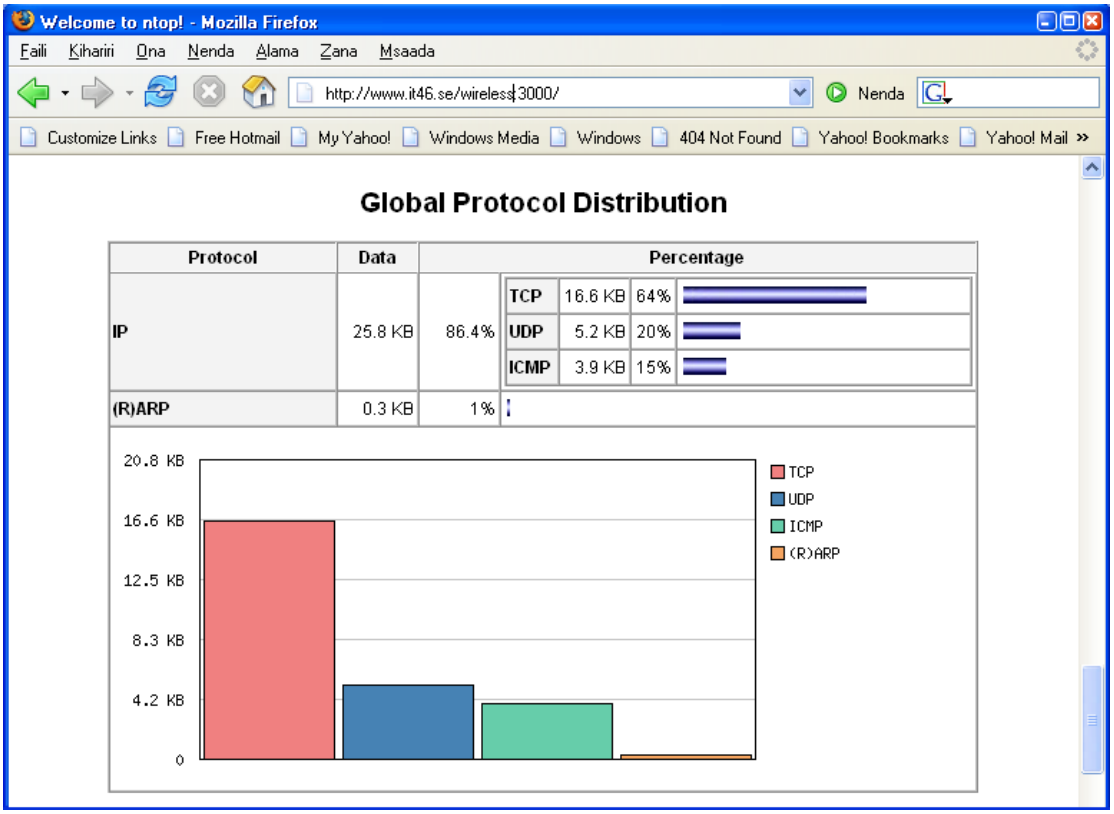
Ntop هي أداةٌ حرّةٌ ومفتوحة المصدر لمراقبة وقياس حركة بروتوكول الإنترنت IP تعمل ضمن أنظمة التشغيل المتعددة. يمكن تشغيل جميع ميزات هذه الأداة (الإعداد والمراقبة) عبر واجهةٍ تعتمد على الويب.

تعني تسمية أداة قياس حركة بروتوكول الإنترنت IP بأنّ هذه الأداة لن تقوم بتجميع أيّة معلوماتٍ متعلّقةٍ بالشبكة اللاسلكية (مثل نسبة الإشارة للضجيج، عدد المحطات المرتبطة بنقطة الولوج ..إلخ). يجب استخدام أداة Ntop جنباً إلى جنب مع أداة مراقبةٍ تعمل ضمن الطبقة الثانية Layer 2 كتلك المذكورة في الفقرة السابقة.

تركّز وظائف أداة Ntop على ما يلي:

- قياس الحركة ضمن الشبكة
- توصيف ومراقبة الحركة
- كشف محاولات إختراق الشبكة
- تحسين الأداء وتخطيط الشبكة

يتضمّن ملحق هذه الوحدة شرحاً تفصيليّاً لميزات الأداة Ntop.



شكل: استخدام أداة Ntop لمراقبة توزيع البروتوكولات ضمن الوصلة

III – ٥ : أداة Spam-Assassin

تتضمّن هذه الوحدة قسماً خاصّاً بمكافحة الرسائل التجاريّة المرسلة عشوائيّاً Spam والتي أصبحت كابوساً حقيقياً للعاملين في مجال إدارة الشبكة. تعتبر حماية المستخدمين من الرسائل المرسلة عشوائيّاً هدفاً أساسيّاً لأيّ مزوّد خدمة.

تعتبر أداة Spam-Assassin من أكثر أدوات مكافحة الرسائل المرسلة عشوائيّاً شهرةً واستخداماً. أداة Spam-Assassin هي مصفاةٌ ذكيّةٌ للرسائل المرسلة عشوائيّاً تستخدم عدّة أساليب للتمييز بين هذه الرسائل والرسائل الطبيعيّة. يمكن استخدام أداة Spam-Assassin في كلٍّ من زبائن أو مخدمات البريد الإلكتروني لتفحّص البريد الصادر والوارد.

لا تقوم أداة Spam-Assassin عادةً لمنع مرور الرسائل المرسلة عشوائيّاً، بل تقوم بوسم هذه الرسائل ومنحها علامةً تعتمد على محتواها. كلّما ارتفعت العلامة التي تحصل عليها الرسالة كلّما ازداد احتمال كونها مرسلةً عشوائيّاً Spam. يعود القرار النهائي في جميع الأحوال للمستخدم فيما إذا أراد حذف هذه الرسائل أو الإحتفاظ بها.

من أهم نقاط القوّة في أداة Spam-Assassin بنيتها المرنة والقابلة للتوسّع Modular مما يتيح إضافة التقنيّات الجديدة إلى المصفاة بالإضافة إلى إمكانيّة تركيبها ضمن أي نظامٍ للبريد الإلكتروني.

تستخدم أداة Spam-Assassin الأساليب الأساسيّة التالية لتحليل رسائل البريد الإلكتروني وتحديد إحتمال كونها مرسلةً عشوائيّاً:

- تفحّص الترويسة (حقل المرسل، الموضوع)
- تفحّص العبارات الواردة ضمن نص الرسالة باستخدام مجموعات قواعد مطورّةٍ من قبل جهاتٍ أخرى (الكلمات المفتاحية Keywords، نصوص HTML، عناوين بروتوكول الإنترنت IP، عناوين URL)
- المصافي الديكارتيّة
- قوائم العناوين البيضاء / السوداء اليدويّة
- قواعد بيانات تعريف الرسائل المرسلة عشوائيّاً التشاركيّة Collaborative Spam Identification Databases
- قوائم حجب DNS (قوائم الثقوب السوداء في الزمن الحقيقي RealTime Blackhole Lists – RBL)

- مجموعات المحارف والإعدادات المحليّة

. الخلاصة

تتطلّب إدارة الشبكة (سواءٌ كانت سلكيّةً أم لاسلكيّةً) أن نبدأ بتحديد أهدافنا كمزودين للخدمة. إذا كنّا لا نعرف ما نريد تحقيقه سيصعب علينا بالتالي تحديد ماذا نريد أن نراقب. إذا لم نعرف ماذا نريد أن نراقب، من الصعب علينا إيجاد الأدوات التي ستساعدنا في اتخاذ القرار.

يمكن تلخيص الأمور الخمس الرئيسية التي ينبغي عليك تذكرها من هذه الوحدة بما يلي:

١. لا يكفي جمع البيانات الأوليّة أو تركيب الأدوات للحصول على شبكةٍ تعمل بشكلٍ جيّدٍ. لن تجد صعوبةً في إيجاد الأدوات الملائمة إذا عرفت تماماً ماذا تريد.
٢. لن تكفي مراقبة وضعيّة الوصلة اللاسلكية إذا كانت شبكتك تعجّ بنشاط الفيروسات. لن يكفيك أيضاً إيقاف الفيروسات مالم تكن وصلاتك اللاسلكية ثابتةً.
٣. عند تركيب أدوات مراقبة و/أو إدارة الشبكة، يتوجّب عليك تعلّم كيفية تركيب وتشغيل الأدوات المختلفة بحيث تصبح كافّة المعلومات المطلوبة لاتخاذ القرار سهلة المنال.
٤. فكّر دوماً أنّه قد يكون من الأسهل عليك في حال كانت الأدوات المتوفرة لا تلائم متطلباتك أن تقوم بكتابة أداةٍ بسيطةٍ بنفسك لتفي باحتياجاتك عوضاً عن التصارع مع أداةٍ تلائم متطلّبات شخصٍ آخر.
٥. حدد أهدافك > حدد المبادئ التقنيّة > أوجد / صمم الأدوات > اتخذ القرارات

قياس الحركة باستخدام الأداة NTOP

تقوم NTOP بربط كل حزمةٍ تلتقطها بمرسل هذه الحزمة ومستقبلها. يمكن بهذا الأسلوب استحصال جميع الأنشطة المتعلّقة بمضيفٍ واحدٍ عبر معرفة إسم هذا المضيف، عنوان الإنترنت IP الخاص به أو عنوان بطاقة الشبكة NIC.

يمكن الحصول على هذه المعلومات لكل مضيفٍ باستخدام NTOP:

- البيانات المرسلة والمستقبلة: مجموع البيانات المرسلة أو المستقبلة (الحجم وعدد الحزم) مصنفّةً حسب البروتوكول المستخدم (IP, IPX, AppleTalk إلخ) وبروتوكول الإنترنت المستخدم أيضاً (FTP, HTTP, NFT إلخ)
- الإرسال المتعدد لبروتوكول الإنترنت IP Multicast: الحجم الكلّي لحركة الإرسال المتعدد المرسل أو المستقبل من قبل المضيف
- تاريخ جلسة TCP (TCP Session History): يعطي جلسات TCP الفعّالة والتي بدأها أو قبل بها المضيف بالإضافة إلى إحصاءات الحركة المتعلّقة بكل جلسة
- حركة بروتوكول UDP (UDP Traffic): الحجم الكلّي لحركة بروتوكول UDP مصنّفةً حسب البوابة المستخدمة
- خدمات TCP/UDP المستخدمة (TCP/UDP Services Used): يعطي الخدمات التي تعتمد على بروتوكول الإنترنت IP والتي يوفّرها المضيف بالإضافة إلى الزبائن الخمس الأخيرة التي استخدمت كلاً منها.
- نظام التشغيل المستخدم في المضيف
- النسبة المئويّة لعرض الحزمة المستهلك (الفعلي، الوسطي والأعظمي)
- توزّع الحركة (بين الشبكات الفرعيّة Subnets)
- توزّع حركة بروتوكول الإنترنت IP Traffic Distribution (UDP مقابل TCP، التوزّع النسبي لبروتوكولات IP)

تقوم أداة NTOP أيضاً بتجميع معلوماتٍ عامّةٍ (لا تتعلّق بمضيفٍ معيّن) عن توزّع الحركة، توزّع الحزم واستثمار عرض الحزمة.

توصيف ومراقبة الحركة باستخدام الأداة NTOP

تتطلّب مراقبة الحركة تحديد الحالات التي تحيد فيها الحركة ضمن الشبكة عن اتبّاع القواعد أو الحدود الموضوعة من قبل مدير الشبكة. بإمكان أداة NTOP إكتشاف الحالات التاليّة:

- الإستخدام المتكرر لنفس عنوان الإنترنت IP
- تحديد جميع الموجّهات الموجودة ضمن شبكةٍ فرعيّةٍ Subnet
- تحديد جميع الحواسب التي تم إعداد بطاقة الشبكة ضمنها للعمل وفق نمط
- إكتشاف الإعدادات الخاطئة للتطبيقات البرمجيّة
- إكتشاف إساءة استخدام الخدمات (كالحواسب التي لا تستخدم الأنظمة الوكيلة Proxies المحددة)
- إكتشاف الحواسب التي تستهلك عرض الحزمة بشكلٍ مفرط

إكتشاف الإختراقات الأمنيّة للشبكة باستخدام أداة NTOP

تأتي غالبيّة الهجمات الأمنيّة في الشبكة من ضمن الشبكة نفسها لا من الخارج. توفّر أداة NTOP لمستخدميها إمكانيّة ملاحقة الهجمات أثناء حدوثها وتحديد نقاط الضعف في أمن الحواسب عبر تقديم الميزات التالية:

- إكتشاف محاولات مسح البوابات "Portscan" و "Slow Portscan": تقدّم أداة NTOP تقريراً بأسماء آخر ثلاثة حواسب أرسلت حزمةً إلى كلّ بوابةٍ أصغر من ١٠٢٤. يمكن اكتشاف محاولات مسح البوابات Portscan ضمن جميع الحواسب التي تقوم NTOP بمراقبتها
- إكتشاف انتحال الشخصيّة Spoofing Detection (للحزم التي تنتمي إلى نفس الشبكة الفرعيّة Subnet التي تعمل NTOP ضمنها): إنتحال الشخصيّة Spoofing يعني أن المضيف سيدّعي بأنّه مضيفٌ آخر للتمكّن من التلصص على الحزم. تقوم أداة NTOP بتنبيه المستخدم عند اكتشاف عنواني إنترنت IP مختلفين يعملان على نفس بطاقة الشبكة في الشبكة الفرعيّة Subnet.
- إكتشاف التجسس Spy Detection: يعتبر مضيفٌ ما جاسوساً إذا كانت بطاقة الشبكة الخاصّة به معدّة للعمل ضمن نمط التنصت والذي يتيح إلتقاط الحزم المارّة عبر الشبكة بغضّ النظر عن وجهتها.
- أحصنة طروادة Trojan Horses: يبدو حصان طروادة لأول وهلةٍ برنامجاً مسالماً لكنّه في الحقيقة يحتوي على برنامجٍ خفيٍ ضارٍ قادرٍ على تدمير حاسبك. تستخدم أحصنة طروادة عادةً بواباتٍ معروفةً، وبالتالي يمكن لأداة NTOP أن تكتشف وجود هذه الأحصنة عبر مراقبة الحركة على هذه البوابات.
- هجمات إيقاف الخدمة Denial of Service (DoS): وهي تصرفات المضيف الذي يقوم بإرسال حزمٍ تحتوي SYN Flag (لفتح وصلات TCP) إلى بوابات "الضحايا" دون متابعة إجراءات الوصلة. سيؤدّي ذلك في النهاية إلى امتلاء جميع منافذ الوصلات ضمن كدسة بروتوكول الإنترنت IP Stack في الضحيّة مما يمنعها من قبول أيّة وصلات إضافيّة.

تحسين أداء وتخطيط الشبكة باستخدام الأداة NTOP

يؤدّي الإعداد الردئ للحواسب والاستثمار غير الفعّال لعرض الحزمة المتوفّر إلى تدّني أداء الشبكة. تقدّم أداة NTOP الخدمات التالية لتحسين أداء الشبكة:

- تحديد البروتوكولات غير الضروريّة (الحواسب التي تستخدم بروتوكولات غير مستخدمةٍ في الشبكة).

- تحديد التوجيه غير الأمثل عبر تتبع رسائل إعادة التوجيه ICMP وتحليل قائمة الموجّهات الموجودة ضمن الشبكة.
- توصيف الحركة والتوزيع عبر دراسة أنماط الحركة Traffic Patterns.
- الإستخدام الحكيم لعرض الحزمة: تساعد دراسة توزّع الحركة بين البروتوكولات مدير الشبكة على تحديد التطبيقات التي تحتاج إلى وكلاء Web Proxies .

تدعم أداة NTOP قواعد بيانات SQL في حال أراد المستخدم حفظ البيانات التي تمّ تجميعها خلال جلسة المراقبة.