مراقبة الشبكات
NETWORK MONITORING

استاذ المقرر

الأستاذة أمل زهران
ماجستير في نظم المعلومات الحاسوبية
Master Computer Information System
المدرب العتمد لدورات نظم الحاسب الإلكترونية

الساعات المكتبية
الأثنين 7-8:15 مساء
البريد الإلكتروني a.saleh@mu.edu.sa
الموقع الإلكتروني http://faculty.mu.edu.sa/asaleh
هاتف العمل 06 404 2779

مراقبة الشبكة

تعريف مصطلح مراقبة الشبكة :

- استخدام ادوات تجميع وتحليل المعلومات لتحديد كيفية سير البيانات في الشبكة واستهلاك مواردها إضافة الى العديد من المؤشرات على أداء الشبكة
- توفر أدوات مراقبة الشبكة الجيد قياسات لمؤشرات أداء الشبكة إضافة الى تحويل المؤشرات الرقمية الي رسم بياني مما يساعد على تكوين صورة واضحة عن حالة الشبكة وبالتالي تقدير مدى الحاجة الى التغييرات

مراقبة الشبكة

هي عملية فحص الكمبيوتر والنظم والخدمات التي تتكون منها الشبكة.فيجب البحث عن الحل الذي سيساعد على رصد وقياس وابلاغ ومتابعة وتقديم تقرير عن صحة و جودة البنية التحتية للتكنولوجيا الخاصة بك .و هذا يسمح لمدير الشبكة بالحفاظ على الشبكة و تحسينها

الأدوات المستخدمة عادة ما تكون مزيجا من المصادر المفتوحة والبرمجيات المرخصة ، وتندرج ضمن فئتين أساسيتين :

- حلول النقطة (Point Solutions)
- والإدارة المتكاملة الأجنحة (Integrated Management Suites)

جامعة المجمعة
Majmaah University

الحاجه لبرامج مراقبه الشبكات

في السابق كانت مراقبة الشبكة تعتبر ترف الشركات الكبيرة .ولكن اليوم ، مراقبة الشبكة هو ضرورة حتى لأصغر متجر لتكنولوجيا المعلومات .المشكلة مع هذه الضرورة هو أن الأمر يحتاج إلى الكثير من الوقت و المال

الأستاذه أمل زهران

هناك عوامل عديدة قد تساهم في تعطيل الشبكة نهائيا او تعطيل عملها مثل:

1. انقطاع التيار الكهربائي
2. تعطل احد الخوادم (server)
3. اسقاطات عرض النطاق الترددي للشبكة(network bandwidth drops)
4. اختراق الشبكات المحلية LAN

مظاهر تأثر أداء الشبكة

1- بطء عمل الشبكة
2- زياده الوقت للدخول الى الحساب الشخصي
3- زيادة فترات الانتظار للطباعة او اى جهاز موصول بالشبكة(هذه المشاكل تزيد بزياده الاجهزة التي تتصل بالشبكة)

مراقبة الشبكة الفعال سينبهك اللحظة التي تنشأ فيها حالة ما , لكي تتمكن من التعامل معها فورا ، و بالتالي خفض و تقليل وقت العطل (down-time).

في حين أن الربط الشبكي لنظام الرصد يمكن أن يوفر معلومات عن المشاكل ، يمكنه أيضا أن يقدم معلومات عن تحسين الشبكة

العوامل المؤثرة في أداء الشبكة :

- يمكن القول أن هناك عدة عوامل تؤثر في أداء شبكة هي :
- 1. عدد أجهزة الحاسوب المتصلة بها
- 2. البرمجيات المستخدمة
- 3. المسافة بين الأجهزة
- 4. سرعة نقل البيانات وتقاس بالبت في الثانية

فكره عامة عن كيفية عمل مراقبة الشبكة

كلما كبرت و توسعت الشبكة ,كلما زادت أهمية سياسات الصيانة و التخطيط الاستراتيجي لإدارة الشبكة

إدارة الشبكة تعتمد على علاقة المستخدم –الخادم (client-server relationship)

اي ان البرامج تكون في المستخدم (client)و جميع التحركات مراقبه من الخادم (server).

- عند حصول اي نوع من الانشطه مثل محاولة دخول الحساب الشخصي لشخص أخر يقوم النظام برسال انذار الى الخادم .
- اذا كانت هناك محاولة دخول غير مصرح بها أي من قبل اشخاص غير مصرح لهم يستجيب النظام و يقوم بعملية انذار المستخدم و حماية المعلومات الحساسة

فكره عامة عن كيفية عمل مراقبة الشبكة

مراقبه الشبكات تشمل على

1- ادارة الامن (Security management)

2- اداره الاخطاء (Fault management)التي تعمل على

- تعقب الاعطال و عزلها و اصلاحها .
- تشمل على آليات تبحث عن أقصى قدر من الاستفادة من الموارد ،
- إعداد التقارير
- تقدم معلومات دقيقه عن قياس أداء الشبكة
- وتوفر احصاءات في نفس الوقت الحالي لجميع أجهزة الكمبيوتر في الشبكة.

و بالتالى تعمل الشبكة حتى تصل الى ذروها مع كل ما يقدمه هذه البرنامج من خيارات تقلل من العبء الملقى على عاتق مدير الشبكة و موظفي الدعم في قسم تقنية المعلومات ,

الأستاذه أمل زهران

مراقبة الشبكة الحاسوبية

مراقبة الشبكة الحاسوبية تنطوي على بعض الأمور مثل

1- الأمن والمخاطر ،

2-والأداء ،

3-والخطأ ،

4-النظام ،

5-التهيئة موازنة الحمل ،

6- وتوجيه حركة المرور ، وإدارة حركة المرور .

الغرض من إدارة الأداء هو مثلا لقياس المستخدم (أداء زمن الاستجابة ، وأداء التطبيقات

مثال عن مراقبة الشبكة

- سنفترض اننا مسؤوليين عن شبكة بنيت منذ 3 أشهر وتحوي 50 جهاز حاسب و3 خادمات ,خادم للبريد الإلكتروني وخادم للويب وخادم للوكيل..بعد فتره من الإستخدام الجيد للشبكة بدأ المستخدمون بالتذمر من بطء الشبكة ومن ازدياد ملحوظ في عد الرسائل غير المرغوب فيها(Spam)

ومن الواضح ايضا ان أداء الحواسيب يزاد بطاءً حتى في عدم استخدام الشبكة مما أدى الى توتر المستخدمين

المشكلة

مجلس ادارة الشركة بحاجة منا الى تبرير

1- هل تستخدم الشركة النطاق الممنوح لها من مزود خدمة الإنترنت بالكامل داخل الشبكة

2- مدى الحاجة الى جميع التجهيزات في الشبكة

الحل :

1- مراقبة الشبكة المحليةLAN

للحصول على فكره واضحة عن أسباب انخفاض أداء الشبكة يجب مراقبة تدفق البيانات داخل الشبكة المحلية

فوائد مراقبة الشبكة المحلية :

- تبسيط عملية كشف الأخطاء بشكل كبير
- امكانية اكتشاف الفيروسات والقضاء عليها
- امكانية اكتشاف الأشخاص المزعجين والتعامل معهم
- امكانية تبرير تجهيزات وتكاليف الشبكة بشكل احصائي

الحل :

2- مراقبة الشبكة الواسعة WAN

لتبرير مدى استغلال الشركة لحزمة الإنترنت (نطاقها) مراقبة البيانات المتدفقة خارج الشبكة المحلية

تدفق البيانات الخارجي هي اية بيانات مرسلة عبر الشبكة الواسعة المجال WAN مرسلة او مستقبلة

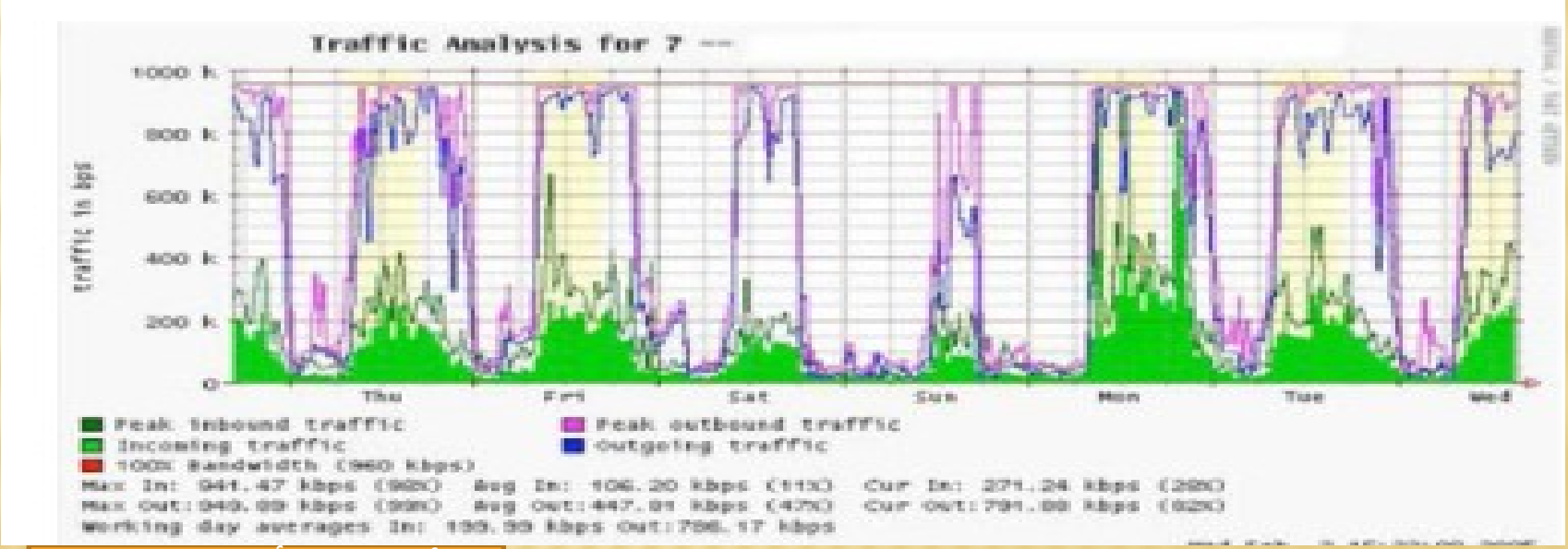
فوائد مراقبة تدفق البيانات الخارجي:

- تبرير تكاليف الإتصال بالإنترنت عبر إظهار لإستثمار الفعلي لتناقل البيانات خارج الشبكة
- تقدير المتطلبات المستقبلية للشبكة عبر متابعة انماط الإستخدام الحالي والتنبؤ بالتوسع والإنتشار
- اكتشاف المتطفلين القادمين من خارج الشبكة ومحاولة ايقافهم قبل ايذاء الشبكة

الحل :

3- كشف انقطاعات الشبكة

عد تركيب أدوات مراقبة الشبكة نستطيع الحصول على قياسات افضل لعرض الحزمة الذي يستهلكة المستخدمون في الشركة وبالتالي تحديد ساعات الذروة في استهلاك الحد الأقصى من حزمة الإنترنت



الأستاذه أمل زهران

3- كشف انقطاعات الشبكة

من الواضح ان استهلاك الإنترنت في وقت الذروة يتجاوز إستطاعتها القصوي مما يؤدي الى التأخير في استجابة الشبكة

وبالتالي نقوم بتقديم هذا الرسم البياني لمجلس الإدارة لتبرير ضعف الشبكة وبالتالي المطالبة برفع طاقة الإنترنت المزودة للمؤسسة لتغطية احتياجات المستخدمين

موضوع للمناقشة

بعد فتره زمنية يرد اتصال لمسؤول الشبكة يوضح ان جميع المستخدمين غير قادرين على الإتصال بالإنترنت دون استثناء ؟؟

يجب كتابة الخطة من وجهة نظرك لإيجاد الحل ..

فوائد نظام المراقبة الفعال في الشبكة

1- تبرير مصاريف الشبكة والموارد المرفقة
2- اكتشاف المتطفلين على الشبكة ومنعهم من إيذائها
3- اكتشاف الفيروسات بسهوله
4-تبسط معالجة مشاكل الشبكة بشكل هائل
5- تحسين أداء الشبكة بشكل كبير
6- تسهيل عملية تحطيط استطاعة الشبكة (حسب نطاق الإنترنت يتم توزيعه على المستخدمين)

انواع ادوات المراقبة في الشبكة

1- أدوات كشف الأعطال Spot Check Tools

1.1 Ping :

تحتوي معظم أنظمة التشغيل على نسخة من أداة Ping تعتمد هذه الأداة على حزمة ببروتوكول رسائل تحكم الإنترنت ICMP لمحاولة افتصال بمضيف ما لتعاود إخبارنا بالزمن الذي استغرقة الحصول على رد من هذا المضيف

حالات الرد :

- تأخر الرد على الحزم المرسلة يفيد بانه يوجد ازدحام ما على الشبكة
- لم تظهر Pingأي بيانات وهنا يفيد بأن ترجمة اسماء الناطق DNSغير صحيح

انواع ادوات المراقبة في الشبكة

1- أدوات كشف الأعطال Spot Check Tools

1.2 Treceroute :

توجد هذه الأداه في معظم أنظمة التشغيل وتسمى أحيانا Tracert وتقوم هذه الأداء بتحديد موقع الخلل في الوصلة بين الحاسوب المحلي وأي 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 * * *
```

1.2 TRECEROUTE :

يقوم الخيار n– باعلام Trecerout الى اهمال ترجمة اسم النطاق ويؤدي بالتالي لتسريع العمل ,نلاحظ ان زمن رحلة الذهاب والإياب تفوق الثانيتين في المحاطة السابعة في حين ان الحزم تضيع كليا في المحطة الثامنة وهذا يدل على وجود مشكلة في هذه المنطقة من الشبكة وإن كانت هذه المنطقة تابعة للشبكة المحلية فيجب البدء بكشف العطل انطلاقا منها .

انواع ادوات المراقبة في الشبكة

1- أدوات كشف الأعطال Spot Check Tools

1.3 mtr (My TraceRoute)

تجمع هذه الأداة بين الأداتين Ping و Treseroute في برنامج واحد حيث باستخدام هذا البرنامج بستطيع الحصول على متوسط زمن التأخير وخسارة حزم البيانات في مضيف واحد عوضا عن البيانات اللحظية التي تقدمها اداتي Ping و Traceroute

انواع ادوات المراقبة في الشبكة

2- أدوات تحليل البروتوكولات Protocol Analyzers

تستخلص الكثير من التفاصيل عن المعلومات المنقوله عبر الشبكة من خلال تفحص حزم البيانات المارة على حده

2.1 Tcpdump

وهي أداة تعمل ضمن سطر Command line لمراقبة تدفق البيانات ضمن الشبكة حيث يمكنها تجميع وعرض معلومات جميع بروتوكولات الشبكة

انواع ادوات المراقبة في الشبكة

2- أدوات تحليل البروتوكولات Protocol Analyzers

Wireshark 2.2

وهو برنامج حر لتحليل البروتوكولات يعمل ضمن أنظمة تشغيل اليونكس والويندوز ويعتبر اكثر برمجيات تحليل البروتوكولات شعبية في العالم

يتيح هذا البرنامج تفحص البيانات الماره عبر الشبكة واستعراض هذه البيانات وترتيبها حسب الحاجة

انواع ادوات المراقبة في الشبكة

3- أدوات تحليل الأنماط Trending Tools

- تستخدم أدوات تحليل الأنماط لمراقبة استخدام الشبكة ضمن فتره زمنية معينة
- تقوم بمراقبة اداء الشبكة بشكل دوري وعرض ملخص للنتائج بصيغة يسهل استيعابها (رسم بياني مثلا)
- تقوم هذه الأداة بتجميع وتحليل وعرض البيانات المتعلقة بأداء الشبكة في آن واحد

انواع ادوات المراقبة في الشبكة

3- أدوات تحليل الأنماط Trending Tools

MRTG 3.1

تقوم ادات التمثيل البياني لتدفق البيانات ضمن عدة موجهات Multi Router Traffic Grapher (MRTG)بمراقبة استهلاك وصلات الشبكة بواسطة برتوكول ادارة لشبكة البسيط SNMP وتوليد رسوم بيانية تمثل البيانات الصادرة والوارده في كل وصله

انواع ادوات المراقبة في الشبكة

3- أدوات تحليل الأنماط Trending Tools

Ntop 3.1

تقوم هذه الأداة ببناء تقرير تفصيلي بالزمن الحقيقي لنشاط الشبكة وعرضه ضمن متصفح الواب , تستهلك هذه الأداة الكثير من موارد المعالج ومساحة القرص الصلب ولكن تعطي رؤية دقيقية عن كيفية استخدام الشبكة

مميزات الأداة Ntop

1- ترتيب عرض نشاط الشبكة ضمن معايير مختلفة (المصدر , الوجهه , البروتوكول ,الخ)

2- تجميع احصائيات نشاط الشبكة وفق بروتوكول او رقم بوابة

يتبع مميزات الأداة NTOP

3- مصفوفة تدفق البيانات والتي تظهر الوصلات بين الأجهزه

4-تحديد نظام التشغيل المستخدم على كل جهاز

5-تحديد البيانات المستخدمة من قبل برمجيات الند للند P2P

مساوئ الأداة Ntop

عجزها عن توفير بيانات لحظية لأداء الشبكة لأنه تعتمد على القيم الكلية والمتوسطة لفترة زمنية مما يحول دون امكانية استخدامها للكشف عن الأعطال المفاجئة

انواع ادوات المراقبة في الشبكة

3- أدوات تحليل الأنماط Trending Tools

Cacti 3.2

واجهه لحزمة الأدوات RDDtools تحتفظ بجميع المعلومات الضرورية لتوليد الرسوم البيانية ضمن قاعدة بيانات MySQL تتولى مهام ادارة الرسوم البيانية ومصادر المعلومات وبالإضافة الى عملية تجميع البيانات ,تدعم أيضا برتوكول الشبكة البسيط SNMP .

بمقدور Cacti تجميع البيانات من تجهيزات الشبكة المختلفة وبناء رسوم بيانية معقدة عن كيفية مسار الشبكة

انواع ادوات المراقبة في الشبكة

3- أدوات تحليل الأنماط Trending Tools

NetFlow 3.3

وهو برتوكول لتجميع معلومات تدفق بيانات بروتوكول الإنترنت IP صممته شركة سيسكو Cisco

يوفر هذا البروتوكول مجموعة من الخدمات الأساسية لتطبيقات الإنترنت IP أهمها :

1- احصائيات تدفق البيانات ضمن الشبكة

2- تخطيط الشبكة

3- أمن الشبكة

4- معلومات عن مستخدمي الشبكة وتطبيقاتها

5- معلومات عن أوقات الذروة في الشبكة

توجيه حظم البيانات

انواع ادوات المراقبة في الشبكة

3- أدوات تحليل الأنماط Trending Tools

Flowc 3.4

برنامج مفتوح المصدر لتجميع بيانات برتوكول NetFlow صغير الحجم وسهل الإعداد

يعتمد Flowc على قاعدة بيانات MySQL لتخزين معلومات تدفق البيانات و لذلك يمكن تعديل الرسوم البيانات بناء على طلب المستخدم او استخدام التقارير القياسية الموجوده في البرنامج

انواع ادوات المراقبة في الشبكة

4- أدوات فحص انتاجية الشبكة Throughput Testing

انتاجية الشبكة : السرعه القصوى لنقل البيانات ضمن الشبكة و الإستطاعة الفعلية لوصله ضمن الشبكة خلال زمن معين

الأدوات المستخدمة في قياس السرعه والإستطاعة في الشبكة المحلية :

انواع ادوات المراقبة في الشبكة

4- أدوات فحص انتاجية الشبكة Throughput Testing

Bing 4.1

تقوم هذه الأداة بتقدير الإستطاعة المتاحة لوصلة تربط بين نقطتين من خلال تحليل زمن رحلة الذهاب والاياب لحزمة ICMP محتلفة الاحجام.

يمكن لاداة Bing تقدير استطاعة الشبكات الكبيرة و محاولة تخمين استطاعة الوصلات الخارجية دون الحاجة لتشغيل برنامج الزبون في الطرف الاخر نظرا لاستخدام هذه الشبكات لطلبات ICMP بشكل دوري

تتميز هذه الاداة بـ استهلاكها المنخفض لعرض الحزمه مما يتيح الحصول على فكرة تقريبية عن اداء الشبكة دون الحاجه الى اغراق الشبكة بالبيانات لمجرد قياس ادائها

انواع ادوات المراقبة في الشبكة

5- أدوات المراقبة في الزمن الحقيقي realtime

تستخدم لمراقبة التسلل الى الشبكة و حدوث عطل مفاجئ فيها فهي تعمل على مراقبة الشبكة بشكل مستمر وإعلام المختص في حال حدوث عطل مفاجئ بها

snort 5.1

برنامج لتحسس الشبكه Sniffer يمكن استخدامه لاكتشاف المتسللين ويتمتع بقدرته على تبيه مسؤول الشبكة باحدى طرق الاتصال

انواع ادوات المراقبة في الشبكة

5- أدوات المراقبة في الزمن الحقيقي realtime

Zabbix 5.2

وهي اداة مفتوحة الصدر لمراقبة الشبكة بشكل مستمر

موضوع للبحث

- تقديم بحث ,مناقشة في واحد من المواضيع التالية :

Keylogger

Network and System Monitoring: ipMonitor

Security Monitoring: Spytech SecurityWorks