بسم الله الرحمن الرحيم

جامعة السّودان المفتوحة

برنامج الحاسوب

استخدام وادارة الشبكات (1)

رمز المقرر ورقمه: حسب 2039

إعداد المادة العلمية:

أ. د. عبد الحميد محمد رجب

أ . د. السيد محمود عبد الحميد الربيعي

تصمـــيم تعلـــيمي: إيهاب عبد الحي

التدقيق اللغوي : الهدي عبد الله محمد

التصميم الفني : منى عثمان أحمد النقة

منشورات جامعة السودان المفتوحة، الطبعة الأولى 2007م

مقدمة المقرر

الحمد لله بجميع محامده كلها ماعلمت منها وما لم أعلم عدد خلقه كلهم ماعلمت منهم وما لم أعلم والصلاة والسلام علي السلطان الاعظم والنائب العام الاكرم باب الرحمة المفتوح عند إنغلاق جميع الابواب في وجوه المذنبين وقبس الرجاء الملموح عند سيطرة اليأس في قلوب المعذبين الباسط يد الاحسان لكل تآئب ليأخذ بيمنه الي الصف الاول والمستغفر للغافلين من أمته لينقذهم بجاهه من الهبوط الي الدرك الاسفل فطوبي لكل منتمي اليه وياقرةعين المكثرين من الصلاة والسلام عليه

عزيزى الدارس مرحبا بك الي هذا المقرر

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

السنوات القليلة المقبلة خاصة في مجالات الشبكات بأحجامها وأنماطها المختلفة.

والمتطلبات الأساسية لدراسة هذا الكتاب عزيزي الدارس هو أن يكون لديك معرفة أساسية مسبقة **بأساسيات** وتقنيات اتصال البيانات في شبكات الحاسب الآلي، **ويهدف هذا الكتاب في مجمله إلى تزويد الطالب بالمعرفة اللازمة والتهيئة لمستقبل مهني في مجالات استخدام وإدارة الشبكات وما يدخل فيها من مفاهيم متعلقة بالإدارة المثلي لموارد الشبكة من عتاد وبرمجيات بغرض تقديم خدمة مثلي للمستخدمين المتصلين بالشبكة بتكلفة مناسبة وسرعة وأمان مناسبين وهي مجموعة من المفاهيم تؤصل للدارس كيف يقوم بالتخطيط الجيد في المستقبل للشبكات.**

ويشمل هذا الكتاب على الوحدات التالية :

الوحدة الأولى : وعنوانها : "مفاهيم أساسية في علم إدارة الشبكات" ، إعطاء القارئ فكرة واضحة دقيقة حول مجموعة من المفاهيم لعلم إدارة واستخدام الشبكات وقد اشتملت هذه المفاهيم ، تعريف شبكة البيانات ، دور مهندس الشبكات ، أهداف إدارة الشبكات ، إدارة الأعطال ، إدارة التهيئة، إدارة الأمن ، إدارة الأداء ، إدارة الحسابات، بروتوكولات إدارة الشبكة.

الوحدة الثانية : وعنوانها : "نظام إدارة الشبكات" ، توضيح:- مكونات نظام إدارة الشبكات، برنامج إدارة الشبكات، معمارية إدارة الشبكات، المعماريات المختلفة للشبكات(المركزية، الهرمية، الموزعة)، تطبيقات إدارة الشبكات، طريقة اختيار نظام إدارة الشبكة، إدارة الوسط الموزع DME، إدارة شبكات الاتصال TMN.

الوحدة الثالثة : وعنوانها : "إدارة الأعطال" ، وفيها تم بيان:- فوائد عملية إدارة الأعطال، وكيفية تحقيق عملية إدارة الأعطال، بداية بتجميع المعلومات اللازمة لتحديد المشكلة، تحديد الأعطال الواجب إدارتها، إدارة الأعطال في نظام إدارة الشبكة، الوسائل البسيطة والمركبة والمتقدمة لإدارة الأعطال، تأثير الأعطال على الشبكة، أشكال تدوين الأعطال، استخدام الخرائط الهرمية والألوان.

الوحدة الرابعة : وعنوانها : "إدارة التهيئة" ، وفيها تم توضيح كل من:- فوائد إدارة التهيئة، تحقيق عملية إدارة التهيئة، الاستكشاف الآلي لأجهزة الشبكة، تعديل وتخزين معلومات التهيئة، إدارة التهيئة في نظام إدارة الشبكة، الأداة البسيطة والمركبة والمتقدمة لإدارة التهيئة، طرق توليد تقارير إدارة التهيئة.

الوحدة الخامسة : وعنوانها : **"إدارة الأمن"** ، وفيها تم بيان كل من:- فوائد إدارة أمن شبكة البيانات، كيفية تحقيق إدارة أمن الشبكة، إيجاد نقاط الاتصال وتأمينها والحفاظ عليها، توثيق المستخدم والحاسب ومفتاح الدخول، التشفير والجدار الناري وترشيح الحزم، نظام

مقدمة الكتاب

الأمن في نظام إدارة الشبكة، الأدوات البسيطة والمركبة والمتقدمة لإدارة الأمن، تدوين حوادث الأمن في الشبكة، تطبيقات .

الوحدة السادسة : وعنوانها : "إدارة الأداء" ، وفيها تم توضيح كل من:- فوائد إدارة الأداء، كيفية تحقيق إدارة الأداء، رصد معدل الاستخدام واتجاهات الشبكة، قياس مستوى الخدمة في الشبكة، قياس زمن الاستجابة ومعدل الرفض والإتاحة، تحليل بيانات الشبكة وضبط القيم الحدية، استخدام محاكاة الشبكة والمحاكي، إدارة الأداء في نظام إدارة الشبكة، وسائل الإدارة البسيطة والمركبة والمتقدمة، القيم الحدية والقيم التأهيلية، رسومات الأداء ثنائية وثلاثية الأبعاد، تدوين معلومات الأداء، برامج عملية للتدريب على قياس الأداء.

الوحدة السابعة : وعنوانها : "إدارة الحسابات" وفيها تم بيان:- فوائد إدارة الحسابات، كيفية تحقيق إدارة الحسابات، استخدام المعايير وضبط الحصص، تحديد فواتير الاستخدام للشبكة، إدارة الحسابات في الشبكات المحلية، إدارة الحسابات في نظام إدارة الشبكة، الأدوات البسيطة والمركبة والمتقدمة لإدارة الحسابات، تدوين معلومات الحسابات.

وختاماً نتمني

أن نكون قد وفقنا في تقديم إضافة جديدة لك عزيزي الدارس في مجال إدارة شبكات الحاسب الالي آملين تزويد الجامعة بالمىحظات التي تراها مناسبة لتطوير هذا المقرر

وفق الله الجميع وسدد الخطي

محتويات المقرر


الوحدة الاولى
مقدمة في علم الشبكات

محتويات الوحدة

مقدمة

تمهيد

عزيزي الدارس، مرحبا بك في الوحدة الأولى من مقرر إدارة الشبكات التي ستتناول عدداً من الأقسام القسم الأول منها نتعرف على وظائف شبكة البيانات. وسنعدد المهام الوظيفية لمهندس الشبكة ثم نتعرف على وظائف علم شبكات البيانات ونوضح بالامثلة وظائف الشبكة ، بعدها نتعرف على أدوات إدارة الشبكة ومنها نعدد وظائف إدارة الاعطال وإدارة التهيئة والحسابات وندرج بعدها إدارة الاداء وإدارة الأمن وفي القسم الاخير نتعرف على كيفية إدارة الشبكة بكفاءة عالية.

عزيزي الدارس تكمن أهمية هذه الوحدة في كونها وحدة ابتدائية تأسيسية تنبني عليها بقية الوحدات، ولذا لابد أن نوليها اهتماماً خاصاً وذلك بإجابة التدريبات المصاحبة لها، وأسئلة التقويم الذاتي الواردة في ثناياها لأنها ستساعدك في فهم ماورد فيها من مفاهيم.

أهلا بك مرة أخرى إلى هذه الوحدة عسى أن تنتفع بها وأن تفيد منها، وأن تساعدنا في نقدها وتطويرها .

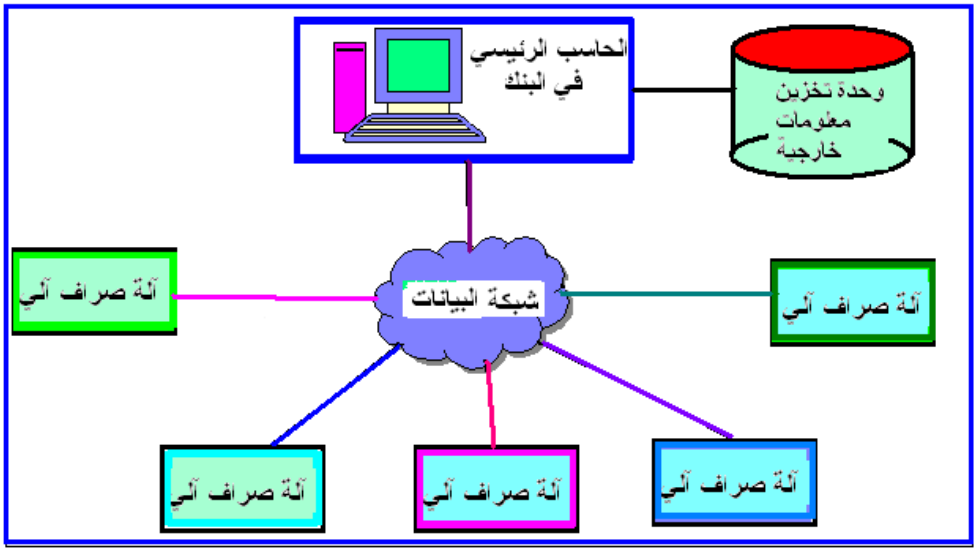
أهداف الوحدة

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

- تعرف وظائف شبكة البيانات.
- تعدد المهام الوظيفية لمهندس الشبكة.
- توضح وظائف علم إدارة شبكات البيانات.
- تشرح بعض الأمثلة لتوضيح وظائف إدارة الشبكة.
- تعرف أدوات إدارة الشبكة.
- تبين وظائف إدارة الأعطال.
- تذكر وظائف إدارة التهيئة.
- تعدد وظائف إدارة الحسابات.
- تصف بعض وظائف إدارة الأداء.
- توضح بعض وظائف إدارة الأمن.
- تبين كيفية إدارة شبكة البيانات بكفاءة عالية .

1. تعريف شبكة البيانات

عزيزي الدارس، تعرف شبكة البيانات بأنها **مجموعة الأجهزة والأسلاك المستخدمة في نقل البيانات من جهاز كمبيوتر لآخر**. وذلك لتمكين المستخدمين من القدرة على مشاركة عتاد الشبكة من أماكن متعددة. مثال على ذلك هو ربط آلات الصراف الآلي ATM (Automatic Teller Machines) بواسطة شبكة كمبيوتر بنكية حتى يستطيع العميل سحب النقود من أماكن مختلفة كما هو موضح في شكل1.1. ومثال أخر شبكة المعلومات العالمية (الانترنت) التي يستطيع المستخدمين استخدامها في التواصل لنقل المعلومات من مكان لآخر وكذلك إرسال رسائل البريد الالكتروني وعمل حوارات. أو استخدام شبكات محلية لربط مجموعة حاسبات داخل المؤسسات والجامعات لربط الأقسام العلمية و الوحدات الإدارية لتحقيق سرعة تبادل المعلومات عبر الشبكة.



شكل1.1 شبكة بيانات تستخدم في توصيل آلات الصرف الآلي بالبنك.

2. دور مهندس الشبكات

عزيزي الدارس، لكي تقوم الشبكة بأداء وظائفها بشكل صحيح فإنه يتم عادة تكليف مجموعة من مهندسي الشبكات بمسئولية تشغيل وصيانة الشبكة. وكلما زادت عمليات التوسع في الشبكة، زادت مشاكلها وبالتالي زادت الأعباء الوظيفية على مهندسي الشبكة. إذ **يجب عليهم الإلمام بكميات ضخمة من المعلومات حول الشبكة**. ولهذا السبب يأتي دور علم إدارة الشبكات فهو **علم نشأ لمساعدة مهندسي الشبكات** على أداء وظائفهم المهنية.

إن الهدف من بناء شبكة البيانات هو **تحقيق احتياجات المؤسسة من توفير عمليات الاتصال**. ولتحقيق ذلك فإنه يجب على مهندس الشبكة إجراء العمليات الضرورية لتخطيط الشبكة. إذ يقوم مهندس الشبكة بإجراء عملية مسح Survey شاملة لأماكن تجمع المستخدمين. حتى يمكن إضافة ملحقات للشبكة الموجودة وتحقيق الاتصال بالأماكن الجديدة المطلوبة. وبعد وضع خطة تطوير إنشاء الشبكة نجد أن:

مهندس الشبكة يقوم بتنفيذ الوظائف التالية لبناء شبكة المعلومات:

- **تجهيز مخطط الشبكة.**
- **تحديد وسائل الصيانة.**
- **دراسة إمكانية التوسعة.**
- **وضع خطة صيانة الأعطال.**
- **دراسة الجدوى الاقتصادية وتحديد التكاليف.**

يقوم مهندس الشبكة أولا باستخدام خطة الشبكة وتحديد التوصيلات المطلوبة وكذلك العتاد والبرامج اللازمة لتشغيل الشبكة. ويوجد **نوعان من تقنيات طرق توصيل الشبكات هما:**

أن يتم إنشاء شبكة محلية LAN (Local Area Network)، أو أن يتم إنشاء شبكة واسعة WAN (Wide Area Network). إن الشبكة المحلية تقوم بتوصيل الحاسبات معا بسرعة مداها يتراوح من 4 ميجا بايت / الثانية إلى 155 ميجا بايت / الثانية (4MB_____155MB). وهي توصل المستخدمين لمسافات قصيرة نسبيا. أما الشبكة الواسعة فهي تعمل عند سرعات نقل بيانات تتراوح من 9.6 كيلوبت / ثانية إلى أكثر من 45 ميجا بت / الثانية. وهي توصل المستخدمين لمسافات أطول. إن الشبكة الواسعة عادة توصل مجموعات من الشبكات المحلية مع بعضها من عدة أماكن متفرقة.

بعد بناء الشبكة فإن مهندس الشبكة سوف يحتاج متابعة عملية صيانتها. فمثلا قد تتغير برامج تشغيل الشبكة أو أجهزة الحاسبات المتصلة بها، أو قد يتم توسعة الشبكة أو قد يحدث أعطال أو إجراء عملية إحلال لأجزاء تالفة من الشبكة. إن تغير احتياجات مستخدمي الشبكة عادة سوف يؤثر في خطة إنشاء الشبكة، وهذا بدوره يتطلب خطة لتوسعة الشبكة. **إن عملية توسعة الشبكة الموجودة فعليا يكون عادة أفضل من إعادة تصميم وبناء شبكة أخرى جديدة.** وعلى مهندس الشبكة أن يأخذ هذه العوامل في الاعتبار وأن يستخدم الحلول السليمة لمعالجة إجراءات توسعة الشبكة. كما يجب أن تتوفر لمهندس الشبكة القدرة المعرفية والاطلاع على المنتجات الجديدة، و إمكانية إحلال منتج جديد محل الأجزاء المتهالكة من الشبكة. وذلك بهدف تحقيق العمليات الاقتصادية في الموارد المتاحة وتحقيق خدمة أفضل لمستخدمي الشبكة بكلفة مناسبة. كما يجب على مهندس الشبكة استخدام الأدوات المناسبة اللازمة لفحص أعطال الشبكة وصيانتها.

3. مهام مدير إدارة الشبكة

تستخدم التعبيرات: مدير إدارة الشبكة Network Administrator، اختصاصي الشبكات Network Specialist، ومحلل الشبكات Network Analyst، لتشير الى التنظيم الوظيفي للمهام التي يقوم بها المهندسون المتخصصون في شبكات الحاسبات. والذين يؤدون مهام متعلقة بإدارة الشبكة. إن مديري الشبكات يؤدون أعمالا تكافئ المهام التي يؤديها مديرو النظم System Administrators.

وتشمل صيانة العتاد والبرمجيات الخاصة بالشبكة. ويشمل أيضا رصد وتهيئة مكونات وعناصر الشبكة. كما أنهم مسؤلون عن تخصيص العناوين لأجهزة الشبكة وتحديد جداول تهيئة الموجهات وعمليات تفويض الشبكةAuthorization. أما إخصائيوا ومحللو الشبكات، يتركز عملهم في تقييم أمن الشبكة وفحص الأعطال وتشخيص مشاكل الشبكة، وكذلك صيانة العمليات المتعلقة بالتفويض، وعمل النسخ الاحتياطي Backup لنظم الشبكة.

4. أهداف إدارة الشبكات

عزيزي الدارس، تقوم المؤسسات والهيئات عادة باستثمار أموال كثيرة وبذل الوقت والجهد في بناء شبكات البيانات. بالإضافة إلى تعيين مهندس أو أكثر لصيانة هذه الشبكات. وقد يكون من الأفضل من ناحية التكلفة أن يقوم النظام الشبكي نفسه بالنظر آليا بفحص بعض العمليات التي تؤدى داخله. وهذه الترتيبات يمكن أن تخفف العبء الواقع على مهندسي صيانة الشبكات. من هذه الفكرة نشأ علم إدارة الشبكات. إن علم إدارة الشبكات هو العلم الخاص بعمليات التحكم في شبكات البيانات المعقدة بهدف زيادة كفاءتها وإنتاجيتها.

وقد قامت المؤسسة الدولية للقياسات (ISO Organization for Standardization International).

بتقسيم وظائف إدارة الشبكات إلى خمسة وظائف أساسية هي:

- إدارة الأعطال Fault Management.
- إدارة التهيئة Configuration Management.
- إدارة الأمن Management. Security
- إدارة الأداء Performance Management.
- إدارة الحساباتAccount Management.

1.4 إدارة الأعطال

عزيزي الدارس، تكون وظيفة إدارة الأعطال **هي تحديد مكان المشكلة المسببة للعطل في شبكة البيانات** وذلك باتباع الخطوات التالية:

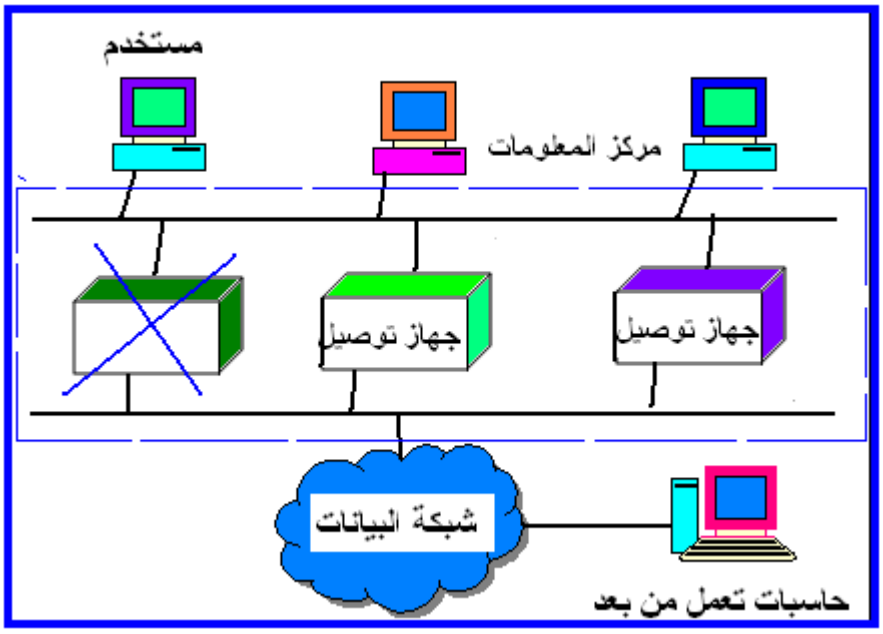
- اكتشاف المشكلة.
- عزل المشكلة.
- علاج المشكلة (إن أمكن).

ويستطيع مهندس الشبكة أن يستخدم أدوات إدارة الأعطال في تحديد مكان وحل مشكلة الأعطال بسرعة أكبر مما كان متوقعا بدون استعمال هذه الأدوات.

مثال على ذلك، نفترض أنه عندما يبدأ المستخدم عملية التشغيل، فإنه يطلب الدخول إلى الشبكة من عدة أجهزة متصلة بالشبكة، وقد يحدث أن تتوقف الشبكة فجأة. عندما تحدث هذه الحالة، يقوم المستخدم بإبلاغ هذه المشكلة لمهندس الشبكة، كي يقوم مهندس الشبكة بعزل هذه المشكلة وحلها.

بدون استعمال أدوات إدارة الأعطال، فإن **مهندس الشبكة يقوم بتحديد سبب المشكلة. هل هو بسبب أن المستخدم قام بكتابة أوامر التشغيل خطأ، أم أنه قام بمحاولة الدخول إلى مكان غير مسموح به في الشبكة.** إذا لم يجد مهندس الشبكة أن الخطأ ناتج بسبب سوء استعمال من المستخدم. فإن مهندس الشبكة يقوم بفحص الأجهزة الموجودة بين

وصلة المستخدم والشبكة. بغرضِ أنه وجد أن السبب هو وصلة اتصال المستخدم بالشبكة كما هو موضح في شكل1.2.



شكل1.2 استخدام أدوات إدارة الأعطال في تحديد مكان العطل وعزله.

وبالرجوع إلى مسار وصلة المستخدم بالشبكة، وجد أن وصلة المستخدم مفصولة. وعندما يقوم مهندس الشبكة بتوصيلها فإن المستخدم يستطيع الدخول إلى الشبكة والعمل بشكل صحيح. وبذلك يتم تصليح العطل.

ولكن باستعمال أدوات إدارة الأعطال فإنه كان من الممكن تصليح هذا العطل بسرعة أكثر، حتى دون أن يتم الإبلاغ عن مثل هذا العطل.

أسئلة تقويم ذاتي

ما دور مهندس الشبكات ؟
ما وظائف إدارة الشبكات ؟
كيف يتم تحديد مكان المشكلة في إدارة الأعطال ؟

2.4 إدارة التهيئة

عزيزي الدارس، إن تهيئة أجهزة شبكة بيانات معينة **يعني التحكم في سلوكيات أجهزة هذه الشبكة**. حيث إن إدارة التهيئة هي عملية إيجاد وضبط (تهيئة) Setting up لهذه الأجهزة الحرجة Critical Devices. على سبيل المثال، بفرض أن أحد الإصدارات البرمجية من نوع الإصدار A، موجود في جسر شبكة إثرنيت يسبب مشاكل في أداء الشبكة. ولتصليح هذه المشكلة الشاذة Anomaly، فإن منتجي هذا الصنف من الجسر قد أصدروا برمجيات تحديث، هو الإصدار B، وهذا يتطلب تنصيب Installing برمجيات دائمة Firmware جديدة في كل خمسون جسر متصل متصلة بالشبكة.
وطبقا لهذا، فإنه تم التخطيط لعمل ذلك في الشبكة. ولكن أولا، فإن مهندس الشبكة يحتاج تحديد نوع الإصدار البرمجي الموجود في كل جسر. ولكن لا يوجد أدوات إدارة تهيئة فاعلة. ولهذا فإنه يجب عليه أن يعمل ذلك فعليا بنفسه لكل قنطرة.

إن أدوات إدارة التهيئة تقوم بتزويد مهندس الشبكة بقائمة بأسماء الجسور المتصلة بالشبكة موضحا بها نوع الإصدار البرمجي الحالي المستخدم في كل جسر، وهذا يسهل معرفة مكان القنطرة المراد تغيير الإصدار البرمجي الجديد لها. و يوضح جدول1.1 بعض معلومات إدارة التهيئة التي تساعد لهذه الحالة.

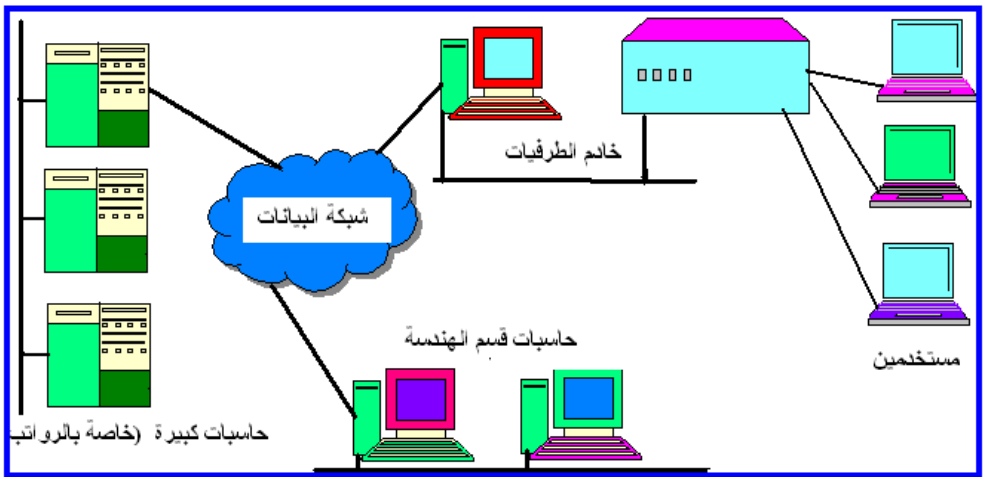
جدول1.1 يبين بعض معلومات إدارة التهيئة (اسم القنطرة ونوع إصدار البرنامج).

معلومات إدارة التهيئة	
Bridge Name اسم القنطرة	Software Version نوع إصدار البرنامج
مشترك 1	A
موقع 20	B
موقع 30	B
مشترك 5	A
موقع 50	B
مشترك 15	A
.....	.....
.....	.....

3.4 إدارة الأمن

عزيزي الدارس، إن إدارة الأمن هي عملية **التحكم في الوصول إلى المعلومات المخزنة في شبكة البيانات.** إن بعض المعلومات المخزنة في أجهزة الحاسبات المتصلة بالشبكة ربما يكون من غير المناسب أن يطلع عليها كل المستخدمين. فربما تشمل هذه المعلومات الحساسة على سبيل المثال تفاصيل عن منتجات جديدة للشركات، أو قد تحتوى على قواعد بيانات تخص العملاء بالشركة.

على فرض أن مؤسسة ما قد قررت استخدام وسائل إدارة الأمن كي تسمح للأجهزة الطرفية البعيدة بالاتصال بالشبكة من خلال خطوط الاتصال بخادم الوحدات الطرفية Terminal Server وذلك لمجموعة من المهندسين، كما هو موضح في الشكل1.3.



شكل1.3 استخدام أدوات الأمن لرصد الاتصال بحاسبات خادم الطرفيات.

يستطيع المهندسون الدخول إلى جهاز الحاسب لأداء عملهم من خلال الاتصال بخادم الطرفيات. بعد أسابيع قليلة، قام مدير المؤسسة بالإبلاغ عن أنه قد تم محاولات عديدة خاطئة بالاتصال بخادم الطرفيات المستخدمة من قبل المهندسين. وأن خادم الطرفيات لم يسمح بتوصيل أي حاسب بالشبكة، تاركا حاسب الهدف المضيف يمنع توصيل المعلومات الحساسة. وبذلك لا أحد من المهندسين يتمكن من التوصيل إلى حاسب الرواتب Payroll.

كمحاولة أولى، يمكن استخدام أدوات إدارة التهيئة لتحديد وسيلة التوصيل بخادم الطرفيات. ولكن للكشف عن من هو الذي يقوم بمحاولة الوصول إلى حاسب بيان الرواتب Payroll، سوف ينبغي على مهندس صيانة الشبكة أن يدخل إلى خادم الطرفيات بشكل دوري وتسجيل أي من المهندسين يقوم باستخدامه. يقوم مهندس الشبكة بعمل ترابط Correlation الأوقات التي يتم فيها محاولات دخول غير ناجحة ومعرفة من هو متصل بخادم الطرفيات.

إن إدارة الأمن ستعطي مهندس الشبكة وسيلة لرصد Monitoring نقط الاتصال Access Points على خادم الطرفيات وتسجيل المتصلين بخادم الطرفيات بصفة

دورية. كما أن إدارة الأمن تزود مهندس الشبكة بتحذيرات صوتية Sound Alarms للتنبيه باحتمالات قوية قد حدثت أو سوف تحدث في الشبكة لخرق أمن الشبكة.

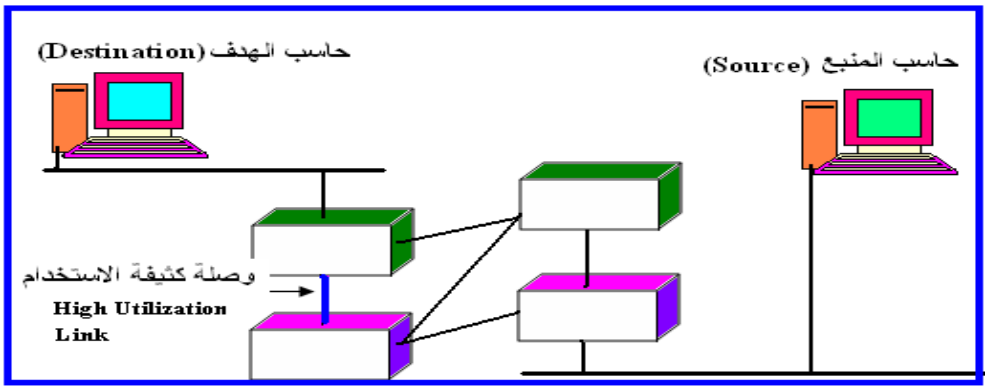
4.4 إدارة الأداء

تتضمن إدارة الأداء إجراءات لقياس أداء عتاد الشبكة والبرمجيات والوسط. من أمثلة هذه القياسات : قياس سرعة أداء الشبكة Throughput – قياس معدل الأخطاء Error Rates – قياس نسبة الاستخدام Percentage Utilization – قياس زمن الاستجابة Response Time. وباستخدام معلومات إدارة الأداء، يستطيع مهندس الشبكة التأكد من أن الشبكة تتوفر لها السعة اللازمة لاحتواء احتياجات المستخدمين.

مثال:

بفرض أن أحد المستخدمين **يشتكي من أن أداء نقل الملفات** عبر الشبكة **يتم ببطء. بدون وسيلة إدارة الأداء، فإن مهندس** الشبكة يجب عليه أولا النظر في أعطال الشبكة. إذا لم يجد أعطال بالشبكة، فإنه سوف يقوم بتقييم أداء كل الأجهزة والوصلات الموجودة بين أجهزة الطرفيات التي يستخدمها العميل والشبكة. **وأثناء عملية الفحص،** يمكنه اكتشاف أن متوسط استعمال أحد الوصلات Link Utilization كان قريبا جدا من سعته.

فيقرر بعد ذلك أن حل هذه المشكلة يكون بتحديث الوصلة الحالية بأخرى جديدة ذات سعة أكبر. يبين شكل1.4 شبكة البيانات والوصلة المطلوب تغييرها.



شكل1.4 يستخدم مهندس الشبكة أدوات إدارة الأداء لتحديد وصلة بين حاسب الهدف وحاسب المصدر تسبب مشكلة في معدل الاستخدام (بطئ في الاتصال).

أما إذا توفرت وسيلة لإدارة الأداء، فإن مهندس الشبكة كان باستطاعته كشف هذا العيب مبكرا. وأن يعرف أن السبب هو سعة الوصلة، وذلك قبل أن تحدث المشكلة ويؤثر ذلك العيب على أداء الشبكة.

5.4 إدارة الحسابات

عزيزي الدارس، تختص إدارة الحسابات بمتابعة كل مستخدم أو مجموعة من المستخدمين باستعمال مصادر الشبكة للتأكيد من أن المستخدمين يتوفر لهم مصادر شبكية كافية. كما تكون أيضا مسئولة عن منع أو منح الصلاحية بالتوصيل بالشبكة.

مثال: بفرض أن مهندس الشبكة يحتاج تحديث الوحدة البينية لخادم شبكة قسم الملفات لأنها وصلت إلى السعة القصوى لمعالجة حزم البيانات.

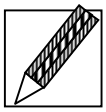
بدون وسيلة أداء الحسابات، فإن مهندس الشبكة لن يستطيع معرفة أي من المستخدمين يكون له عملاء Clients يقومون بتوصيلهم إلى خادم الملفات. لذلك فإن مهندس الشبكة يسأل المستخدمين ليعرف من منهم يكون له حاسب عميل يقوم بالتوصيل بخادم الملفات بشكل منتظم. ونتيجة لهذا الاستطلاع، يكتشف مهندس الشبكة أن فريق قسم التوثيق، يكون له عملاء عديدون هم الذين يستعملون أجهزة حاسبات متصلة بخادم الملفات.

وبذلك يجد مهندس الشبكة أن هذه الحركة Traffic هي التي تمثل تقريبا نصف الحمل الواقع على الوحدة البينية لشبكة خادم الملفات.

يمكن لمهندس الشبكة أن يقرر إعطاء فريق التوثيق خادم ملفات خاص بهم، يستطيع مواجهة حركة الشبكة Network Traffic ويترك باقي الشبكة بدون تغيير. بالإضافة إلى أن مهندس الشبكة يمكن أن يقرر تحديد مكان خادم ملفات جديد في نفس قطاع الشبكة لخدمة فريق التوثيق، والذي يمكن أن يقلل حركة الشبكة في قسم التوثيق.

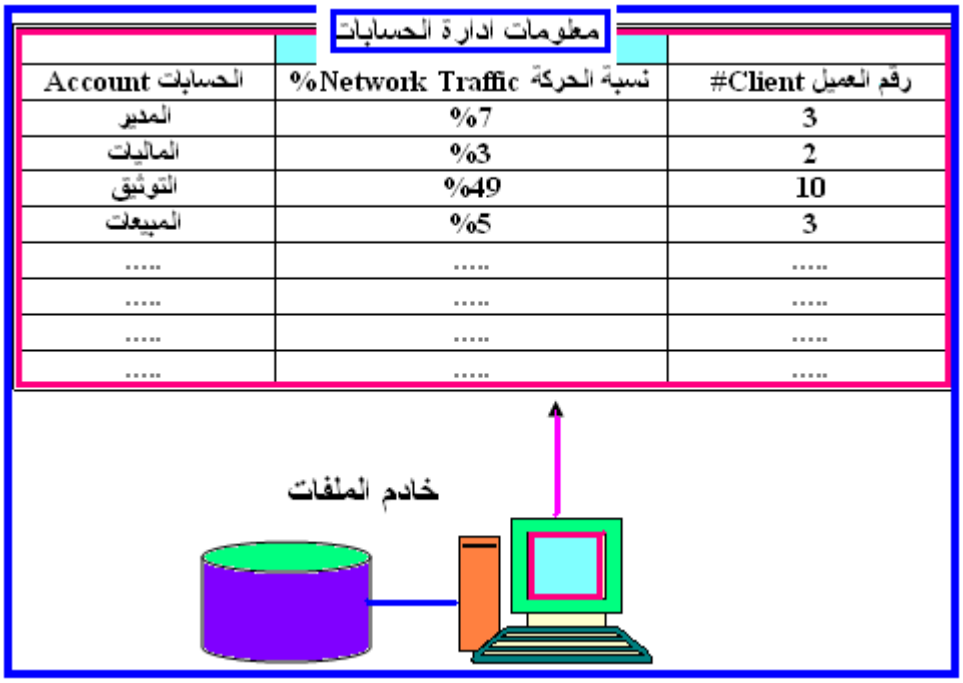
باستخدام أدوات إدارة الحسابات، يستطيع مهندس الشبكة بسرعة معرفة أن قسم فريق التوثيق يقوم بالاتصال بخادم الملفات بمجموعة كبيرة من العملاء بشكل منتظم. وبذلك يستطيع معالجة هذا الوضع بأسرع وقت ممكن. يوضح شكل1.5 بعض المعلومات التي يوفرها نظام إدارة الحسابات بالشبكة.

تدريب (1)



أجب بلا أو نعم :

1. يحدد مهندس صيانة الحاسب الالى مخطط الشبكة
2. يحدد مهندس الشبكة خطة صيانة الاعطال فى الشبكة
3. من مهام مدير الشبكة عمل النسخ الاحتياطية لنظم الشبكة
4. من مهام مدير الشبكة عمل دراسة جدوى لاهمية الشبكة
5. من مهام مدير الشبكة عمل تقييم أمن الشبكة
6. من مهام مدير الشبكة عمل رصد وتهيئة مكونات وعناصر الشبكة
7. الجمعية العالمية لمهندسى الالكترونيات قسموا وظائف الشبكة إلى خمسة أقسام
8. إدارة الامن تعني التحكم في سلوكيات الشبكة
9. إدارة الأداء تعني التحكم في سلوكيات الشبكة
10. إدارة الأمن أيضأ تعني الوصول الي المعلومات بسلامة
11. إدارة الأداء تعمل علي حساب نسبة الاستخدام



شكل1.5 يستخدم مهندس الشبكة أدوات إدارة الحسابات في تحديد المستخدم الذي يهيمن على خادم الملفات.

5. بروتوكولات إدارة الشبكة

إن أحد العوامل الضرورية لتحقيق أهداف إدارة الشبكة هو القدرة على الحصول على معلومات عن تأثير التغير في أجهزة الشبكة. إن بروتوكول إدارة الشبكة البسيط، يحدد شكل البيانات الشائعة والمعاملات التي تسمح باسترجاع المعلومات بسهولة. وإن بروتوكولات الشبكة الأكثر تعقيدا تستطيع إضافة بعض القدرات المختلفة بالإضافة إلى وسائل أمن لحماية المعلومات المطلوبة ومنع أي شخص من إجراء تغييرات عليها. إن **البروتوكولات المتطورة** لإدارة الشبكة، يكون **لديها القدرة على تنفيذ وظائف إدارة الشبكة عن بعد بشكل لا يعتمد مطلقا على مستويات بروتوكول الشبكة.** لذلك فإن كل أجهزة الشبكة بغض النظر عن بروتوكول الشبكة يمكن إدارتها.

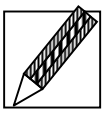
لقد تم تطوير العديد من البروتوكولات القياسية لإدارة الشبكة والتي تساعد على استخلاص Extract المعلومات الضرورية من كل أجهزة الشبكة.ومن هذه البروتوكولات الأكثر شيوعا:

- بروتوكول إدارة الشبكة البسيط SNMP (Simple Network Management Protocol) **ويوجد منه ثلاثة إصدارات :**

  أحدثهم هو الإصدار الثالث SNMPv3.

- وبروتوكول إدارة المعلومات الشائع CMIP (Common Management information Protocol) أو بروتوكول خدمات إدارة المعلومات الشائع CMIS (Common Management Information Services). ويفضل استخدام بروتوكول SNMP عن البروتوكول CMIS/CMIP، وذلك لأن البروتوكول CMIS/CMIP محدود الاستخدام بسبب صعوبة تنفيذه.

تدريب (2)



أجب بلا أو نعم :

1) تستخدم شبكة البيانات بروتوكولات قياسية لإدارة الشبكة منها برتوكول IBM
2) تستخدم شبكة البيانات بروتوكولات قياسية لإدارة الشبكة منها برتوكول Win xp
3) . تستخدم شبكة البيانات بروتوكولات قياسية لإدارة الشبكة منها برتوكول SNMP
4) تستخدم شبكة البيانات بروتوكولات قياسية لإدارة الشبكة منها برتوكول CMIP
5) من أشهر وأبسط البروتوكولات القياسية لإدارة شبكة البيانات هو: برتوكول CMIS
6) من أشهر وأبسط البروتوكولات القياسية لإدارة شبكة البيانات هو برتوكول CMIP
7) من أحد أشهر وأبسط البروتوكولات القياسية لإدارة شبكة البيانات هو: برتوكول SNMP

الخلاصة

عزيزي الدارس، تعرفنا في هذه الوحدة على وظائف شبكة البيانات، وعددنا المهام الوظيفية لمهندس الشبكة، ثم تعرفنا على وظائف علم شبكات البيانات واوضحنا بالامثلة وظائف الشبكة، وبعدها تناولنا بالشرح المؤسسة الدولية للقياسات ISO (International Organization for Standardization) وتقسيم **وظائف إدارة الشبكات إلى خمسة وظائف أساسية هي:**

- إدارة الأعطال Fault Management
- إدارة التهيئة Configuration Management
- إدارة الأمن Security Management
- إدارة الأداء Performance Management
- إدارة الحساباتAccount Management

ثم تعرفنا على أدوات إدارة الشبكة ومنها بينا وظائف إدارة الأعطال وإدارة التهيئة والحسابات ودرجنا بعدها لإدارة الأداء وإدارة الأمن وفي القسم الأخيرأوضحنا كيفية إدارة الشبكة بكفاءة عالية.

لمحة مسبقة عن الوحدة القادمة

عزيزي الدارس، في الوحدة القادمة سنشرح عملية إدارة الشبكات بالتفصيل. ونشرح الفرق بين نظام إدارة الشبكة وتطبيقات إدارة الشبكة. حيث إن لكل منهما الأهداف الخاصة به والتي يجب تحقيقها. وسنتناول شرح ثلاثة أنواع من بناء وعمارة الشبكات هما: الإدارة المركزية – الإدارة الهرمية – والإدارة الموزعة.

،كن معنا في الوحدة القادمة وستجد الكثير المفيد إنشاالله .

إجابات التدريبات

تمرين (1)

السؤال	1	2	3	4	5	6	7	8	9	0	1
الاجابة	لا	نعم	لا	لا	لا	نعم	لا	لا	لا	لا	نعم

تمرين (1)

السؤال	.1	.2	.3	.4	.5	.6	.7
الاجابة	نعم	لا	لا	نعم	نعم	لا	لا

مسرد المصطلحات

إدارة الأعطال Fault Management

هي تحديد مكان المشكلة المسببة للعطل في شبكة البيانات وذلك باتباع الخطوات التالية:اكتشاف المشكلة، عزل المشكلة وعلاج المشكلة.

إدارة التهيئة Configuration Management

يعنى التحكم في سلوكيات أجهزة هذه الشبكة. حيث إن إدارة التهيئة هي عملية إيجاد وضبط (تهيئة) Setting up لهذه الأجهزة الحرجة.

إدارة الأمن Security Management

التحكم في الوصول إلى المعلومات المخزنة في شبكة البيانات. إن بعض المعلومات المخزنة في أجهزة الحاسبات المتصلة بالشبكة ربما يكون من غير المناسب أن يطلع عليها كل المستخدمين.

إدارة الأداء Performance Management

تتضمن إدارة الأداء إجراءات لقياس أداء عتاد الشبكة والبرمجيات والوسط. من أمثلة هذه القياسات : قياس سرعة أداء الشبكة – قياس معدل الأخطاء– قياس نسبة الاستخدام – قياس زمن الاستجابة.

إدارة الحسابات AccountManagement

تختص إدارة الحسابات بمتابعة كل مستخدم أو مجموعة من المستخدمين باستعمال مصادر الشبكة للتأكيد من أن المستخدمين يتوفر لهم مصادر شبكية كافية. كما تكون أيضا مسئولة عن منع أو منح السماحية بالتوصيل بالشبكة.

المصطلح بالإنجليزية	معناه بالعربية
Account Management	إدارة الحسابات
Access Points	نقط الاتصال
ATM (Automatic Teller Machines	آلات الصراف الآلي
Anomaly	شاذة
Bridge Name	اسم القنطرة
Management Configuration	إدارة التهيئة
Critical Devices	الأجهزة الحرجة
Correlation	ترابط
Clients	عملاء
CMIP (Common Management Information Protocol)	بروتوكول إدارة المعلومات الشائع
CMIS (Common Management Information Services)	خدمات إدارة المعلومات الشائعة
Error Rates	معدل الأخطاء
Fault Management	إدارة الأعطال
Firmware	مكونات مرنة
Installing	تنصيب
LAN (Local Area Network)	شبكة محلية
Monitoring	رصد
Network Traffic	حركة الشبكة

المصطلح بالإنجليزية	معناه بالعربية
Payroll computer	حاسب الرواتب
Performance Management	إدارة الأداء
Percentage Utilization	نسبة الاستخدام
Security Management	إدارة الأمن
Setting up	وضع (تهيئة)
Software Version	نوع إصدار البرنامج
Sound Alarms	تحذيرات صوتية
SNMP (Simple Network Management Protocol)	بروتوكول أدارة الشبكة البسيط
Survey	مسح
Terminal Server	خادم الطرفيات
Throughput	سرعة أداء الشبكة
Traffic	الحركة (المرور)
Response Time	زمن الاستجابة
WAN (Wide Area Network)	شبكة إقليمية

المراجع

1- Managing Computer Networks: A Case-Based Reasoning Approach, By Lundy Lewis. Artech House Publishers 1995, ISBN-10: 0890067996.

2- Network Management Systems Essentials, By Divakara K. Udupa., *McGraw-Hill, 1996. ISBN 0-07-065766-1.*

3- Applications for Distributed Systems and Network Management, by Kornel Terplan, Jill Huntington-Lee., 1994, ISBN: 978-0-471-28639-4.

4- Object-Oriented Networks: Models for Architecture, Operations, and Management, By Subodh Bapat. Prentice Hall 1994, ISBN-10: 0130310972.

5- LAN Operations: A Guide To Daily Management, By Peter D. Rhodes. 1991, ISBN: 0201563010).

6- Network Management: A Practical Perspective, by Allan Leinwand, Karen Fang-Conroy. Addison Wesley 1996, ISBN-10: 0201609991.

7- Internet System Handbook, By Marshall T. Rose, Daniel C. Lynch (Editor). Addison-Wesley Professional 1992,ISBN-10: 0201567415.


الوحدة الثانية
نظام إدارة الشبكات

محتويات الوحدة

مقدمة

تمهيد

عزيزي الدارس، مرحبا بك إلى هذه الوحدة التي نشرح فيها نظام إدارة الشبكات بالتفصيل. ونشرح الفرق بين نظام إدارة الشبكة وتطبيقات إدارة الشبكة، حيث إن لكل منهما الأهداف الخاصة به والتي يجب تحقيقها. وسنتناول شرح ثلاثة أنواع من بناء وعمارة الشبكات هما: الإدارة المركزية – الإدارة الهرمية – والإدارة الموزعة. والغرض الشمولي من دراسة هذه الوحدة هو أن يتمكن الدارس من اختيار نظام إدارة الشبكة وتطبيقاتها المناسبة والتي تفي باحتياجاته واحتياجات المؤسسة أو الهيئة التي يعمل بها.

أهلا بك مرة أخرى إلى هذه الوحدة عسى أن تنتفع بها وأن تفيد منها، وأن تساعدنا في نقدها وتطويرها .

أهداف الوحدة

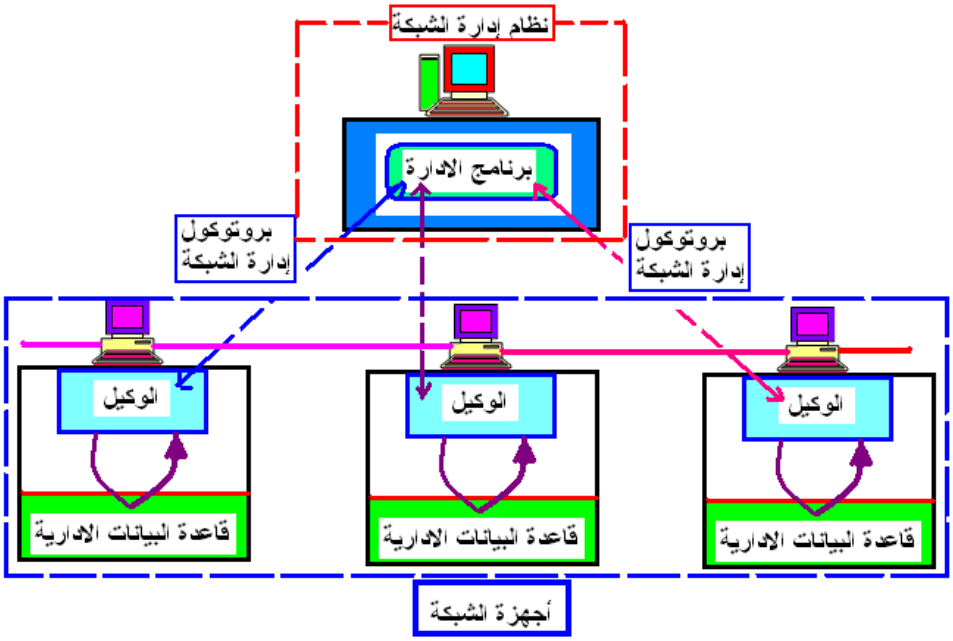
عزيزي الدارس، بعد فراغك من دراسة هذه الوحدة ينبغي أن تكـــون قادرا على أن :

- تعرف وظائف نظام إدارة الشبكات.
- تصف مكونات نظام إدارة الشبكة.
- تعدد طرق التفاعل بين إدارة الشبكة وأجهزة الشبكة.
- تبين المهام الوظيفية لبرنامج إدارة الشبكات.
- تحدد المكونات الأساسية لبرنامج إدارة الشبكات.
- تشرح بعض الأمثلة لتوضيح وظائف برنامج إدارة الشبكة.
- تفرق بين انواع معمارية الشبكات الثلاثة .
- تفهم كيفية اختيار نظام إدارة الشبكة.
- تصف هيكلية نظام إدارة الوسط الموزع DME، والخدمات الموزعة.
- تشرح نظام إدارة شبكات الاتصال TMN ومستويات إدارتها.

1. مكونات نظام إدارة الشبكة

عزيزي الدارس، إن معظم المكونات المعمارية المستخدمة لبناء نظام إدارة شبكات البيانات، تتكون من بناء هيكلي كما هو موضح في شكل 2.1. وتشمل ما يلي:

- محطة إدارة الشبكة: وهي عبارة عن حاسب مركزي يوجد به برامج الإدارة والتحكم.
- الأجهزة التي يتم إدارتها، وهي تشمل العناصر المكونة لشبكة البيانات، مثل الموجهات Routers، والبوابة السريعة Gateway،على سبيل المثال.
- بروتوكول الاتصال بين محطة إدارة الشبكة، وأجهزة الشبكة. وأشهر هذه البروتوكولات هو بروتوكول الشبكة البسيط SNMP.
- مجموعة المعاملات Parameters، المطلوب رصدها لإجراء عمليات التحكم الإدارية اللازمة لأجهزة الشبكة.



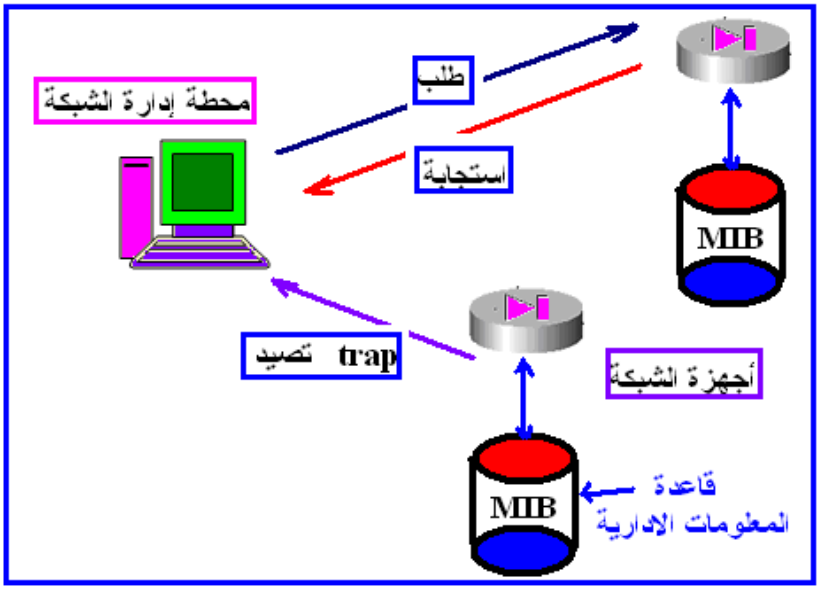
شكل2.1 مكونات نظام إدارة الشبكة.

ويوجد في كل جهاز شبكة يتم إدارته برنامج يسمى الوكيل Agent، وقاعدة بيانات. حيث يقوم برنامج الوكيل بمعالجة وتخزين معلومات عن جهاز الشبكة المطلوب إدارته. ويقوم بتزويد هذه المعلومات إلى نظام إدارة الشبكة عن طريق بروتوكول إدارة الشبكة. كما يقوم برنامج الوكيل أيضا، بتحديد المعاملات التي يستخدمها نظام إدارة الشبكة لرصد وتهيئة أجهزة الشبكة.

ويوضح شكل 2.2 التفاعلات التي تتم في إدارة الشبكة بين محطة التحكم المركزية الإدارية، وبين أجهزة الشبكة المطلوب إدارتها.

ويوجد طريقتان للتفاعل والاتصال بين وحدة الإدارة المركزية وأجهزة الشبكة هما:

أولا : طريقة الانتخاب Polling: في هذه الطريقة تقوم محطة نظام إدارة الشبكة، إما آليا أو بواسطة مهندس الشبكة، بإرسال استفسارات Queries، لكل وكيل موجود داخل جهاز الشبكة، بطريقة دورية، لفحص قيم معينة عن معلومات الأجهزة. وعيب هذه الطريقة أنها تستهلك جزءاً من سعة النطاق المخصصة لنقل البيانات داخل الشبكة. ويقوم نظام إدارة الشبكة بإرسال طلب Request، إلى جهاز الشبكة، للحصول منه على معلومات بيان حالته، أو لضبط معاملات تشغيل الجهاز. ويقوم جهاز الشبكة بعد ذلك بإرسال رسالة استجابة Reply، تحمل معها بيان حالة الجهاز.



شكل2.2 طرق التفاعل والاتصال بين محطة إدارة الشبكة وأجهزة الشبكة تحت الإدارة.

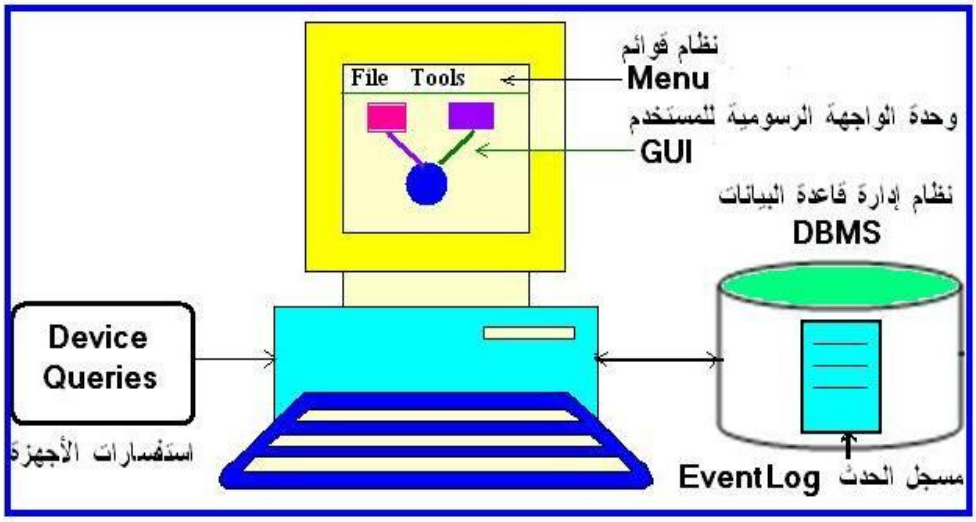
ثانيا :طريقة الولوج Logging: تقوم أجهزة الشبكة بتوليد إشارات تحذير عندما تصل معاملات الأجهزة إلى الحد الحرج، وهذه الإشارات تسمى مصايد Traps. بعد ذلك، تقوم محطة نظام إدارة الشبكة بتسجيل رسالة تنبيه إلى مهندس الشبكة. وهذه الطريقة تستهلك سعة نطاق قليلة. وفور استقبال هذه التحذيرات فإن محطة وحدة التحكم في نظام إدارة الشبكة، يتم برمجتها كي تتعامل مع هذه التحذيرات بواسطة تنفيذ واحد أو مجموعة من الإجراءات، من ضمنها، تنبيه العاملين بالشبكة، تسجيل الأحداث التي وقعت داخل الشبكة، إغلاق النظام عندما يتطلب الأمر ذلك، أو محاولة تصليح وضبط النظام آليا إن أمكن.

2.منصة إدارة الشبكات

Network Management Platform

لقد تعاقبت على إدارة الشبكات من الناحية التاريخية نظم متعددة. كل منها استخدم لإدارة مجموعة معينة من مكونات شبكة البيانات. إن مركز إدارة شبكة نوعية يمكن أن يخصص نظاماً منفصلاً لإدارة أجهزة مكونات الشبكة المختلفة مثل : المودم Modem– مجمع البيانات Data Multiplexer – أجهزة توصيل الشبكة (مثل: المجمع Hub – الموجه Router– القنطرة Bridge – أجهزة أخرى). لكن القيود المادية، والمساحة الفعلية، وإمكانية توفر الخبير التقني كلها عوامل أدت إلى وجود رغبة لامتلاك مكونات شبكية تدار بواسطة نظام منفرد Single System الذي يستطيع أيضا إظهار التوصيلات على خريطة الشبكة. وبغض النظر عن هذه الاحتياجات فقد ظهرت الحاجة إلى وجوب توفر برنامج لإدارة الشبكات. إن برنامج إدارة الشبكات هو عبارة عن حزمة برمجية Software Package توفر الوظائف الأساسية المطلوبة لإدارة الشبكة وعناصرها المتعددة. و لتحقيق هذه الوظائف يجب أن تحتوي الحزمة البرمجية لإدارة الشبكة، كما هو مبين في شكل2.3، على الآتي :

- وحدة الواجهة الرسومية للمستخدم GUI (Graphic User Interface).
- خريطة إظهار الشبكة.
- نظام إدارة قاعدة البيانات.
- نظام قوائم Menu مخصص للمستخدم.
- مسجل الحدث (الأعمال التي تحدث داخل الشبكة) Event Log.



شكل2.3 المكونات الأساسية لبرنامج إدارة الشبكة.

1.2 تبيين محتويات الحزم البرامجية

1.1.2 وحدة الواجهة الرسومية للمستخدم

إن وحدة الواجهة الرسومية للمستخدم تكون مفيدة لعدة أغراض. فهي تجعل المستخدم يتصل بسهولة بخصائص برنامج إدارة الشبكة. ويجب أن تكون وحدة الواجهة الرسومية للمستخدم قياسية Standard، متوافقة مع نظم التشغيل المتعددة مثل ميكروسوفت ويندوز أو نظام أى بى إم أو نظام يونيكس. وأن تكون موثقة ومعتمدة من قبل منتجي برمجيات الشبكات. إن نظم إدارة الشبكات يمكن أن تستخدم لتطبيقات متعددة باختلاف نوع المنتج والشركة المصنعة له. وعندما تصدر التطبيقات البرمجية على شكل موحد شائع، فإن هذا يسهل إدارة النظام والتعامل معه.

2.1.2 خريطة إظهار الشبكة

تكون الخريطة Map مفيدة لكل مساحة إدارة الشبكة، تقريبا. وتوجد على الخريطة عدة ألوانColors. وباستعمال أدوات إدارة الأعطال والألوان على الخريطة يستطيع مهندس الشبكة المساعدة في عزل سبب العطل في الشبكة. إن أدوات إدارة التهيئة تستطيع إظهار التهيئة الفعلية Physical والمنطقية logical للشبكة بطريقة مصورة Pictorially. إن أدوات إدارة الأداء تستطيع بواسطة الجرافيك إظهار أداء حالة الأجهزة والوصلات بواسطة الألوان والصور المتنوعة. وعندما يقوم برنامج إدارة الشبكة بتوفير طريقة آلية للكشف Auto-discovery عن أجهزة الشبكة وبعد ذلك يتم رسم خريطة الشبكة Auto-mapping فإن ذلك تُعتبر فوائد إضافية.

إن تطبيق الطرق القياسية للاستفسار عن أجهزة الشبكة تعتبر ضرورية لأن برنامج إدارة الشبكة يجب أن يكون قادرا على تفسير وتجميع المعلومات عن مكونات وعناصر الشبكة المختلفة التي تصنع من قبل مصنعي ومنتجي هذه المكونات.

3.1.2 نظام قوائم Menu متهيئ للمستخدم

يعمل نظام القوائم المتهيئ للمستخدم الموجود في برنامج إدارة الشبكة على جعل النظام يبدوا مألوفا لدى المستخدم.

4.1.2 نظام إدارة قاعدة البيانات

إن نظام إدارة قاعدة البيانات يساعد في إجراء الوظائف العديدة لإدارة الشبكة. تستطيع التطبيقات استخدام قاعدة البيانات لتخزين المعلومات. ويمكن إنشاء علاقات بين قوائم البيانات التي تساعد برنامج إدارة الشبكة في التشخيص والصيانة. وتسمح كثير من نظم إدارة قواعد البيانات للمستخدمين في توليد تقارير للمستخدم وكذلك عمل نسخ احتياطية Backup بطريقة آلية.

5.1.2 مسجل الحدث Event Log

يستخدم مسجل الحدث لتسجيل الأعمال التي تتم داخل الشبكة مرتبة زمنيا Chronologically في شكل فورمات مقروءة. ويقوم برنامج إدارة الشبكة بكتابة المعلومات في السجل عن أي أحداث معروفة تحدث في الشبكة، كما يمكنه توليد الأحداث الخاصة بشبكته. كما يمكن لأجهزة الشبكة إرسال رسائل غير متزامنة يمكن تفسيرها على أنها أحداث للشبكة. وبغض النظر عن كيفية تعلم البرنامج عن أحداث الشبكة، فإنه يجب على البرنامج توفير سجل للحدث وذلك لمساعدة مهندس الشبكة في معرفة التطورات الجديدة التي تحدث في شروط الشبكة Network Conditions.

2.2 الخصائص التي يجب توفرها في برامج إدارة الشبكة

- أدوات جرافيك .
- وحدة برمجة تطبيقية بينية
- أمن النظام.

1.2.2 أدوات جرافيك Graphic Tools

إن برنامج إدارة الشبكة يجب أن يوفر لمهندس الشبكة الوسائل المعينة له كي يستطيع إنشاء رسومات بيانية للبيانات بأشكال متعددة منها الرسم الخطي Line Drawing – رسم قضيبي Bar Drawing – رسم الكعكي Pie Chart Drawing. وكذلك إمكانية لدمج الرسومات البيانية مع التقارير. وهذا يكون ذا فائدة كبيرة حيث إن المديرين عادة تفضلون رؤية المعلومات على شكل رسومات بيانية بدلا من تقديم هذه المعلومات على شكل تقارير نصية Text. إن الرسومات البيانية التي توضح حركة الشبكة Network Traffic الحالية ومعدلات الأخطاء، تساعد كثيرا في إدارة الأعطال وإدارة الأداء. وأن الرسومات البيانية التي تمثل بيانات سابقة تساعد في تكوين الاتجاه نحو عزل الشبكة من عدمه.

2.2.2 وحدة البرمجة التطبيقية البينية

API (Application Programming Interface)

إن وحدة API هي عبارة عن مكتبة برمجية تسمح بالوصول إلى المعلومات التي يتم الاحتفاظ بها داخل برنامج إدارة الشبكة. تستطيع البرامج الخارجية من خلال API استخدام خريطة الشبكة، والاتحاد مع قائمة Menu النظام، وتخزين واسترجاع المعلومات من قاعدة البيانات وإرسال رسائل إلى مسجل الحدث Event Log. وبذلك فإن برنامج API يكون مهما لسببين هما:

أولا :يمكنها التكامل مع التطبيقات التي تباع مع منتجات الشبكة.

ثانيا :تسمح للمهندس بكتابة البرامج الخاصة بهم والتي تناسب الوسط المحيط.

ويفضل أن تكون وحدة API ذات معايير قياسية وتصلح للاستخدام مع العديد من برامج إدارة الشبكات. ويعتبر برنامج OSF DME مثالاً مناسباً يحقق المواصفات القياسية لوحدة API من أجل برنامج إدارة الشبكة.

3.2.2 أمن النظام System Security

أحد الخواص الهامة لبرنامج إدارة الشبكة هو أن يحتوي على نظام لتحقيق الأمن لنفسه داخل الشبكة. إن برنامج إدارة الشبكة والتطبيقات المصاحبة لها تحتوي على معلومات هامة جدا عن الشبكة تشمل: بيانات تهيئة أجهزة مكونات الشبكة – أمن الشبكة وتطبيقاتها – بيانات الأداء – طرق الحسابات وغيرها. وهذه المعلومات تكون مفيدة لقراصنة Crackers الشبكة الذين قد يحاولون اقتحام أمن الشبكة. إن الجزء المتعلق بأمن برنامج إدارة الشبكة يفضل أن يكون إضافي إلى ما يستطيع أن يقدمه نظام التشغيل من توفير وسائل للحماية والأمن.

إن الوظائف الأساسية لبرنامج إدارة الشبكة يجب أن تمكن مهندس الشبكة من تحقيق كل الأعمال المتعلقة بمناطق إدارة الشبكة. ويستطيع مهندس الشبكة أن يستفسر عن كل

معلومات الأجهزة من خلال برنامج إدارة الشبكة. وأن يستخدم هذه المعلومات بعد ذلك بحسب احتياجاته.

مثال : بفرض أن مهندس الشبكة يريد **إنشاء مخطط بياني يوضح علاقة استخدام وصلة توالي** Serial Link Utilization، لكل الوصلات في الشبكة. في هذه الحالة فإنه يتبع الخطوات التالية:

1- يحدد نوع المعلومات التي يحتاجها من كل مكونات الشبكة(عادة يكون عدد الحروف bytes المرسلة أو المستقبلة من كل وحدة بينية Interface).

2- يسجل الأرقام التي تم تحديدها في جدول برنامج إكسل Excel ويحصل على الرسم البياني المطلوب.

وتعتبر الخطوة الأولى هي الأكثر صعوبة. فعلى الرغم من أن برنامج إدارة الشبكة يستطيع استخدام طرق قياسية للاستفسار عن كل مكونات الشبكة، فإن كل مكون ربما يحتفظ بالبيانات بشكل منفرد Unique خاص به فقط. إن الوسط المحيط في مجال الشبكات حاليا ينظم حفظ أجزاء المعلومات على أشكال قياسية تسمى قاعدة المعلومات الإدارية MIB(Management Information Base). وهذا يعني أنه إذا تم معرفة جزء من المعلومات فإن ذلك ينطبق على كل أجهزة الشبكة، على الرغم من أن نظام قاعدة المعلومات الإدارية MIB يحتوي عادة على المئات من أجزاء المعلومات المنفردة Unique والتي تحتاج مزيدا من الفحص لتحديد حالتها.

ويوجد العديد من حزم برامج إدارة الشبكات المتوفرة حاليا في الأسواق،

وفيما يلي أمثلة لبعض هذه البرامج:

- برنامج من إنتاج شركة "صن" هو Sun Connect Sun Net Manager
- برنامج من إنتاج شركة هيوليت بيكارد HP (Hewlett Packard) OpenView
- برنامج من إنتاج شركة أي-بي-أم IBM Netview / AIX
- برنامج شركة أي- آند- تى AT & T StarSentry

إن كلاً من هذه البرامج توفر الخصائص الأساسية التي تم شرحها سابقا، بالإضافة إلى توفير بعض الإضافات. فعلى سبيل المثال، فإن برنامج شركة أي-بى-إم يكون مبنياً على أساس برنامج شركة هيوليت بيكارد، ويستخدم فهرساً يسمح للمستخدمين تتبع مشاكل الشبكة. وأن برنامج شركة "صن" يسمح للمستخدمين بإنشاء رسومات بيانية ثلاثية الأبعاد لتمثيل معلومات الشبكة. وبغض النظر عن المنتجات المختلفة، فإن الهدف من برنامج إدارة الشبكة هو توفير الوظائف العامة الأساسية لإدارة الشبكة ككل بفاعلية وكفاءة.

تدريب (1)

أجب بلا أو نعم فيما يلي :

1) ينبغي أن يحتوي برنامج إدارة الشبكة على المكونات وحدة واجهة رسومية للمستخدم.

2) ينبغي أن يحتوي برنامج إدارة الشبكة على المكونات خريطة لإظهار الشبكة.

3) ينبغي أن يحتوي برنامج إدارة الشبكة على المكونات نظام إدارة قاعدة البيانات.

4) ينبغي أن يحتوي برنامج إدارة الشبكة على المكونات نظام قوائم معالجات الشبكة ومسجل للحدث.

4. معماريات إدارة الشبكة

Network Management Architectures

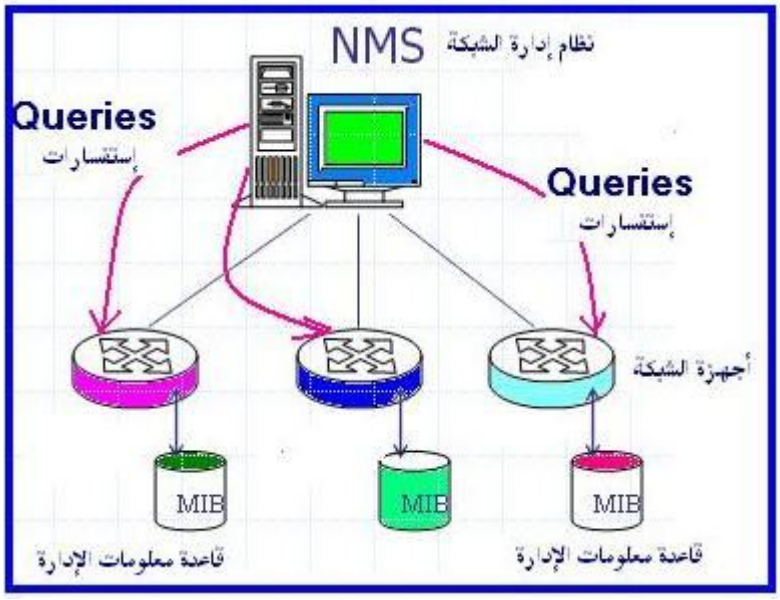
عزيزي الدارس، يستطيع برنامج إدارة الشبكة استخدام معماريات متعددة لأداء وظائفه. ويوجد ثلاثة أنواع شائعة من معماريات إدارة الشبكة هي:

- العمارة المركزية Centralized
- العمارة الهرمية Hierarchical
- العمارة الموزعة Distributed

ولا يوجد في هذه التقسيمات معمارية أحسن من غيرها. فإن كلاً منها له خصائصه التي تجعله يعمل بشكل جيد في الوسط المحيط المناسب له. والقاعدة البديهية هي أن يستخدم النظام المعماري لإدارة الشبكة الذي يكون أقرب إلى الهيكل المؤسسي. حيث إنه في حالات كثيرة فإن هيكل الشبكة يكون في شكل مشابه.

1.3 العمارة المركزية

في البناء المعماري المركزي يتم تنصيب برنامج إدارة الشبكة على نظام كمبيوتري واحد عند الموضع المسئول عن واجبات إدارة كافة الشبكة، كما موضح في شكل2.4 .



شكل2.4 يوضح نموذج بنائي عمارة مركزية لإدارة الشبكة.

يستخدم النظام قاعدة بيانات وحيدة مركزية. من أجل جميع الإضافات، فإن هذا النظام يتم نسخه احتياطيا Backed up على نظام آخر خلال فترات منتظمة. وعلى الرغم من أن النظام المركزي هو نقطة التركيز لإدارة الشبكة، فهو يستطيع السماح بالاتصال وتوجيه الأحداث إلى وحدات إظهار Consoles (وحدة الإظهار هذه عبارة عن شاشة عرض مزودة بوحدة مفاتيح) أخرى تعمل من خلال الشبكة.

مميزات برنامج إدارة الشبكة المركزية :

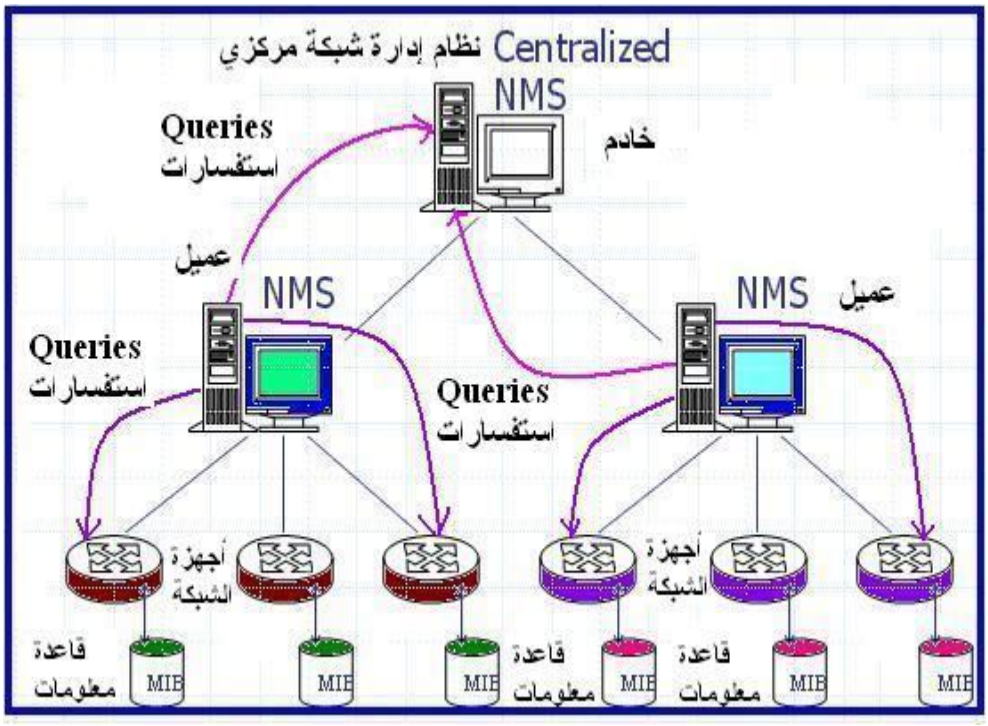
- **يدير الأحداث والإنذارات.**
- **يدير المعلومات.**
- **يدير الاتصال بكل التطبيقات الإدارية.**

ويستطيع مهندس الشبكة استعمال مكان منفرد لمشاهدة جميع التحذيرات Alerts والأحداث التي تكون ذات فائدة لتشخيص وحصر المشاكل. إن وجود مكان وحيد يوصل لكل التطبيقات الإدارية والمعلومات في الشبكة يفي بالغرض ويحقق الوصول Accessibility، وتكون عملية الأمن أكثر سهولة في صيانتها. ومن الناحية الفعلية Physically فإن محطة إدارة الشبكة يمكن أن توضع في مكان مغلق في منطقة محظور دخولها، وأن يسمح بدخولها فقط للمستخدمين المعنيين بالشبكة. إن اعتماد تأدية كل وظائف إدارة الشبكة على نظام مركزي منفرد لا يوفر حماية كافية. لأنه لا يحتوي على نظم فائضة Redundant أو نظم سماحة بالخطأ Fault Tolerant. ولهذا فإنه يجب عمل نسخ احتياطية كاملة Full Backup يتم الاحتفاظ بها في مكان آخر. وعندما يتم زيادة عناصر إضافية للشبكة، ربما يسبب ذلك صعوبة وتكلفة لتوسعة النظام الفردي للتعامل مع الأحمال الضرورية. إن العيب المميز في هذا النظام المعماري المركزي هو أنه يتم الاستفسار عن كل أجهزة الشبكة من مكان واحد. وهذا يسبب وجود عبء حمل حركة Traffic Load على كل وصلات أجهزة الشبكة، وكذلك زيادة عبء الأداء Throughput. وعندما تتأثر وصلات إدارة الشبكة فإن جميع قدرات الشبكة قد تفقد.

ومن أمثلة العمارة المركزية لإدارة الشبكات، هو برنامج شركة أي–بي–إم المسمى IBM NetView الذي يعمل على حاسب مضيف ويحقق كل أنشطة إدارة الشبكة المعمارية من نوع SNA (System Network Architecture). ويستطيع المستخدم تحقيق نقاط اتصال متعددة إلى مركز النظام، وتسمح هذه النقاط بالاستفسار واستقبال أحداث الشبكة وكذلك مخاطبة شاشة إظهار الشبكة.

2.3 العمارة الهرمية

عزيزي الدارس، تستخدم عمارة إدارة الشبكة الهرمية نظماً متعددة، ويوجد به نظام وحيد يعمل كخادم مركزيCenter Server، أما النظم الأخرى فتعمل كعملاء Clients. ويبين شكل2.5 نظام العمارة الهرمي. إن بعض وظائف برنامج إدارة الشبكة تكون موجودة على الخادم، وبعض الوظائف الأخرى تؤدي بواسطة العملاء Clients.



شكل2.5 نموذج يوضح العمارة الهرمية.

مثال: يستطيع مهندس الشبكات تهيئة نظم عملاء منفصلة وذلك بإجراء عملية انتخاب Polling لرصد أجزاء مختلفة من الشبكة. ويمكن لبرنامج إدارة الشبكة استخدام تقنيات قاعدة البيانات التي تعمل بنظام الخادم/العميل Client/Server. في هذه الحالة فإن

العملاء لا يكون لها نظم قواعد بيانات منفصلة، ولكنها تستخدم قاعدة بيانات الخادم المركزي من خلال الشبكة.

وبسبب أن وجود النظام المركزي في العمارة الهرمي مهم جدا، لذلك يتم عمل نسخ احتياطية Backup لتحقيق فائض Redundancy.

مميزات برنامج إدارة الشبكة المعماري الهرمي منها ما يلي:

- **لا يعتمد على نظام منفرد.**
- **توزيع وظائف إدارة الشبكة.**
- **رصد الشبكة يكون موزعاً خلال الشبكة.**
- **مخزن المعلومات يكون مركزياً.**

إن استخدام الطريقة الهرمية تساعد في برنامج إدارة الشبكة على تخفيف واحدة من المشاكل الموجودة في الطريقة المركزية، وذلك بواسطة توزيع أعمال إدارة الشبكة بين النظام المركزي والعملاء. ويستطيع مهندس الشبكة إسناد عمليات رصد Monitoring الشبكة إلى العملاء، وبذلك يتم توفير سعة نطاق Bandwidth المصادر Resources داخل شبكة البيانات. أيضا وبسبب الاحتفاظ بأن تكون عمليات رصد الشبكة قريبة من النظم الطرفية End Systems يكون أكثر حرجا في توفير سعة النطاق، حيث إن العملاء ربما يحتاجون إلى كل الأعمال المتعلقة بالخادم المركزي. وسوف يتم فيما بعد دراسة خادم الرصد RMON (Remote Monitoring of Network device).

إن العديد من وظائف إدارة الشبكة تتطلب استرجاع معلومات عن الكثير من أسطح Facets الشبكة. ولهذا يكون من المفيد عادة وجود مكان مركزي للبيانات. حتى إن بعض وظائف الإدارة تكون مسئولية العملاء Clients عند استخدام الطريقة الهرمية، فإن هذا البناء مازال يوفر مكاناً منفرداً لتخزين المعلومات عن الشبكة.

وبما أن العمارة الهرمية تستخدم نظماً متعددة لإدارة الشبكة، فإنه لا يوجد مكان مركزي منفرد لإدارة الشبكة بأكملها، ربما يجعل هذا عملية تجميع المعلومات صعباً إلى حد ما، وكذلك يستغرق وقتا من مهندس الشبكة. وعامل آخر هو أن قائمة الأجهزة التي تدار بواسطة كل عميل، تحتاج أن يتم تحديدها مسبقا من الناحية المنطقية ويتم تهيئتها يدويا. وإذا لم تتم هذه العمليات بدقة، فقد يؤدى ذلك الي أن كلا من النظام المركزي والعميل قد يقوما بالرصد والانتخاب على نفس الجهاز. أحد النتائج الممكنة التي قد تسببها هذه المشكلة هو أن يتم استهلاك Consumption سعة النطاق بنسبة مرتين أكثر على الشبكة لأغراض إدارة الشبكة.

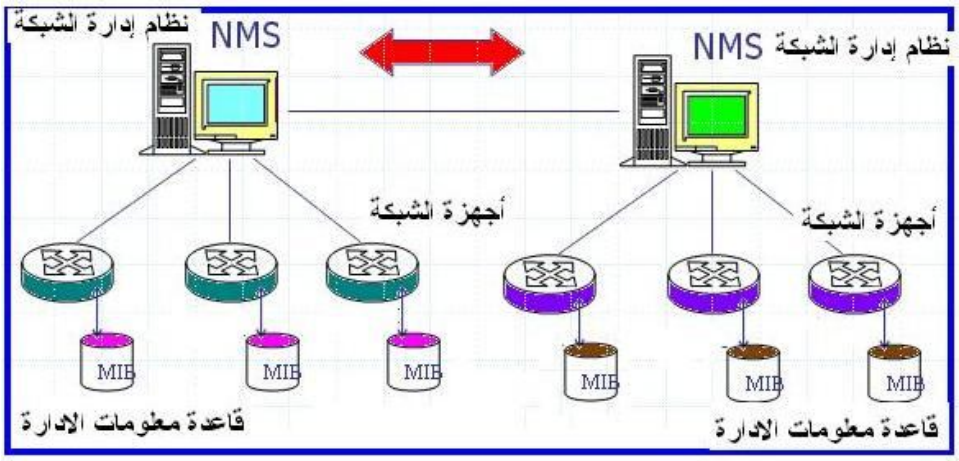
ومن أمثلة بعض الحزم البرمجية الشائعة التي تستخدم العمارة الهرمية ما يلي:

- برنامج من إنتاج شركة "صن" هو Sun Connect Sun Net Manager
- برنامج من إنتاج شركة هيوليت بيكارد HP (Hewlett Packard) OpenView
- برنامج من إنتاج شركة أى–بي–أم IBM Netview / AIX
- برنامج شركة أتي– أند– تى AT & T StarSentry

وتعمل هذه الحزم البرمجية بأسلوب هرمي، وتسمح لمهندس الشبكة في تشغيل برنامج إدارة الشبكة بالتوازي Concurrently.

3.3 العمارة الموزعة

تجمع العمارة الموزعة خصائص كلّ من العمارة المركزية والعمارة الهرمية. ويبين شكل2.6 نموذج للعمارة الموزعة. فبدلا من استخدام برنامج إدارة مركزي أو برامج هرمية، فإن العمارة الموزعة تستخدم برامج إدارية نظيرPeer Platforms متعددة. أحد هذه البرامج يعمل قائدا لمجموعة من النظم الإدارية النظيرة. وكل برنامج نظير منفرد يمتلك قاعدة بيانات كاملة للأجهزة خلال الشبكة بأكملها. وهذا يسمح له بتحقيق وظائف مختلفة، ويرسل تقرير النتائج إلى النظام المركزي.



شكل2.6 يوضح نموذج لبناء العمارة الموزعة.

وبما أن الإدارة الموزعة تجمع معا كلاً من الطريقة المركزية والهرمية فهي بذلك تحقق مميزات كلا من الطريقتين.

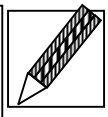
مميزات برنامج إدارة الشبكة الموزعة :

- **تخصيص مكان منفرد لكل معلومات الشبكة وكذلك التحذيرات والأحداث**
- **تخصيص مكان منفرد للوصول إلى التطبيقات الإدارية.**
- **لا تعتمد على نظام منفرد.**
- **توزيع وظائف إدارة الشبكة.**
- **توزيع الرصد من خلال الشبكة.**

وتعتبر تقنية خادم مضاعفة استنساخ قاعدة البيانات مفيدا بدرجة كبيرة لهذا النوع من برامج إدارة الشبكات. إن خادم الاستنساخ يحتفظ بقواعد بيانات متعددة على نظم مختلفة متزامنة تماما. إن نظام خادم الاستنساخ قاعدة البيانات بحد ذاته هو نظام معقد. حيث إنه ؛في الواقع يسبب عبء اتصال Communication Overhead مصاحب لعملية

التزامن. وهذا يؤدي إلى استهلاك مصادر شبكية كثيرة مقارنة بنظام تقنية قاعدة البيانات المستخدمة في نظام الخادم/العميل.

تمرين (2)



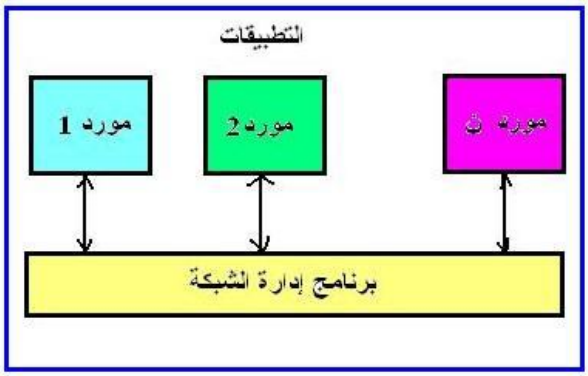
أجب بلا أو نعم

1) من خصائص العمارة الهرمية أنها لا تعتمد على نظام منفرد.
2) من خصائص العمارة الهرمية توزيع وظائف إدارة الشبكة .
3) من خصائص العمارة الهرمية رصد الشبكة يكون موزعاً خلال الشبكة.
4) من خصائص العمارة الموزعة يتم توزيع الرصد من خلال الشبكة.
5) من خصائص العمارة الموزعة يتم فيها إعدادات وظائف إدارة الشبكة.
6) من خصائص العمارة الموزعة تخصيص مكان منفرد لكل معلومات الشبكة.

4. تطبيقات إدارة الشبكة

عزيزي الدارس، يوفر برنامج إدارة الشبكة وظائف عامة لإدارة الشبكة. وعلى العكس من ذلك فإن تصميم تطبيقات إدارة الشبكة هو لمساعدة مهندس الشبكة في إدارة مجموعة خدمات أو أجهزة معينة. ويوضح شكل 2.7 العلاقة بين برنامج إدارة الشبكة وبين التطبيقات. إن كثيراً من تطبيقات إدارة الشبكة قد تم تطويره من قبل منتجي أجهزة الشبكات لمساعدة المستخدمين في إدارة أجهزتهم. فعلى سبيل المثال : فإن مصنعي أجهزة الشبكات مثل(المودم Modem– المجمع hub – الجسر Bridge) قد قاموا ببناء مجموعة من التطبيقات المناسبة Suite كي تعمل بالترابط مع برنامج إدارة الشبكة. وذلك لتزويد مهندس الشبكة بمجموعة متماسكة Cohesive من الأدوات. وباستخدام هذه التقنيات، فإن مهندس الشبكة يحتاج فقط شراء الأدوات الضرورية لإدارة

مجموعة معينة من الأجهزة. فعند محاولة إدارة مجموعة مفاتيح ربط الشبكات(المجمع hub)، وخادم الملفات – على سبيل المثال– يمكن لمهندس الشبكة أن يسأل موردي أجهزة الشبكة Vendors إذا كانوا يمتلكون مجموعة تطبيقات معينة تعمل بالتواصل مع برنامج إدارة الشبكة. وبذلك نحصل على نظام إدارة شبكة يوفر كل الأعمال العامة لبرنامج الإدارة والتطبيقات. ويمكننا ذلك من إدارة خصائص معينة على جهاز التوصيل hub وخادم الملفات باستخدام نفس وحدة الواجهة الرسومية للمستخدم. وتحقيق التواصل من خلال نفس قائمة النظام، والاستفسار من نفس قاعدة بيانات النظام.



شكل2.7 العلاقة بين برنامج إدارة الشبكة والتطبيقات.

وتهدف تطبيقات إدارة الشبكة إلى تحقيق الأهداف التالية:

- أن تعمل مع برامج إدارية متعددة.
- إدارة مجموعة محددة من الأجهزة بكفاءة.
- تجنب حدوث تداخل over lap مع برنامج إدارة الشبكة.
- تحقيق التكامل مع برنامج إدارة الشبكة من خلال وحدة API وقائمة النظام.

وكمثال على ذلك: فإن مصنعي وحدة المجمع Hub يستطيعون بناء تطبيقات تظهر الوصلات الفعلية الموجودة على هذه الوحدة، وذلك عندما يقوم المستخدم بتحديد هذه الوحدة على خريطة الشبكة. وقد يسمح هذا التطبيق للمستخدم بتهيئة بعض خصائص

جهاز المجمع، وتشغيل بعض المنافذ Ports ويجعلها في حالة تشغيل On أو حالة عدم تشغيل Off، أو رصد معدلات الخطأ Error Rates، أو معرفة سرعة الأداء Throughput. وهذا التطبيق قد يساعد في إتمام تأدية وظائف إدارة الأداء بجهاز المجمع

إن تطبيقات **إدارة الشبكة لا ينبغي أن تنشئ تطبيقات يمكن أن تتداخل مع برنامج إدارة الشبكة**، لأن هذا التداخل قد ينتج عنه إيجاد طرق متعددة، يمكن أن تؤدى نفس النتائج التي يمكن الحصول عليها من برنامج إدارة الشبكة. وربما يؤدي ذلك إلى إرباك الوحدة البينية Interface للمستخدم. أيضا فإن إنتاج خصائص قد تكون موجودة في برنامج إدارة الشبكة يؤدي إلى ضياع مجهود مطوري النظم والتطبيقات. والاستثناء الوحيد فقط لهذه القاعدة يكون عندما لا يقوم برنامج إدارة الشبكة بتوفير الخصائص التي تحتاجها التطبيقات. وكمثال على ذلك:

إذا قام برنامج إدارة الشبكة بتوفير إمكانية إنتاج رسومات خطية Line Graphs ولكن التطبيق يحتاج وجود رسومات دائرية Pie Charts، فإن مطوري التطبيقات يقومون بتوفير هذه الخصائص. عندما توجد تطبيقات متعددة – يتم إنتاجها بواسطة مطورين متعددين– وكل منتج منها ينتج خرائط دائرية مع وحدات المواجهة المصاحبة لها، فإن مطوري التطبيق ربما تستعجل منتجي برامج إدارة الشبكة بعدم إجراء (إنتاج) هذه الخصائص، وذلك كي لا تسبب إرباكاً محتملاً للمستخدم.

إن تطبيق إدارة الشبكة يكون أحد أهدافه أيضا، هو أن **يتم إجراء التطبيق من خلال وحدة API وقائمة النظام. وهذا يسمح للمستخدم برؤية التطبيقات وإدارة شكل نظام الشبكة في وضع موحد** Uniform. إن وحدة API تسمح بوجود وحدة مواجهة برمجية لبرنامج إدارة الشبكة. كما أن وحدة القوائم بالنظام تسمح بتشغيل برامج التطبيق من نفس قائمة النظام الذي يراه المستخدم على نفس برنامج إدارة الشبكة. إن عملية التكامل مع التطبيق من خلال قائمة النظام– في العديد من برامج إدارة الشبكة– لا تتطلب أكثر

من عملية تحرير ملف نصي. إذا تم تنفيذ التطبيق كعملية منفصلة، فإن التكامل مع القائمة يكون عادة عمل معتاد. إذا كانت كل التطبيقات التي يستخدمها مهندس الشبكة في برنامج إدارة الشبكة تتم بالتعاون من برنامج إدارة الشبكة بنفس الأسلوب، فإن ذلك يمكن أن يوفر كثيرا من الخصائص التي تساعد على تحقيق إدارة الشبكة.

إن التطبيق الذي يكون متاحا لبرنامج إدارة واحد فقط، يرغم مهندس الشبكة على أن يستخدم هذا البرنامج فقط لإدارة وظائف الشبكة. وهذا ليس حلا مناسبا، لأن برنامج الإدارة هذا ربما لا يوفر الخصائص الضرورية لدعم التطبيقات الأخرى التي قد تحتاجها. إن الهدف من تطبيقات إدارة الشبكة هو أن تعمل مع كل برامج إدارة الشبكة الشائعة. ولكن عملية التكامل هذه، تتطلب وجود مخطط دقيق للاحتفاظ بعمليات تحديث المنتجات، لتواكب التغيرات التي تحدث في برامج إدارة الشبكة، وذلك كلما ظهر منتج إدارة شبكة جديد.

5. طريقة اختيار نظام إدارة الشبكة

عزيزي الدارس، يتم بناء نظام إدارة الشبكة من جزأين أساسيين هما: برنامج إدارة الشبكة، والتطبيقات المصاحبة له. وبواسطة اختيار هذين المكونين بعناية فإنه يمكن أن يتم بناء نظام يساعد مهندس الشبكة في تحقيق الأعمال المطلوبة في مجال إدارة الشبكات. وفيما يلي بيان الخطوات العملية التي تساعد على اختيار نظام إدارة الشبكة:

- عمل بيان بالأجهزة.
- وضع أولويات Priorities لمجالات أعمال إدارة الشبكة.
- عمل مسح Survey لتطبيقات إدارة الشبكة.
- اختيار برنامج إدارة الشبكة.

الخطوة الأولى: هي تحديد أجهزة شبكة البيانات. وغالبا تتضمن هذه القائمة: محطات العمل – الحاسبات الشخصية – معالجات المقدمة والمؤخرة Front-end Processors – المتحكمات Controllers – بوابات الطريق Gate Ways – مفاتيح – موجهات –

قناطر – وحدات توصيل Hub – طابعات – أجهزة مودم. ونحتاج معرفة إن كانت هذه الأجهزة يمكن إدارتها بواسطة بروتوكولات الشبكة، سواءاً كانت هذه البروتوكولات قياسية، أو غير ذلك (ذو ماركة مسجلة Proprietary). إذا كان الجهاز لا يمكن إدارته بواسطة بروتوكول الشبكة القياسي، لا يتم حذفه من قائمة الأجهزة، فإن برنامج بوابة الطريق ربما يتيح لنا توفير ترجمة Translation بين بروتوكول الجهاز والبروتوكول القياسي. وبعد إنشاء قائمة الأجهزة، فإننا نحتاج عمل أولويات للأجهزة ذات المهام الحرجة Critical Mission. فعلى سبيل المثال: فبالرغم من أنه يكون من المرغوب فيه إدارة جميع طابعات الشبكة. ربما تكون إدارة هذه الأجهزة ذات أولوية أقل من إدارة معالجات المقدمة والمؤخرة والتي تقوم بتوفير عمليات الاتصال بالحاسب الكبير Mainframe.

الخطوة الثانية: هي وضع أولوية لمجالات إدارة الشبكة الخاصة بالمؤسسة. في حالات كثيرة يمكن أن يكون المجال المهم جدا في إدارة الشبكة هو إدارة الأعطال. على الرغم من أن المؤسسة قد تعطي أولوية أولى لأمن الشبكة أو لتهيئة الشبكة، وبذلك فإن هذه الخطوة تكون ضرورية لأنها تحدد الاحتياجات الأكثر أهمية لإدارة تطبيقات الشبكة وأجهزتها.

الخطوة الثالثة: هي إيجاد تطبيقات إدارة الشبكة التي تساعد على تحقيق المجالات الأساسية في إدارة الشبكة وأجهزتها – والتي تم تحديدها في الخطوة السابقة. إن تطبيقات إدارة الشبكة تساعد في إتمام مجالات أعمال إدارة الشبكة. وبدون هذه التطبيقات فإن الوظائف العامة لبرنامج إدارة الشبكة هي التي تساعد على إتمام أعمال إدارة الشبكة. وباستعمال التطبيقات المصممة لإدارة الأجهزة يستطيع مهندس الشبكة وضع أولويات تسمح بتخصيص مصادر فعالة لإدارة الشبكة بدلا من بناء تطبيقات تسمح بتحقيق إدارة الشبكة.

الخطوة الرابعة: هي اختيار برنامج إدارة الشبكة. من الطبيعي أن تكون التطبيقات التي يتم اختيارها جميعها سوف تعمل بواسطة برنامج إدارة الشبكة. إذا كانت هذه التطبيقات

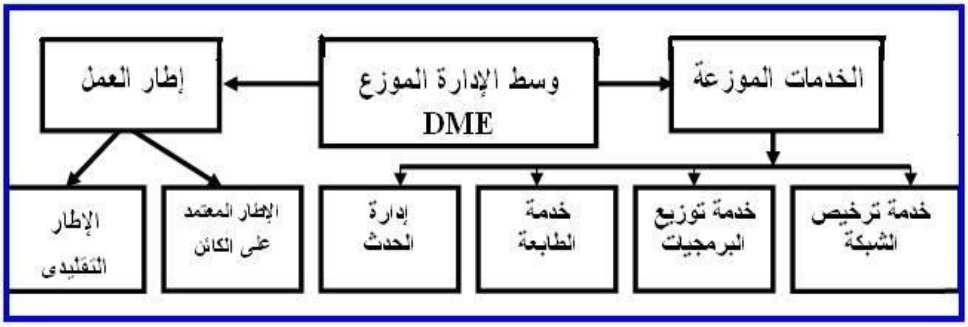
تعمل على برنامج إدارة شبكة واحد فقط، فإن هذا الاختيار يكون مباشرا. أما إذا كان هناك اختيار لعدة برامج لإدارة الشبكة، فإنه يجب اختيار برنامج إدارة الشبكة الذي يناسب معمارية الشبكة التي تزمع المؤسسة في التخطيط لإدارتها. على سبيل المثال، إذا كانت المؤسسة تخطط لإنشاء مركز إدارة شبكة مركزي واحد، دون الاحتياج إلى إنشاء شبكات عند مواقع أخرى، فإن برنامج الإدارة المركزي أو الهرمي يكون هو الأفضل. إذا كانت المؤسسة تخطط لإنشاء مراكز إدارة شبكة ذات فائض متعدد Multiple Redundant من خلال الشبكة، فإن اختيار إدارة شبكة موزع يكون هو الأنسب. على سبيل المثال، إذا كان برنامج إدارة الشبكة المناسب لشبكة البيانات يتطلب عتاد لا تملكه المؤسسة، ولا تستطيع توفيره فإنه يكون من الأفضل اختيار برنامج إدارة شبكة أقل من المناسب بحيث يمكن تشغيله على العتاد الذي تملكه المؤسسة أو تستطيع توفيره. إن برنامج إدارة الشبكة، يحتاج وجود عتاد لتشغيله، وإذا لم يتوفر هذا العتاد فإن ذلك يجعل مهمة برنامج إدارة الشبكة صعبا. ويوجد متاحا في الأسواق، برامج إدارة شبكات تعمل على نظم عتاداً متنوعة (تشمل: الحاسبات الشخصية – محطات العمل – الحاسبات الكبيرة) وكذلك برامج مناسبة لنظم عتاد متعددة.

وباتباع الخطوات السابقة فإن مهندس الشبكة يستطيع اختيار نظام إدارة الشبكة الذي يعمل بطريقة جيدة على شبكة البيانات التي توفرها المؤسسة.

6. إدارة الوسط الموزع DME

قامت مؤسسة "إيجاد البرامج المفتوحة OSF" وهي إحدى المؤسسات التي تستكشف التقنيات التي تستخدم في صناعة الحاسبات بإصدار البناء الهيكلي لنظام تقنية "إدارة الوسط الموزع DME" وهى تقنية خاصة بالتعامل مع مشاكل أجهزة إدارة الشبكة الموزعة. وتقوم هذه المؤسسة بتحديد الطرق القياسية لإتمام وظائف تطبيقات ونظم إدارة الشبكات. وعندما تتبع برامج تطبيقات ونظم إدارة الشبكات هذه المواصفات القياسية عند تنفيذ هذه الخصائص، فإنه يتم تحقيق طريقة موحدة تحدد المجالات

الوظيفية لإدارة الشبكة. وبذلك تؤدي هذه الطريقة إلى إيجاد مرونة عظيمة وسوق منتجات مفتوحة لمهندس الشبكات. وقد قامت مؤسسة OSF بإصدار البناء الهيكلي لنظام DME كما هو مبين في شكل2.8 .



شكل2.8 هيكلية نظام إدارة الوسط الموزع DME.

الجزء الأول من هيكل DME .. إطار العمل :

يحدد إطار العمل اتجاهين يمكن أن يستخدمهما برنامج إدارة الشبكة هما:

الاتجاه الأول : إطار العمل التقليدي

الاتجاه الثاني الإطار المعتمد على الكائن.

ويستخدم إطار العمل التقليدي **نظام الخادم/العميل التقليدي لإدارة برامج وتطبيقات الشبكة.** أما إطار العمل المعتمد على الكائن Object Oriented Framework فهو يناسب بيئة التقنيات المعتمدة على الكائن.

الجزء الثاني من هيكل DME .. الخدمات الموزعة :

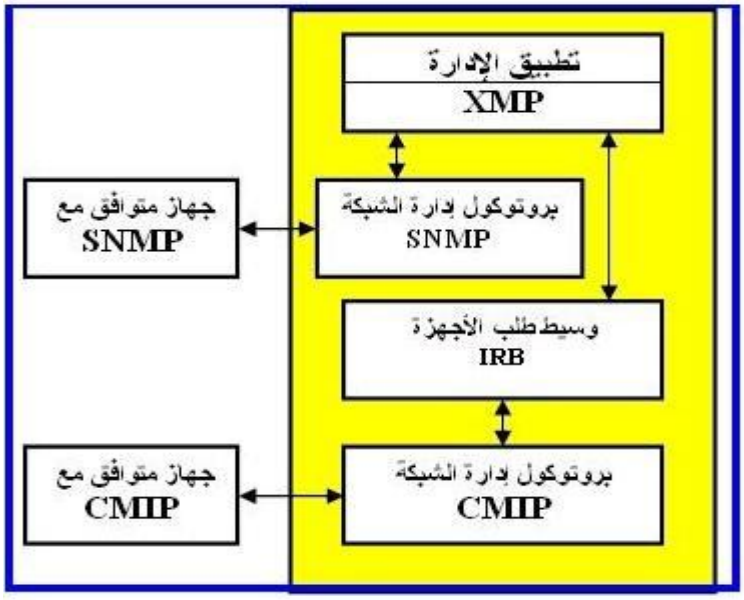
وهي تصنع من كل الخدمات التي تساعد في إدارة الوسط الموزع، مثل إدارة الحدث – خدمة الطابعة – طرق البرمجيات الموزعة – خدمات ترخيص الشبكات.

الجزء الأول إطار العمل .. الإطار التقليدي:

يشتمل الإطار التقليدي لنموذج DME على أجهزة شبكات متعددة، والبروتوكولات الموجودة شائعة الاستخدام في غالبية شبكات البيانات، كما هو موضح في شكل2.9. ويستعمل هذا الإطار في شبكات الخادم/العميل، ويمثل الخادم نظام إدارة الشبكة ويمثل

العميل أجهزة الشبكة. **ويحدد إطار العمل التقليدي المواصفات القياسية التي يوفرها برنامج إدارة الشبكة والتطبيقات المصاحبة هي:**

- وحدة واجهة المستخدم الرسومية GUI.
- طريقة للاستفسار عن البيانات من الشبكة.
- طريقة من أجل التطبيقات لفهم المعلومات الإدارية.
- وحدة مواجهة البرامج التطبيقية API .



شكل2.9 مكونات إطار عمل الإدارة التقليدي DME.

يتم تحقيق المواصفات القياسية لوحدة واجهة المستخدم الرسومية GUI باستخدام X11 Motif (وهي مجموعة برمجيات مكتبية توفر تطبيقات من خلال نظام نوافذ موزعة). ويستطيع مهندس البرمجيات استخدامها في كتابة التطبيقات، كما أنه يمكن تشغيلها على محطات عمل وحاسبات شخصية متنوعة. ويستخدم الإطار التقليدي طريقتين لتجميع البيانات من الشبكة هما برتوكول SNMP وبروتوكول CMIS/CMIP. وبذلك

يستطيع هذا البناء إدارة كل الأجهزة التي تدعم بروتوكول SNMP وكذلك الأجهزة التي تدعم CMIS/CMIP.

ويتم بناء وحدة مواجهة البرامج التطبيقية API باستخدام XMP (X Management Application Interface). وهذه الوحدة توفر طريقة اتصال لكل من بروتوكول SNMP وبروتوكول CMIS/CMIP. ولكن هذين البروتوكولين لهما قواعد مختلفة تحكمهما معلومات الإدارة الهيكلية لهما. وهذا يجعل ضرورة أن يستعمل XMP طريقتين مختلفتين لتوصيل هذه البروتوكولات. إن XMP يوفر اتصالاً مباشراً مع البروتوكول SNMP. ولكن يوجد مستوى آخر مجرد هو وسيط طلب الأجهزة IRB (Instrumentation Request Broker) الذي يحاول توفير وحدة بينية مبسطة للبروتوكول CMIS/CMIP كي يسمح لمطوري التطبيقات برؤية أجهزة الشبكة ككائنات يمكن إدارتها. وهذا المستوى المجرد Abstract يسمح بتصميم برتوكول CMIS/CMIP المعتمد على الكائنات كي يعمل من خلال إطار العمل التقليدي. إن وحدة IRB تسمع بالتطبيقات بأن ترى أجهزة الشبكة ككائنات.

الجزء الاول إطار العمل .. الجزء المعتمد على الكائن

والكائن Object هو عبارة عن كيان برمجي تم تحديده وله صفات خاصة به وكذلك دوال Methods تحكم سلوكه، وأعمال داخلية. إن الهيكل الداخلي للكائن يكون غير معلوم Hidden خارج الكائن. إن التطبيقات التي تستخدم الكائن تحتاج أن تعرف صفات الكائن ودوال الكائن. إن الكائنات تخفي التعقيدات وتسهل بناء التطبيقات المعقدة بواسطة تقسيم الأسطح الكثيرة للتطبيق وجعلها مكونات صغيرة غير قابلة للتجزيء Indivisible.

على سبيل المثال: نفترض أنه تم إنشاء تطبيق تقرير موضحا نسبة زمن بداية التشغيل Up-time لكل وصلات التوالي الموجودة في شبكة البيانات. يمكن اعتبار وصلة التوالي هي كائن له الخصائص الخاصة به (المتغيرات) وكذلك الدوال الخاصة

به(سلوكيات). ويمكن أن تكون خصائص الكائن "وصلة التوالي" عبارة عن سعة نطاق نقاط النهاية – التأخير الناتج عن الانتقال Propagation Delay – معدل الأخطاء لكل ثانية – سرعة البيانات في الثانية – زمن بدء التشغيل – محدد الدوائر. ويمكن أن تشمل الدوال الخاصة بالكائن "وصلة التوالي" على بداية التشغيل **استخدام اتساع النطاق Bandwidth Utilization** معدل استخدام الخطأ Error Utilization. وإذا أراد التطبيق **إنشاء تقرير** لتوضيح نسبة بداية التشغيل لكل كائنات وصلات التوالي خلال الشهر الماضي، فإنه يمكن **أن نتبع هذه الخطوات:**

- يطلب كل الكائنات من نوع "وصلة التوالي"
- يشغل الدالة "بداية تشغيل" لكل كائنات "وصلة التوالي".
- يحسب النسبة المئوية لزمن "بداية تشغيل" خلال الشهر الماضي.

من ذلك يتضح أن الكائنات تسمح للتطبيقات بإنتاج النتائج المطلوبة بدون معرفة المكان الفعلي لكل وصلات التوالي. وأيضا معرفة أجهزة الشبكة التي تمتلك وصلات توالي ليس متطلباً مسبقاً Prerequisite. إن مؤسسة OSF تستخدم الإمكانات الموجودة في الكائنات لتعزيز إطار العمل المعتمد على تقنية الكائنات DME.

إن إطار العمل المعتمد على تقنية الكائنات DME يستخدم التقنيات المعتمدة على الكائنات لأغراض إدارة الشبكة. فبدلا من استخدام بناء الخادم/العميل، فإن إطار العمل المعتمد على تقنية الكائنات يسمح لنظام إدارة الشبكة وأجهزة الشبكة أن تبدو كأنها كائنات نظيرة Peer Objects. إن تطبيق إدارة الشبكة هو عبارة عن كائن متصل بأجهزة الشبكة يستخدم الدوال المصاحبة لها، مثل اتصال أجهزة الشبكة مع نظام إدارة الشبكة، وذلك بواسطة مناداة الدوال. إن هذه الدوال تبدأ عملها عندما يتم استلام عملية بواسطة الكائن. وهذا التركيب الهيكلي يكون مشابها لطريقة مناداة الدوال عن بعد RPC (Remote Procedure Call) التي يستعملها المبرمجون. إن وسط الحاسبات الموزعة DCE (Distributed Computing Environment) هو الذي يحدد طريقة RPC التي يستعملها إطار العمل.

إن وحدة وسيط طلب الإدارة MRB (Management Request Broker) هي عبارة عن نوع إصدار برمجي مثل المبين في إطار العمل IRB الموجود في نظام إطار العمل التقليدي. وأحد الفروق الأساسية هي أن MRB يعمل كوحدة مواجهة للعمليات المتعلقة بأجهزة الشبكة عن بعد، في كل تطبيقات الإدارة. إن وحدة MRB بدورها تقوم بالاتصال بكائنات الإدارة عن بعد من خلال وحدة DCE RPC. فإن كائن إدارة واحد يستطيع من خلال وحدة DCE RPC بدء تشغيل الدوال الموجودة على كائن إدارة نظير آخر. إن وحدة DCE RPC تتميز بأن لها نظام أمن صارم Rigorous، وطريقة لتحديد مكان كائنات الشبكة. وعلى الرغم من أن هذه الوظائف قد تكون كثيرة ومتعددة لكي تتم بواسطة جهاز الشبكة، إلا أنه يمكن تحقيقها بسهولة بواسطة النظام. ولهذا فإن إطار العمل المعتمد على تقنية الكائن يستخدم في إدارة النظم، وهذا لا يمنع من استخدامه في إدارة الشبكة.

إن وحدة واجهة إدارة المستخدم MUI (Management User Interface) هي عبارة عن وحدة واجهة رسومية للمستخدم GUI، تستخدم في إطار العمل المعتمد على تقنية الكائنات. وتبنى وحدة MUI باستخدام النظام القياسي X11 Motif، لتوفير وحدة واجهة رسومية قياسية شائعة لكل تطبيقات الإدارة. ومن وجهة نظر تقنية الكائن، فإن وحدة MUI تمثل كائناً إدارياً يقوم بتوفير دوال تستطيع الاتصال بعناصر شاشة العرض في نظام إدارة الشبكة.

ولتحديث وحدة DME لكي تتعامل مع تقنية الكائن، فإنه يمكن استخدام وحدة موائم للبروتوكول SNMP. يستطيع هذا الموائم ترجمة العمليات الأساسية للبروتوكول SNMP كي يعمل مع دوال DME. وهذا يمّكن بروتوكول SNMP من إدارة الأجهزة ورؤيتها كأنها كائنات لها دوال.

الجزء الثاني من هيكل DME .. الخدمات الموزعة:

إن مؤسسة OSF توفر تطبيقات ضرورية للعمل مع وحدة DME

وهذه التطبيقات تشمل ما يلي:

- خدمات الحدث.
- خدمات الطابعة.
- خدمات رخصة الشبكة.
- خدمات البرامج الموزعة.

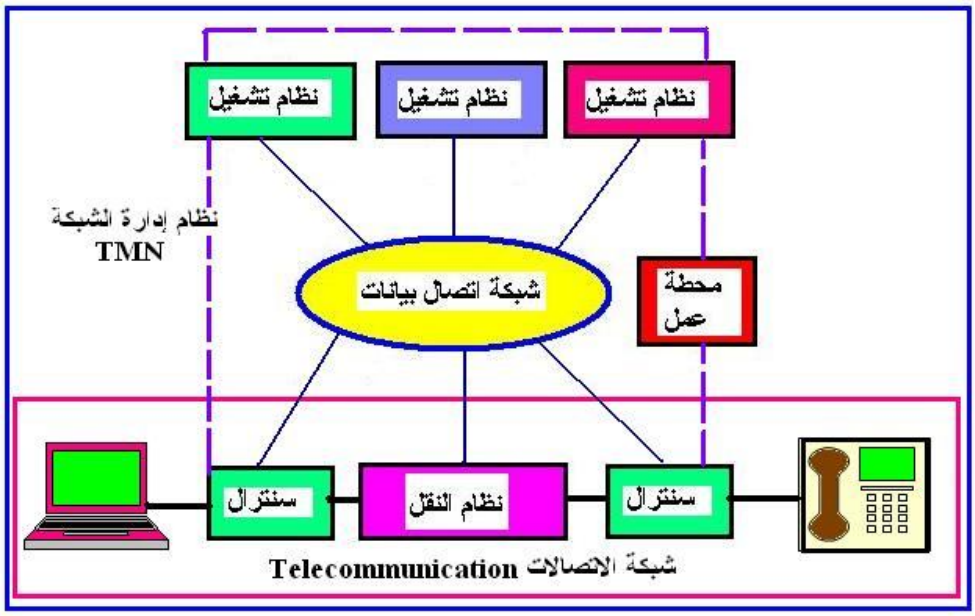
وتوفر خدمات الحدث وسيلة لدخول وترشيح وتوجيه الأحداث ذات العلاقة بالشبكة في الوسط الموزع. وتقوم خدمات الطابعة بتوفير خدمة طباعة موزعة من خلال الشبكة. وتتم عملية التعامل مع رخص البرمجيات الخاصة بأعمال الصيانة والتحكم من خلال الخدمات التي توفرها وحدة خدمات ترخيص الشبكة. وتساعد خدمات البرامج الموزعة على تنصيب التطبيقات من أجل الاستخدام الموزع.

مما سبق شرحه نجد أن إطار العمل التقليدي يستطيع العمل جيدا لإدارة مكونات إدارة الشبكة مستخدما البروتوكولات القياسية المتوفرة في الأسواق. أما إطار العمل المعتمد على تقنية الكائنات فهو يستخدم في بناء تطبيقات إدارة الشبكة المعقدة (الكبيرة)، وذلك بحسب تقنية ومعمارية الشبكة.

7. إدارة شبكات الاتصال TMN

عزيزي الدارس، نشأ مقترح إدارة شبكات TMN من قبل هيئة التوحيد القياسية المعروفة باسم ITU-T والتي كانت تعرف سابقا باسم هيئة الاتصالات CCITT. وتعرف الوثيقة رقم M.3010 التوصيات الخاصة بإدارة شبكات TMN، كما يوجد بها علاقة ترابط قوية مع نظام إدارة OSI. يعمل نظام إدارة الشبكات TMN كشبكة منفصلة تربطها وحدات بينية مع شبكة الاتصالات عند نقاط اتصال مختلفة متعددة من أجل إدارتها. ويوضح شكل2.10 العلاقة بين نظام إدارة شبكات TMN وبين شبكة الاتصالات التي يقوم بإدارتها. ولتحقيق أغراض إدارة الشبكة، يتم ربط السنترالات

Exchanges، ونظم النقل Transmission systems من خلال شبكة اتصالات البيانات، والتي توصل بها مجموعة من نظم التشغيل Operations Systems.

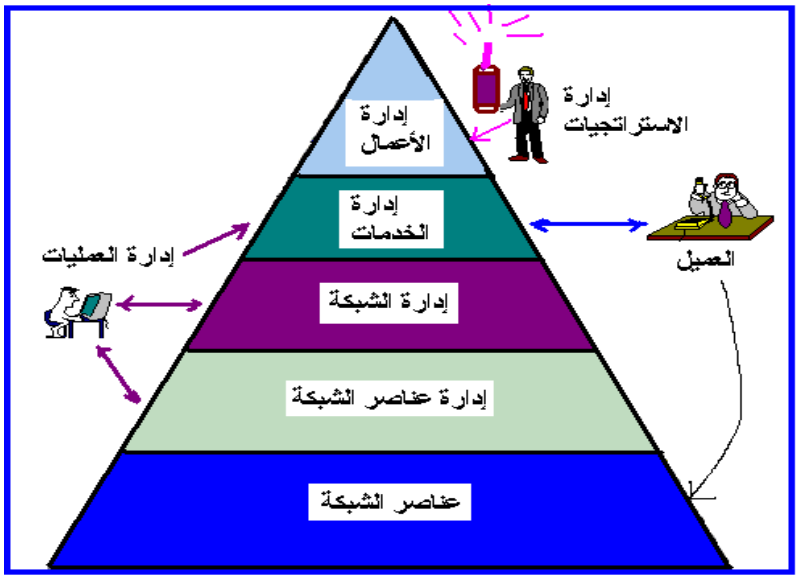


شكل2.10 نظام إدارة الشبكة TMN.

تقوم نظم التشغيل بتحقيق معظم وظائف الإدارة، والتي يمكن أن تتم آليا أو بواسطة مهندس إدارة الشبكة. كما يمكن أن يتم تحقيق وظيفة إدارية واحدة بواسطة العديد من نظم التشغيل. في مثل هذه الحالات، فإن شبكة البيانات سوف تقوم بإجراء عمليات تبادل المعلومات الإدارية بين نظم التشغيل. وتقوم شبكة اتصال البيانات أيضا بتوصيل محطات العمل Work Stations، التي تسمح لمهندس الشبكة بتفسير معلومات الإدارة. وتحتوى محطات العمل على وحدات مواجهة بينية مع المستخدمين. وتقسم أعمال إدارة الشبكات TMN إلى عدة مستويات بنائية هي:

- البناء الوظيفي Functional Architecture : وهو المختص بالوظائف الإدارية للشبكة.

- البناء الفعلي Physical Architecture : وهو مختص بكيفية تحقيق الوظائف الإدارية على الأجهزة الفعلية الموجودة في الشبكة.
- البناء المعلوماتي Information Architecture : ويصف الأعمال التي تم تطويعها من نظام إدارة OSI لتلائم نظام TMN، ويستخدم التقنيات المعتمدة على الكائن Object Oriented.
- البناء الطبقي المنطقي Logical Layered Architecture: وهو يشتمل على واحد من أحسن الأفكار التي استخدمت في إدارة شبكات TMN، وهو بناء نموذج يوضح كيفية تقسيم الأعمال الإدارية إلى هياكل حسب مسئوليات مختلفة، كما هو موضح في شكل2.11.



شكل2.11 يوضح نموذج مستويات إدارة شبكات TMN الأربعة.

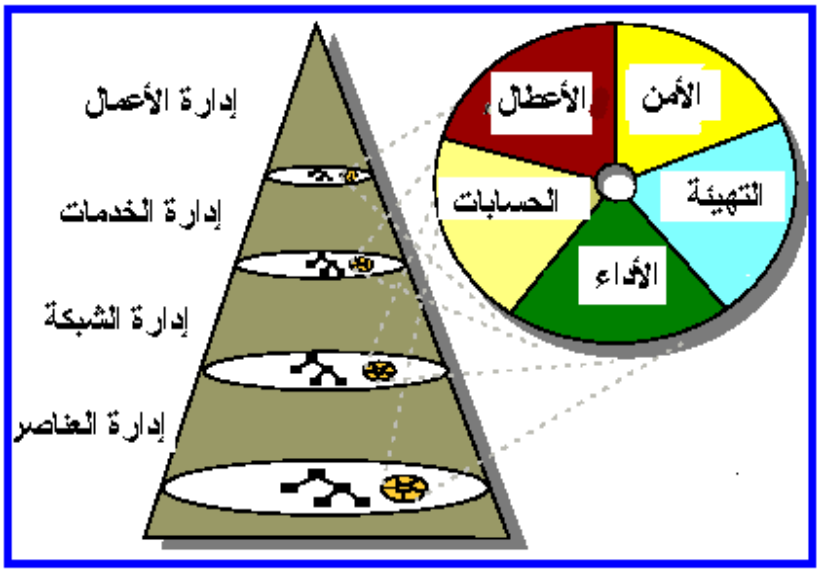
ويتكون نموذج إدارة شبكات TMN، من أربعة مستويات، كما هو موضح في شكل2.11، هي:

- **مستوى إدارة الأعمال:** لتحقيق الوظائف الخاصة بالأعمال، وتحليل الاتجاهات، وعوامل الجودة، وتوفير فواتير الدفع المبنية على هذه الأسس وكذلك التقارير المالية.
- **مستوى إدارة الخدمات:** يحقق مهام متعلقة بتقديم خدمات الشبكة، مثل أعمال الإدارة وتحديد تكلفة الخدمات.
- **مستوى إدارة الشبكة:** يحقق وظائف متعلقة بتوزيع مصادر الشبكة، مثل التهيئة والتحكم في الإشراف على إدارة الشبكة.
- **مستوى إدارة العناصر:** يختص بالمهام المتعلقة بالتعامل مع عناصر الشبكة. ويشمل ذلك إدارة الإنذارات، معالجة المعلومات، النسخ الاحتياطية، عمليات الدخول للشبكة، وصيانة عتاد وبرامج الشبكة.

ويمكن أيضا أن ننظر إلى نموذج إدارة الشبكات TMN من وجهة نظر وظيفية، كما هو موضح في شكل2.12، والتي يمكن من خلالها أن نصف النموذج على أنه يتكون من خمسة مكونات وظيفية هي:

- **إدارة الأعطال:** وهي تختص بالتعرف على العطل وعزله وتدوينه وتصليحه إن أمكن.
- إدارة **الحسابات:** وتختص بتجميع وتخزين، وتحديد الفواتير ومعلومات الحسابات.
- **إدارة الأداء:** و تختص بتجميع البيانات الإحصائية وتحديد خطة اتساع الشبكة.
- **إدارة التهيئة:** وتختص بتنصيب أجهزة الشبكة، وضبط معاملات الشبكة، وتهيئة سعة الشبكة.
- **إدارة الأمن:** وتختص بمهام متعلقة بتوثيق الإدارة، والحماية من الاختراقات والمستخدمين غير المفوضين.

وهذه المجالات الوظيفية الخمسة السابقة، تكون الأساس لجميع نظم إدارة الشبكات لكل من شبكات البيانات، وكذلك شبكات الاتصالTelecommunication .



شكل2.12 نموذج إدارة شبكات TMN والمكونات الوظيفية الخمسة.

تمرين (2)

أجب بلا أو نعم

- من أهداف تطبيقات إدارة الشبكة أن تعمل مع برامج إدارية متعددة
- من أهداف تطبيقات إدارة الشبكة أن إدارة مجموعة محددة من الأجهزة بكفاءة.
- من أهداف تطبيقات إدارة الشبكة تجنب حدوث تداخل مع برامج إدارة الشبكة
- TMN يتكون نموذج إدارة شبكات من عدة مستويات : مستوى إدارة الأعمال.
- يتكون نموذج إدارة شبكات من عدة مستويات مستوى إدارة الخدمات
- يتكون نموذج إدارة شبكات من عدة مستويات مستوى إدارة الشبكة.

الخلاصة

عزيزي الدارس، تعرفنا في هذه الوحدة على عملية إدارة الشبكات بالتفصيل. والفرق بين نظام إدارة الشبكة وتطبيقات إدارة الشبكة. حيث أن لكل منهما الأهداف الخاصة به والتي يجب تحقيقها. وتناولنا ثلاثة أنواع من بناء وعمارة الشبكات هما: الإدارة المركزية الإدارة الهرمية والإدارة الموزعة. ثم من ثم حددنا أدوات الأدوات البسيطة والمركبة والمتقدمة لإدارة الأمن

لمحة مسبقة عن الوحدة القادمة

عزيزي الدارس في الوحدة القادمة التي تتناول إدارة الأعطال عن طريق تحديد مكان العطل أو المشكلة في الشبكة والقيام بتصليحها.

ونستعرض فوائد عملية إدارة الأعطال، ونناقش الخطوات الثلاثة المتعلقة بإتمام صيانة الأعطال في شبكة البيانات. ونصف ثلاثة احتمالات ممكنة للأدوات التي يمكن استخدامها. ونشرح بعض الطرق المتاحة لحصر الأعطال في نظام إدارة الأعطال ،كن معنا في الوحدة القادمة وستجد الكثير المفيد إن شاء الله .

إجابات التدريبات

رقم السؤال	1	2	3	4
الإجابة	نعم	نعم	نعم	لا

رقم السؤال	1	2	3	4	5	6
الإجابة	نعم	نعم	نعم	نعم	لا	نعم

مسرد المصطلحات

طريقة الانتخاب Polling:

في هذه الطريقة تقوم محطة نظام إدارة الشبكة، إما آليا أو بواسطة مهندس الشبكة، بإرسال استفسارات Queries، لكل وكيل موجود داخل جهاز الشبكة، بطريقة دورية، لفحص قيم معينة عن معلومات الأجهزة.

طريقة الولوج Logging:

تقوم أجهزة الشبكة بتوليد إشارات تحذير عندما تصل معاملات الأجهزة إلى الحد الحرج، وهذه الإشارات تسمى مصايد Traps.

وحدة البرمجة التطبيقية البينية

API (Application Programming Interface)

إن وحدة API هي عبارة عن مكتبة برمجية تسمح بالوصول إلى المعلومات التي يتم الاحتفاظ بها داخل برنامج إدارة الشبكة. تستطيع البرامج الخارجية من خلال API استخدام خريطة الشبكة

مسجل الحدث Event Log

يستخدم مسجل الحدث لتسجيل الأعمال التي تتم داخل الشبكة مرتبة زمنيا Chronologically في شكل فورمات مقروءة

البناء الطبقي المنطقي Logical Layered Architecture:

وهو يشتمل على واحد من أحسن الأفكار التي استخدمت في إدارة شبكات TMN، وهو بناء نموذج يوضح كيفية تقسيم الأعمال الإدارية إلى هياكل حسب مسئوليات مختلفة

المصطلح بالإنجليزية	معناه بالعربية
Autodiscovery	الكشف الآلي
Automapping	الرسم الآلي للخريطة
API (Application Programming Interface)	وحدة برمجة تطبيقية بينية
Backup	عمل نسخ احتياطية
Bar Drawing	الرسم القضيبي
Bridge	قنطرة
Centralized Architecture	العمارة المركزية
Communication Overhead	عبء اتصال
Chronologically	مرتبة زمنيا في شكل فورمات
Critical Mission	مهام حرجة
Cracker	قرصان
Data Multiplexer	مجمع بيانات
DBMS (Data Base Management System	نظام إدارة قاعدة البيانات
DM E (Distributed Management Environment)	نظام إدارة الوسط الموزع
DCE (Distributed Computing Environment	وسط الحاسب الموزع
Distributed Architecture	العمارة الموزعة
Event Log	مسجل الحدث
Front End Processors	معالجات المقدمة والمؤخرة
Graphic Tools	أدوات جرافيك

المصطلح بالإنجليزية	معناه بالعربية
GUI (Graphic User Interface)	وحدة الواجهة الرسومية للمستخدم
Line Drawing	رسم خطي
Hierarchical Architecture	العمارة الهرمية
ITU (International Telecommunication Union)	هيئة الاتصالات الدولية
MIB(Management Information Base)	قاعدة إدارة المعلومات
MRB (Management Request Broker)	وسيط طلب الإدارة
MUI (Management User Interface)	واجهة إدارة المستخدم
Menu	نظام قوائم متهيئ للمستخدم
Network Management Architecture	معمارية إدارة الشبكة
Network Management Platform	برنامج إدارة الشبكات
RPC (Remote Procedure Call)	مناداة الدوال عن بعد
Replication Server	خادم مضاعفة
Router	موجه
RMON(Remote Monitoring)	الرصد عن بعد
TMN (Telecommunication Management Network)	إدارة شبكات الاتصال
Peer Platform	برامج إدارية نظيرة
Pie chart Drawing	رسم الخريطة الكعكي
Object Oriented Framework	إطار العمل المعتمد على تقنية الكائن
OSF (Open Software Foundation)	مؤسسة إيجاد البرمجيات المفتوحة
SNA(System Network Architecture)	بناء شبكة النظام

المراجع

1- Network Management, By- Subramanian, Addison Wesley Publishing Co ،ISBN: 8177588206, 2001.

2- Network Management, MIBs and MPLS : Principles, Design and Implementation, By- Stephen B. Morris, Pearson Education India Publisher, ISBN: 8129703467, 2004.

3-Telecommunication Network Management: Technologies And Implications, By- AIDAROUS SALAH, PLEVYAK THOMAS, Prentice Hall of India Publisher, ISBN: 8120316851 ، 2006.

4- Fundamentals of Telecommunications Network Management, By- RAMAN LAKSHMI G., Prentice Hall(IE) Publisher, ISBN: 8120316797 ،2005.

5- Network Management: A Practical Perspective, 2nd Edition, By Allan Leinwand, Karen Fang, by Addison Wesley Professional, ISBN-10: 0-201-60999, 1996.

6- Snmp, Snmpv2, and Rmon: Practical Network Management by William Stallings ,Publisher: Addison-Wesley Pub; 2nd edition, ISBN-10: 0201634791 ،1996.

7- X11/motif:
www.softintegration.com/chhtml/toolkit/demos/X11/motif/
www.cs.cf.ac.uk/Dave/X_lecture/X_book_caller/

8- Replication Server:
www.isug.com/Sybase_FAQ/REP/section1.html
www.isug.com/Sybase_FAQ/REP/index.html
www.enterprisedb.com/products/enterprisedb_replication.do

9- OSF Distributed Management Environment (DME).
www4.informatik.uni-erlangen.de/~tsthiel/Papers/osf-dme-rationale.html
www4.informatik.uni-erlangen.de/~tsthiel/Management.html

10- Recommendation M.3010
www.itu.int/itudoc/itu-t/aap/sg4aap/history/m3010a1/index.html
www.itu.int/itudoc/itu-t/aap/sg4aap/history/m3010a2/index.html


الوحدة الثالثة
إدارة الاعطال

محتويات الوحدة

مقدمة

تمهيد

عزيزي الدارس، مرحبا بك إلى هذه الوحدة التي تتناول إدارة الأعطال، وهي المسئولة عن تحديد مكان العطل أو المشكلة في الشبكة والقيام بتصليحها. إذ تعتبر عملية إدارة الأعطال هي الأكثر أهمية من بين الأعمال الكثيرة الواقعة على عاتق إدارة الشبكة. وتتطلب عملية إدارة الأعطال ثلاثة مراحل هي:

- تحديد مكان العطل في شبكة البيانات.
- عزل سبب العطل.
- تصليح العطل (إن أمكن).

نستعرض في هذه الوحدة فوائد عملية إدارة الأعطال، ونناقش الخطوات الثلاثة المتعلقة بإتمام صيانة الأعطال في شبكة البيانات. ونصف ثلاثة احتمالات ممكنة للأدوات التي يمكن استخدامها. ونشرح بعض الطرق المتاحة لحصر الأعطال في نظام إدارة الأعطال

أهلا بك مرة أخرى إلى هذه الوحدة، وعسى أن تنتفع بها وأن تفيد منها ، وأن تساعدنا في نقدها .

أهداف الوحدة

عزيزي الدارس، بعد فراغك من دراسة هذه الوحـــدة ينبغـــي أن تكون قادرا على أن :

- تعرِّف فوائد عملية إدارة الأعطال.
- تصف متطلبات عملية إدارة الأعطال.
- تشرح طريقة تحديد مكان العطل في الشبكة.
- تعرف طريقة عزل سبب العطل في الشبكة.
- تشرح طريقة تصليح العطل في الشبكة.
- تصف طرق تجميع المعلومات اللازمة لتحديد المشكلة في الشبكة.
- تبرر بعض الأعطال الواجب إدارتها.
- تحلل كيفية إدارة الأعطال في نظام إدارة الشبكة.
- تستخدم الأدوات البسيطة والمركبة والمتقدمة في إدارة الأعطال.
- تبين تأثير الأعطال على الشبكة.
- تحدد طرق وأشكال تدوين أعطال الشبكة.

1. فوائد عملية إدارة الأعطال

عزيزي الدارس،

إن إدارة الأعطال **تزيد من اعتمادية الشبكة** Network Reliability وذلك بواسطة توفير الأدوات التي يحتاجها مهندس الشبكة كي يكتشف مشاكل الشبكة بسرعة ويبدأ عمليات العلاج اللازمة. ويعتبر ذلك مهما، لأن كثيراً من المستخدمين يعتمد كلية على شبكة البيانات لتأدية أعمالهم تماما مثل اعتمادهم على خدمات شبكة التليفونات. يتوقع المستخدمون عادة أن يكون كلا من شبكة البيانات وشبكة الهاتف متاحة لهم بشكل دائم، على الرغم من أنه من غير الطبيعي عدم توقع أن تعمل هذه الشبكات بكفاءة دوما. وعندما تعاني شبكة البيانات من فقدان الاتصال في الأجهزة أو الوصلات، فإنه تكون وظيفة مهندس الشبكة إجراء عمليات الصيانة اللازمة لتحقيق الاتصال المستمر بين المستخدمين والشبكة. وبتأدية هذا العمل، فإن ذلك يحسن من وجهة نظر المستخدمين على اعتمادية النظام. ولكن لسوء الحظ، فإن مهندس الشبكة في كثير من شبكات البيانات يبذل وقتا أكثر من اللازم في المكافحة من أجل صيانة مشكلة بعد أخرى. وبالرغم من أن إدارة الشبكة تؤدي إلى التغلب على هذه المشاكل ولو لوقت قصير؛ إلا أنها لا تترك وقتا لمهندس الشبكة لإجراء عمليات لتحسين الشبكة.

إن إدارة الأعطال تتيح وسائل متنوعة في توفير المعلومات الضرورية عن الوضع الحالي للشبكة. ومن الناحية المثالية، فإن هذه الأدوات تستطيع تماما تحديد متى تقع المشكلة. ويمكن تحويل هذه المعلومات في الحال إلى مهندس الشبكة. الذي يبدأ العمل في حل مشكلة العطل، حتى دون أن يدري المستخدمون بوجود هذه

الأعطال. وباستعمال إدارة الأعطال في معالجة مشاكل الشبكة، فإن ذلك يزيد كلا من فعالية الشبكة، وإنتاجية مهندس الشبكة.

2. تحقيق عمليات إدارة الأعطال

عزيزي الدارس، إن عملية إدارة الأعطال تتم في خطوات ثلاثة هي:

الخطوة الاولى تحديد العطل.

الخطوة الثانية عزل العطل.

الخطوة الثالثة تصليح العطل (إن أمكن).

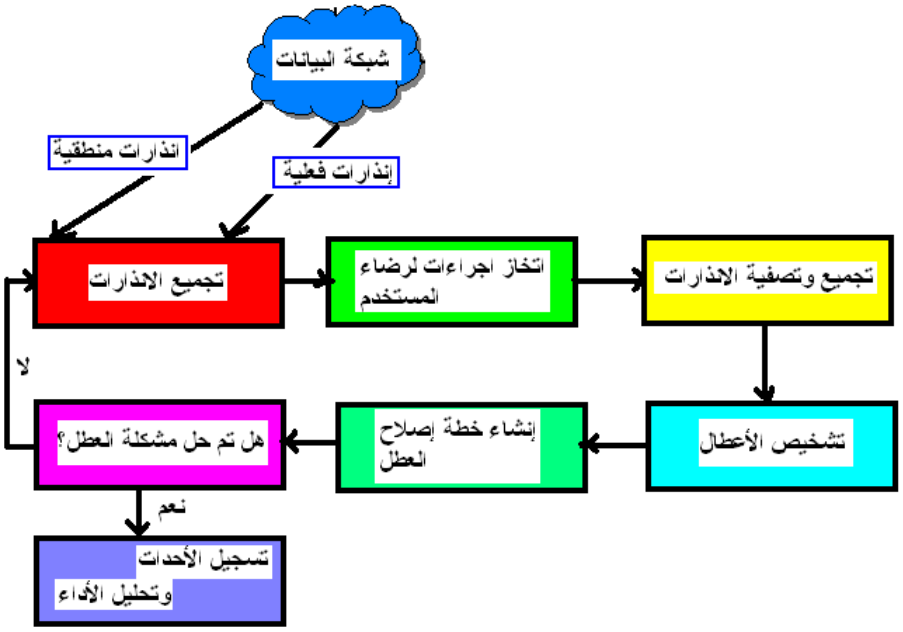
ويوضح شكل 1-3 مراحل عملية أداء إدارة الأعطال لشبكة البيانات.

يتم رصد وتجميع الإنذارات Alarms من أجهزة الشبكة، أو باستخدام التحاليل الإحصائية للشبكة والتي يتم رصدها من تخطي القيم الحرجة. ويمكن تقسيم الإنذارات إلى نوعين (الإنذارات المنطقية Logical Alarms ، والإنذارات الفعلية Physical Alarms). وتنتج الإنذارات الفعلية عن أعطال في عتاد الشبكة (مثل الوصلات المعطلة، أو أجهزة شبكة معطلة، قنطرة موجه- إلخ)، وتنتج الإنذارات المنطقية نتيجة أخطاء إحصائية ناتجة عن أداء سيء أو اختناقات Congestions.

وبعد تجميع وتدوين الإنذارات، فإنه يتم اتخاذ إجراءات خدمية مؤقتة لسد الثغرة الناتجة عن وجود العطل، بينما يتم إجراء عملية تشخيص العطل، كي نضمن أن المستخدم لا يعاني من فقد أو نقص في الخدمات. على سبيل المثال، يمكن تحويل حركة مسار الرسائل لمسارات بديلة، أو تغيير أجزاء العتاد التالف بأجزاء أخرى بديلة صالحة قريبة من موضع الخطأ.

وبعد ضمان عملية رضاء العميل، فإن الخطوة التالية هي أن يتم إيجاد علاقات الارتباط Correlations بين الإنذارات، و تصفية Filter الإنذارات. وذلك بواسطة تحليل الإنذارات وحذف الزيادات Redundant (الإنذارات المتكررة)

منها. ويتم تحديد الأعطال بواسطة تحليل الإنذارات التي تم تصفيتها وإيجاد العلاقات بينها، وكذلك بواسطة اختبارات الانتخاب Polling لمعرفة بيان حالة أجهزة الشبكة.

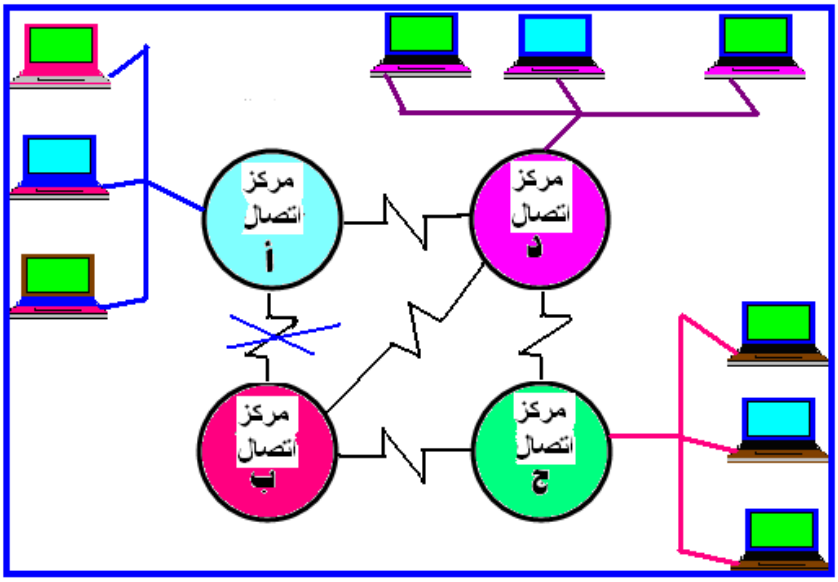


شكل 1-3 مراحل عملية إدارة الأعطال في شبكة البيانات.

وبعد تشخيص العطل، يتم اتخاذ إجراءات الإصلاح، وذلك بواسطة عزل سبب العطل. حيث يقوم نظام إدارة الأعطال بعملية الإصلاح، واتخاذ بعض الإجراءات طبقا للخطة الموضوعة للإصلاح. تتم عملية الإصلاح إما آليا بواسطة برامج وأجهزة التحكم في تشغيل الشبكة، أو بواسطة مهندس الشبكة، وذلك بواسطة إحلال مكونات صالحة للعمل بدلا من التالفة. يتم بعد ذلك تسجيل الأحداث التي وقعت في الشبكة وتشمل الأعطال ويتم عمل تحليل إحصائي بعد ذلك يفيد في بناء الخطة المتطورة لتوسعة الشبكة، وتحديد تكاليف عمليات الصيانة، وإلقاء الضوء على اعتمادية Reliability أنواع معينة لأجهزة الشبكة.

مثال على عملية إدارة الأعطال:

لتوضيح خطوات عملية إدارة الأعطال السابقة، نفترض الشبكة الموضحة في شكل2-3. بفرض أن مركز الاتصال في شبكة البيانات المسمى "أ" له وصلة واحدة بينه وبين شبكة البيانات الرئيسية. وقد تعطلت هذه الوصلة. في هذه الحالة سيتم الإبلاغ بأن نظام إدارة الشبكة المسمى "أ" لا يمكن الاتصال به. لتحقيق هذه الخطوة ة، فإن نظام إدارة الشبكة يستطيع عمل انتخاب Poll دوري لمركز الاتصال "أ" ليرى ما إذا كانت عملية الاتصال به ممكنة، أو يتم الاتصال بجهاز آخر قريب من الشبكة (قريبا من المركز "أ" فعليا) ويستطيع تحويل رسالة إلى النظام.



شكل2-3 يبين أن وصلة الاتصال بين مركزي الاتصال "أ"، "ب" معطلة.

الخطوة التالية وهى أنه ينبغي عزل سبب المشكلة (العطل). وهى أن مركز الاتصال "أ" لا يمكن الاتصال به بسبب أن وصلة خط التوالي من المركز إلى بقية الشبكة به عطل. وذلك باستخدام وصلة اتصال أخرى في الشبكة. والخطوة الثالثة

هي الاستعانة بالوسيلة التي تساعد على تصليح المشكلة (العطل)، إذا أمكن. في هذا المثال، يمكن تصليح المشكلة بواسطة توصيل وصلة أخرى بين المركز "أ" وشبكة البيانات.

يتضح من هذا المثال، أن استخدام عمليات تنفيذ إدارة الأعطال بشكل سليم تمكن مهندس الشبكة من تصليح الأعطال دون ضياع الوقت. ومن الملاحظ أن المهمة الأولى وهي تحديد المشكلة تعتمد على معرفة متى سوف تحدث. بعد ذلك نحتاج معرفة ما إذا كان تحديد هذه المشكلة هو ما سبب القلق. بعد ذلك نحتاج أن نقرر المشكلة الأكثر أهمية التي يجب أن يتم أخذها بعين الاعتبار، حيث إنه ليس كل المشاكل يمكن أن تعطي نفس الأولوية.

3. تجميع المعلومات اللازمة لتحديد عطل الشبكة

لمعرفة أنه يوجد بالفعل عطل أو مشكلة في الشبكة، نحتاج إلى تجميع بيانات عن حالة الشبكة. ونستطيع استخدام أحد الطريقتين التاليتين أو كلاهما معا وهما: إما أن يتم إدخال أحداث حرجة على الشبكة، أو أن يتم إجراء عملية انتخاب مرحلي على أجهزة الشبكة.

الطريقة الأولى: أحداث الشبكة الحرجة

Critical Network Events

يتم إرسال هذه الأحداث بواسطة جهاز الشبكة عندما يحدث شرط العطل. إن أحداث الشبكة الحرجة قد تكون على سبيل المثال: عطل في إحدى الوصلات – إعادة تشغيل جهاز – أو عدم استجابة من الحاسب المضيف Host. في معظم الحالات، فإن الاعتماد على هذه الأحداث بشكل مطلق، لا يوفر كل المعلومات اللازمة لإدارة الأعطال بفاعلية. على سبيل المثال، إذا لم يعمل أحد أجهزة الشبكة تماما، فإنه لا يستطيع إرسال أي حدث. وبذلك فإن أدوات إدارة الأعطال التي تعتمد اعتمادا مطلقا على أحداث الشبكة الحرجة، ربما لا تستطيع أن تظهر الحالة الحالية لكل أجهزة الشبكة.

2.3 الطريقة الثانية: إجراء عملية انتخاب مرحلي لأجهزة الشبكة

يمكن بهذه الوسيلة المعاونة في إيجاد الأعطال على أساس زمني. ولكن قبل استعمال هذه الطريقة يجب حساب الفترة الزمنية اللازمة لإيجاد المشكلة ومقارنتها مع سعة النطاق المطلوب. ويوجد عوامل أخرى يجب أخذها في الاعتبار، عندما يتم تحديد فترة الانتخاب. وهي عدد الأجهزة المطلوب إجراء عملية الانتخاب عليها وكذلك سعة نطاق الوصلات.

مثال: نفترض أن كل عملية استفسار واستجابة تحتاج 100 بايت (ويشمل ذلك البيانات ومعلومات المقدمة Header). وأن الشبكة بها 30 جهاز. عندما يتم إرسال 100 بايت من أجل الاستفسار، وكذلك استقبال 100 بايت استجابة من كل جهاز. فإن ذلك يعطي إجمالا 6000 بايت [(100 بايت + 100 بايت) x 30 جهاز]، وهذه القيمة تساوي 48000 بيت (6000 بايت x 8 بيت / بايت) من سعة النطاق المستخدمة لكل فترة تصويت. إن إجراء عملية التصويت كل 60 ثانية

سوف تعطي في المتوسط 800 بايت / ثانية وهذا يعادل 48000 بايت / 60 ثانية من سعة النطاق. وهذا يمكن من تحديد حالة كل الأجهزة في الدقيقة الواحدة. ويعنى ذلك أنه في خلال ساعة سوف نحصل على 172,800,000 بايت (48,000 بيت x 60 ثانية x 60 انتخاب). وهذه القيمة تعادل بالتقريب 173 ميجا بيت من سعة النطاق المطلوبة المتاحة في الشبكة. وأن هذه القيمة ربما تمثل ؛ أو لا تمثل ؛ عبئً ملحوظاً على الشبكة. عند إطالة فترة التصويت لتصبح 10 دقائق، فهذا يعطينا القيمة 17,280,000 بيت (48,000 بيت x 60 ثانية x 6 عمليات تصويت). وهذا يعادل واحداً إلى عشرة من سعة النطاق. ولكن إذا وقع حدث خلال فترة 10 دقائق، فربما لا يتم إدراك ذلك الحدث.

نستطيع أيضا استخدام أحد البروتوكولات الذي يمكن ببساطة إجراء عمليات التصويت على الأجهزة والتحقق من عملها. ومن أمثلة هذه البروتوكولات:

- ICMP Echo& Echo Reply (ping), *بروتوكول الصدى والاستجابة*
- Apple talk Echo, *بروتوكول أبل توك للصدى*
- Banyan Vines Echo, and *بروتوكول بانيان فينيس للصدى*
- SDLC Receiver Ready (RR) frames *بروتوكول أطر المستقبل*

ملحوظة: إن هذه الطريقة في حد ذاتها توفر فقط المعلومات التي تساعد في تحديد شرط عطل ممكن.

4. تحديد الأعطال الواجب إدارتها في الشبكة

عزيزي الدارس، ليس لكل الأعطال التي قد تحدث في الشبكة نفس الأولوية. بعض هذه الأعطال ربما نرغب في معرفة شيء عنها، والبعض الآخر ربما يريد النظام أن يتعامل معها بدون إخبارك، أو قد تهمل تماما. إن الأعطال التي ينبغي إدارتها هي أنواع الأعطال الأكثر أهمية في الوسط المحيط بشبكة معينة. وينبغي إجراء ذلك لعدة أسباب:

أولا: إذا ارتفع عدد الأعطال، ربما لا نستطيع التعامل معها.

ثانيا: بواسطة تحديد حركة الحدث Event Traffic، نستطيع تقليل عمليات الإرسال الزائد أو المعلومات غير المفيدة وتقليل الفقد في سعة نطاق الشبكة.

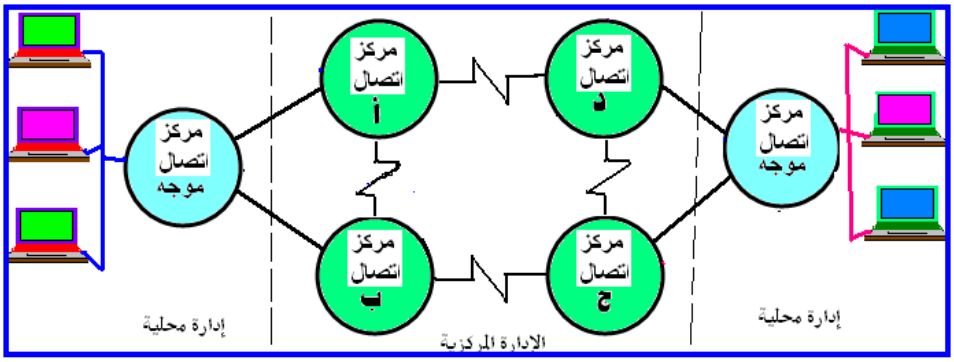
على سبيل المثال، نفترض أن صانع محطة العمل قد قرر توليد أحداث الشبكة عندما يقوم المستخدم بالدخول على النظام. بالرغم من أن هذا الحدث يوفر معلومات مفيدة من أجل الحسابات، فإنه غير مفيد (Irrelevant Event) لإدارة الأعطال. والآن نفترض أن أحد أقسام مؤسسة اشترى 100 محطة عمل. فإن مديري وحدات العمل تقوم بتهيئتهم ليس فقط باستخدام التهيئة المتوفرة من قبل المصنع (Default Configuration)، ولكن أيضا باستخدام التعليمات التي يتم إرسالها إلى أدوات إدارة الأعطال المركزية لكل أحداث الشبكة. ويتم ذلك في كل وقت يتم فيه دخول المستخدم. ويمكن لهذه الأحداث الدخيلة Extraneous Events أن تملأ بسرعة قاعدة بيانات نظام إدارة الشبكة. بالإضافة إلى ذلك فإن سعة النطاق التي تستخدم لإرسال هذه المعلومات يمكنها من الأفضل حمل بيانات المستخدم.

ويمكن حل هذه المشكلة بتمكين مهندس الشبكة من تهيئة كل أجهزة الشبكة كي تستطيع توليد مجموعة جزئية محددة من الأحداث الصالحة Valid Events. إذا كان هذا غير ممكن فإن نظام إدارة الشبكة يحتاج إلى طريقة لترشيح الأحداث القادمة، ويحذر مهندس الشبكة فقط من أحداث محددة .

إن تحديد الأعطال التي سوف يتم إدارتها أولا يعتمد على العوامل التالية:

- مجال التحكم الذي توفره الشبكة. وهذا يؤثر على كمية المعلومات التي نستطيع الحصول عليها من الشبكة.
- حجم الشبكة.

وتمثل المؤسسة المركزية في شبكات عديدة العمود الفقري لإدارة الشبكة، كما هو موضح في شكل3-3. ويتكون هذا العمود الفقري من أجهزة متنوعة مثل مفتاح الشبكة X.25 – موجهات IP – جسور Bridges. وأحد الترتيبات الشائعة هي أن تقوم المؤسسة المركزية بإدارة أحداث الشبكة الحرجة لكل أجهزة العمود الفقري للشبكة، وهذه الأحداث هي التي ربما تؤثر على الشبكة بأكملها. وبذلك يتم تفرغ الإدارة المحلية Local Administration لإدارة الأعطال فقط على الأجهزة و المعالجات المضيفة الخاصة بهم.



شكل3-3 فحص أحداث الشبكة الحرجة بواسطة الإدارة المحلية والمركزية.

ربما يستطيع مهندس الشبكة إدارة كل الأعطال لشبكة بيانات ذات حجم صغير نسبيا، تحتوى على 50 جهازاً، ويشمل ذلك أعطال المعالجات المضيفة – الموجهات – الجسور – المكرر Repeater – إلخ. وفي الشبكات متوسطة الحجم فإن مهندس الشبكة ربما يستطيع فقط إدارة الأعطال المتعلقة بالأحداث الحرجة لكل

من الحاسب المضيف وأجهزة الشبكة. وفي شبكات البيانات الضخمة فإن مهندس الشبكة ربما يجد الوقت لفحص الأحداث الحرجة الخاصة بالحاسبات المضيفة وأجهزة الشبكة الأكثر أهمية فقط في حالات الزيادات الأخرى، لحالات شائعة، فإن المؤسسة المركزية ربما تكون هي المسئولة عن إدارة كل الأجهزة على نطاق واسع. ويشمل ذلك، شبكات البيانات الموزعة على نطاق جغرافي. إذا كان بوسع هذه الشبكة إدارة كل أعطال الشبكة الضخمة، فإنه يجب توظيف نظام إدارة هرمي أو موزع. وهذه الطريقة تساعد في تكثيف عدد الأعطال الممكن رؤيتها ومتابعتها مركزيا. وربما تساعد في ترشيح وتشخيص هذه المعلومات للمعاونة في عزل العطل بسرعة. وفي الشبكات التي يتم توصيلها معا Inter-networks فإن البروتوكول RMON ربما يكون مفيداً جدا استخدامه في مثل هذه الشبكات. إن البروتوكول SNMP يحدد عدد سبعة أعطال حرجة، يتم كشفها بواسطة الأمر "Trap" الذي يستطيع توفير بداية للحصول على المعلومات من شبكة البيانات.

5. إدارة الأعطال في نظام إدارة الشبكة

عزيزي الدارس، بعد تحديد المشكلات المطلوب إدارتها ومعرفة كيفية تجميع بيانات عن حالة الشبكة، فإن الخطوة التالية هي تنفيذ وسائل إدارة الأعطال اللازمة. إن فاعلية الوسيلة (الأداة) سوف يعتمد بكثافة على نوع المعلومات التي توفرها أجهزة الشبكة.

1.5 الأداة البسيطة لإدارة الأعطال

إن أبسط أداة هي التي يمكنها تحديد وجود مشكلة ولكنها لا تبين سببها. فعلى سبيل المثال: الأداة البسيطة تستطيع إرسال رسائل صدى ICMP Echo تسمى "Pings" إلى كل حاسب مضيف وجهاز شبكة البيانات لاختبار إن كان متصلا بمستوى IP الشبكة. وتوجد هذه الأداة في بروتوكولات شبكات كثيرة مثل نوفيل IPX وبرتوكول أبل توك Appletalk حيث بها رسائل من نوع Echo. إذا لم يمتلك بروتوكول الشبكة هذه الإمكانية، فإن هذا الاختبار يمكن تنفيذه بواسطة كتابة برنامج يقوم بمحاولات تكرارية للاتصال بكل حاسب مضيف أو جهاز الشبكة.

في شبكة البيانات المعروفة باسم ميجانت، فإن بروتوكول الاتصال X.25 يستخدم في تنفيذ اختبار الصدى وذلك بمحاولة إنشاء دائرة تخيلى Virtual Circuit لكل عنوان هدف باستخدام X.121 (منظم العناوين) من خلال الشبكة. يتم تدوين الإخفاقات في عمليات الاتصال بالشبكة وذلك لإجراء فحوصات إضافية عليها. وتكون هذه الوسيلة مفيدة بالتحديد إذا كانت الحاسبات المضيفة أو الأجهزة ليست ممزقة بدرجة كافية كي تقوم بإرسال أحداث الشبكة.

إن الخرج الناتج عن هذه الأداة البسطة، يكون بسيطا مثل ملف الدخول أو معقدا مثل تغيير الألوان في الخريطة الهرمية. بعد أن يفقد الجهاز التوصيل، فإن الأداة البسيطة تنبه مهندس الشبكة كل فترة زمنية. من الممكن ضبط تنفيذ الأداة البسيطة كي توصل إلى جهاز الاستدعاء (Pager) مباشرة وترسل رسالة عددية بعنوان الشبكة لبيان الجهاز غير المستطاع الوصول إليه.

اسئلة تقويم ذاتي

لتحقيق عملية إدارة الأعطال في شبكة البيانات نتبع الخطوات الثلاثة التالية

1- .....

2- .....

3- .....

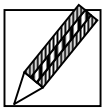
تأثير تبولوجي(شكل) الشبكة على تحديد مكان العطل:

إن الوسط المحيط للشبكات المحلية يكون له كوابل فعلية وأجهزة ربط مثل المكرر – الجسور – المجمع Hub. وقد يوجد للشبكة المحلية نوعين من التبولوجي Topology هما التبولوجي الفعلي Physical و التبولوجي المنطقي Logical. ويمكن تخطيط الشبكة المحلية بإمكانية أن يتم نقل منطقي لقطاعات Segments فعلية من أجهزة الشبكة. وهذا يعني أنه يوجد اختلاف في التبولوجي الفعلي عن التبولوجي المنطقي للشبكة. وعندما تقوم الأداة البسيطة بعملية تبليغ المعلومات فإن الجهاز أو القطاع لا يمكن الوصول إليه. ولهذا يجب أيضا وصف الشبكة المحلية التصورية الموجود بها تبولوجي الشبكة المحلية الفعلي، لمساعدة مهندس الشبكة في تشخيص المشكلة في وقتها.

وباستخدام الأداة البسيطة، فإن الحاسب المضيف قد لا يستطيع الوصول إليه من خلال الوحدة البينية لموجهات معروفة. إذا حدث ذلك فإن الأداة تغير لون الوحدة البينية للموجه لتبين أن الحاسب المتصل به لا يمكن الاتصال به. في الواقع، فإن الوحدة البينية للموجه يمكنها الاتصال بالشبكة المحلية التصورية، ويعني ذلك أن الحاسب المضيف الذي لايستطاع الوصول إليه ربما يكون في أي مكان في تبولوجي الشبكة. وتقوم الأداة البسيطة بعزل المشكلة الخاصة بحاسب مضيف موجود على الشبكة المحلية التصورية. ولكن لإيجاد المكان الفعلي بالضبط لهذا الجهاز ربما يتم ذلك مباشرة. أو ربما بواسطة اختبار الجهاز، حيث إن مهندس

الشبكة يستطيع إحضار معلومات تفصيلية عن مكانه من قاعدة بيانات نظم إدارة الشبكة.

تدريب (1)



أجب بلا أو نعم

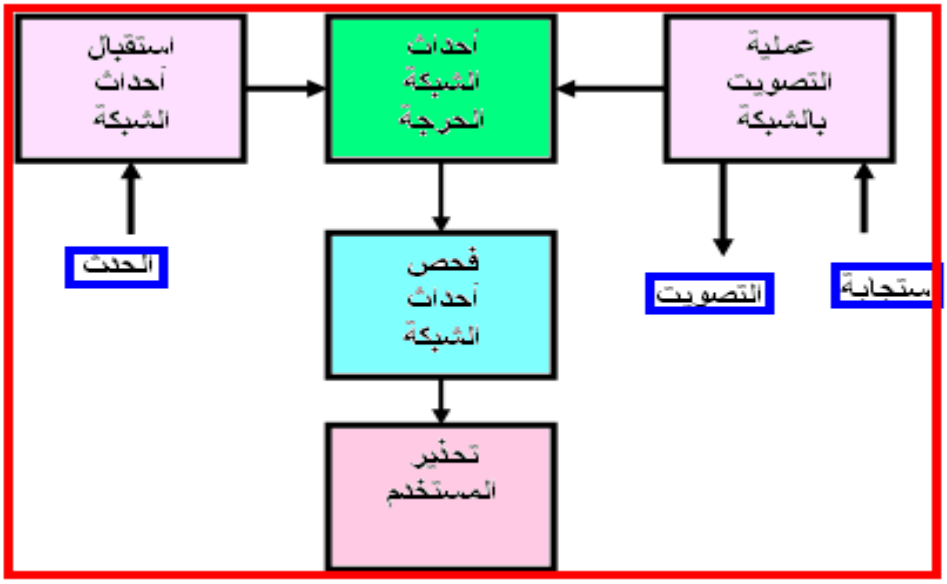
1) من فوائد عملية إدارة الأعطال في شبكة البيانات أنها توفر أدوات لكشف مشاكل الشبكة بسرعة.
2) من فوائد عملية إدارة الأعطال في شبكة البيانات أنها تزيد من اعتمادية الشبكة.
3) من فوائد عملية إدارة الأعطال في شبكة البيانات تحسين وجهة نظر المستخدمين في فعالية الشبكة.
4) تحدث الإنذارات المنطقية من شبكة البيانات نتيجة حدوث عطل في أجهزة الشبكة
5) تحدث الإنذارات المنطقية من شبكة البيانات نتيجة إصلاحات في الشبكة.
6) تحدث الإنذارات المنطقية من شبكة البيانات نتيجة اختناقات داخل الشبكة.
7) تحدث الإنذارات الفعلية من شبكة البيانات نتيجة حدوث إصلاحات في الشبكة.
8) تحدث الإنذارات الفعلية من شبكة البيانات نتيجة عطل في أجهزة الشبكة.

- **برمجيات الأدوات البسيطة المستخدمة لإدارة الأعطال:**

يوجد هذا النوع من الأدوات البسيطة في العديد من برامج إدارة الشبكة المتوفرة بالأسواق. إن برامج إدارة الشبكة يكون بها وسائل نوعية للاستفسار أيضا عن كل حالات الأجهزة، ويمكن تحسس Probe حالات الأجهزة من خلال الاتصالات مع الشبكة. كثيرا من برامج إدارة الشبكة تقوم مبدئيا بفحص الحالة التشغيلية للأجهزة، وبعد ذلك إذا أمكن فحص إحصائيات حيوية مثل تشغيل الوحدة البينية لكل جهاز. إن برنامج إدارة الشبكة يستطيع غالبا إيجاد حالة التشغيل للوحدة البينية لكل جهاز، حتى وإن لم يكن لهذه الوحدة البينية عنوان بالشبكة.

2.5 لأداة المركبة لإدارة الأعطال

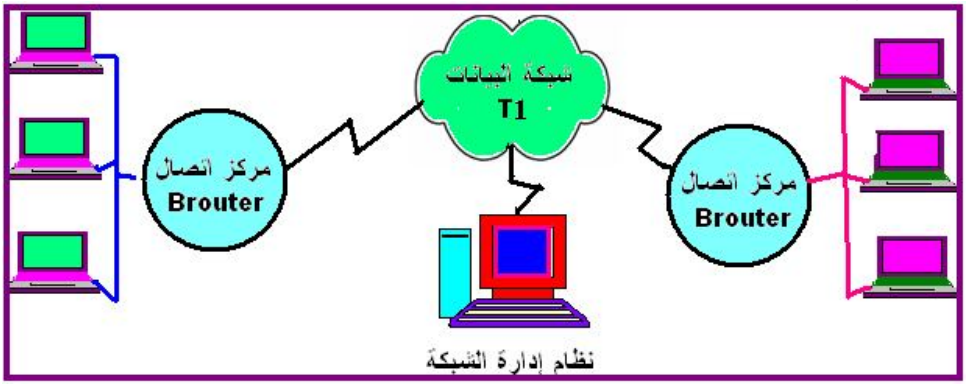
إذا كانت الحاسبات المضيفة والأجهزة الأخرى الموجودة بالشبكة متطورة بدرجة كافية لتدوين أحداث الشبكة، فإن الأداة المركبة يمكن تطويرها للاستفادة من هذه الإمكانية. إن هذه الأداة سوف تقوم بالتبليغ عندما تكتشف مشكلة، إما بواسطة دخول أحداث الشبكة أو بواسطة إجراء عمليةانتخاب Polling. إن عملية إيجاد العطل من خلال الأحداث الحرجة للشبكة يساعد أيضا في عزل السبب، أو على الأقل يقوم بتدوين الجهاز. ويوضح شكل4–3 خريطة التدفق لتوضيح كيفية أداء هذا التطبيق.



شكل4–3 خريطة تدفق تبين تتبع أداة مركبة لإدارة الأعطال في الشبكة.

كيفية عمل الأداة المركبة:

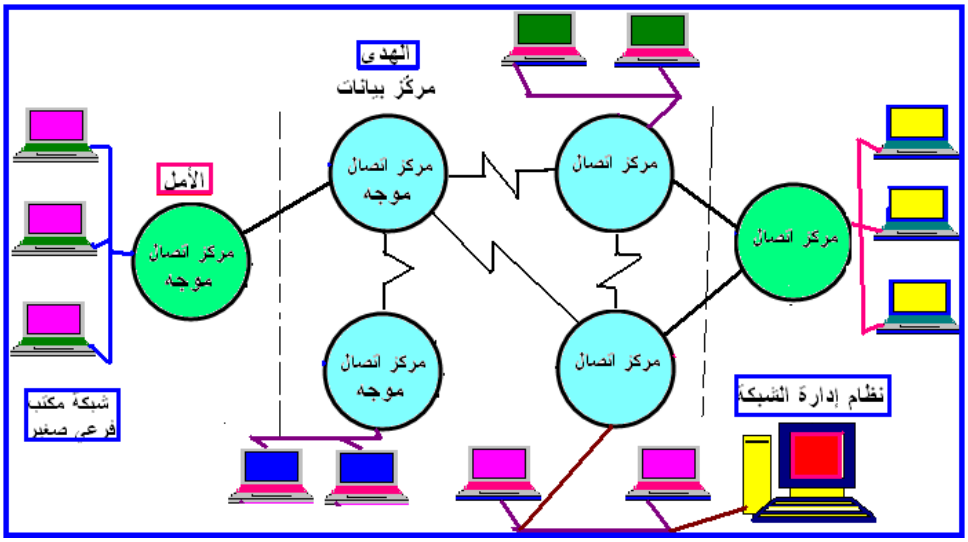
مثال1: لتوضيح كيفية عمل الأداة المركبة، نفترض نظام إدارة شبكة ميجانت الموضح في شكل 5–3. يقوم الجهاز T1 بتوفير دائرة سرعتها 1.544 ميجابت / ثانية بين وحدتين لجهاز موجه / قنطرة (بروتر Brouter) يستخدم بروتوكول الاتصال TCP/IP. إن الجهاز T1 يؤدي عمله بشكل صحيح، ولكن الدائرة الموجودة من قبل شركة التليفون المحلية تعطلت بسبب مشكلة العتاد Hardware. في هذه الحالة فإن كل "بروتر" يقوم بإرسال حدث شبكة حرج إلى نظام إدارة الشبكة. ويقوم التطبيق بعد ذلك في الحال، بتحويل هذه المعلومات إلى مهندس الشبكة.



شكل5–3 توصيل "بروترز" عن طريق شبكة T1 بسرعة 1.544 ميجابت/ثانية.

مثال2: تقوم شبكة ديكنت الموضحة في شكل 6–3 بتوفير مثال أكثر تعقيدا لكيفية استخدام القدرة التدوينية لأجهزة الشبكة. تشمل هذه الشبكة محطة عمل تسمى "الأمل" وهي عبارة عن موجه لشبكة ديكنت متوفر به ذاكرة مقدارها واحد جيجا بايت لإجراء جميع عمليات المعالجة اللازمة للشبكة بما في ذلك مخزن البفر (Buffer Storage). غير معروف لنا، إن هذه الذاكرة غير كافية لمعالجة أنشطة الشبكة المتوقعة من هذا النظام.

إن محطة العمل بمركز اتصال "الأمل" بها شبكة واحدة محلية متصلة بخط توالي بموجه شبكة مماثل يسمى "الهدى"، والذي تم تهيئة ذاكرته لتحتوى 5 جيجابايت لأغراض الشبكة. كما هو موضح بالشكل 6–3، فإن "الأمل" يقيم في مكتب فرعي صغير. بينما "الهدى" هو عبارة عن مركّز بيانات مركزي (Concentrator) متواجد في منتصف الشبكة. المسار المتوفر فقط للبيانات من "الأمل" إلى باقي الشبكة يكون من خلال وصلة توالي متصلة بجهازي الموجهين.



شكل6-3 شبكة ديكنت Dec_Net تربط بين موجه الهدى وموجه الأمل.

- **مظاهر العطل:**

نفترض الآن، أنه قد تم فجأة حدوث حركة مرور بيانات زائدة (Burst of Traffic) سببت طفح (Overflow) في ذاكرة وحدة مركز اتصال "الأمل" المخصصة للشبكة. وينتج عن هذا خطأ برمجي قد يسبب توقف عمليات تحديد المسارات (Routing) في شبكة "دكنت"، والذي بدوره يسبب تعطيل النظام. بعد برهة سوف يدرك مركز اتصال "الهدى" أن الوصلة قد تعطلت وسوف يرسل حدث شبكة حرج عن وصلة التوالي المعطلة إلى أداة إدارة العطل المركزية.

والآن يجيء دور الأداة لتحديد ما إذا كانت الوصلة الفعلية قد تعطلت حقا أم لا. تقوم أداة إدارة الوصلة بالاستفسار من " الهدى"، الذي قد قام توا بإرسال رسالة تفيد بأن "الوصلة معطلة". ربما بعد ذلك تحدد إذا ما كان وحدة التوالي البينية مازال بها إشارة حمل (Carrier Signal) وهي عبارة عن موجة متصلة تم تعديلها بواسطة المعلومات الموجودة على وصلة التوالي. إن إشارة الحمل تخبر الجهاز بأن الوصلة

تؤدى عملها. إذا قامت الأداة بتدوين أن "الهدى" قد قام بإرسال رسالة "الوصلة معطلة" وأن إشارة الحمل مازالت موجودة على الوصلة، فمن الناحية المنطقية يفترض أن السبب الحقيقي للعطل هو أن "الأمل" هو المعطل.

على الرغم من ذلك فإن وصلات التوالي تكون معطلة. بالرغم من أن كلا الجانبين من الوصلات يستقبل الإشارة الحاملة. حيث إن أجهزة المودم أو أجهزة الوصلة المستخدمة ربما ترسل إشارات حاملة متصلة إلي جهاز البروتر سواء أكانت الوصلة تعمل أو لا تعمل.

- **طريقة عزل العطل:**

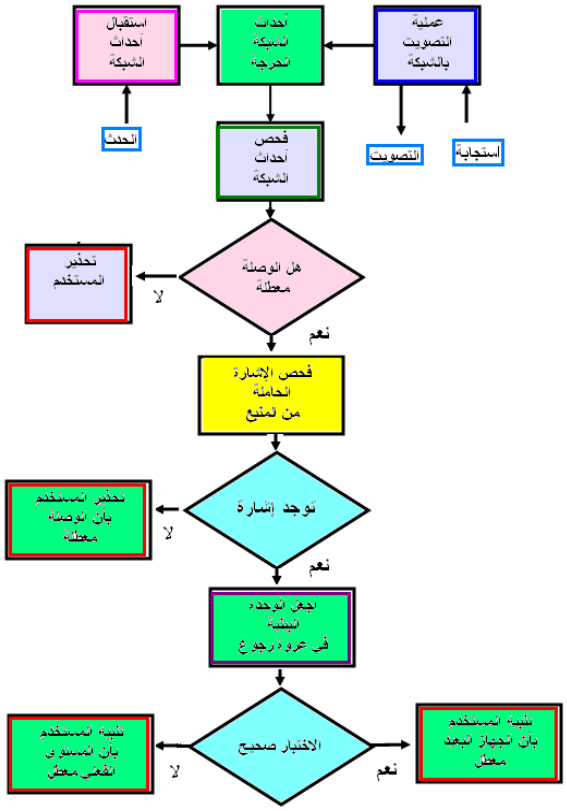
لعزل العطل، فإن أداة إدارة العطل تستطيع اختبار الوصلة بواسطة وضع وحدة التوالي البينية في "الهدى"، وتعمل حلقة رجوع (Loop Back)، ويتم إعطاء تعليمات للموجه باختيار الوحدة البينية الخاصة به. بإجراء هذا الاختبار سيتم اختبار العتاد والتوصيلية لجزء من الوصلة. إذا أخفق هذا الاختبار، فإن الأداة يجب أن تدون ذلك، على الرغم من وجود إشارة الحمل على الوصلة موضع الفحص، وأن البيانات لا يتم انتقالها أثناء عمل عروة الرجوع. بالإضافة إلى أنه إذا كان عتاد مستوى الوصلة الذي يدعم الوصلة يمكن الاتصال به فإن أداة إدارة العطل يمكن أن تشغل بعض اختبارات المستوى الفيزيقي على العتاد للتأكد من عمله. ويبين شكل 3-7 خريطة التدفق التي توضح كيفية أداء عمل هذا التطبيق.

- **تحديد سبب العطل:**

الآن يمكن لتطبيق إدارة الشبكة أن يخلص إلى أن سبب العطل هو وجود عيب في مركز اتصال "الأمل" أو الوصلة بين "الأمل" وبين "الهدى". وبأخذ هذه المعلومات في الاعتبار، فإن ذلك يعتبر سبب تعليق معقول. ولكن لا زلنا لا نعرف أي فكرة عن ما هو السبب الذي جعل وحدة "الأمل" تتعطل. بعد إعادة تشغيل "الأمل" لازالة

المشكلة (Clear the Problem)، فمن الأرجح أن هذا الحوار (Scenario) سوف يشفى Recur أثناء استعمال الذاكرة بكثافة متتابعة في وحدة موجه ديكنت. ربما فقط، بعد أعطال متكررة للموجه، سيكون من المفترض لنا أن نقوم بفحص تهيئة الذاكرة المخصصة للشبكة. بعد ذلك يتم إعادة تهيئة "مركز اتصال "الأمل" بشكل مناسب. ربما يتم منع تكرار العطل في الوقت الذي يقع فيه الحدث الأول إذا كان "الأمل" قد قام بإرسال رسالة حدث شبكة حرج إلى أداة إدارة العطل مدونا أنه كان يستخدم 80% من ذاكرته الشبكية.

محتمل رغم ذلك أن هذا النوع من الحدث ربما لا يستطيع توليد رسالة خطأ لتبليغها. ولكن عندما خلص (استنتج) التطبيق أن المشكلة توجد في مركز اتصال "الأمل" المعطل. فإنه بعد ذلك كان يجب عليه إجراء مسح لكل الأحداث التي وقعت حديثا لأي رسائل تم إرسالها لهذا الموجه بالذات. إن المعلومات الإضافية كان باستطاعتها تعجيل عملية إدارة العطل. من الناحية العملية، فإن الأدوات التي تؤدى كل هذه الخطوات تكون نادرة، أو لا وجود لها مطلقا. ولكن يوجد أدوات كثيرة منفردة تستطيع أداء (تحقيق) كل جزء معين من مجموعة التقنيات الشائعة (اختبار إشارة الحمل – وضع الوحدات البينية في حالة عروة رجوع عن بعد – فحص ملفات الدخول من أجل تصحيح الأعطال – الخ). ولا يوجد أداة منفردة تستطيع أداء وفعل كل شيء.



شكل7–3 تشغيل أداة إدارة العطل بعض الفحوصات لاختبار العتاد الفيزيقي للشبكة.

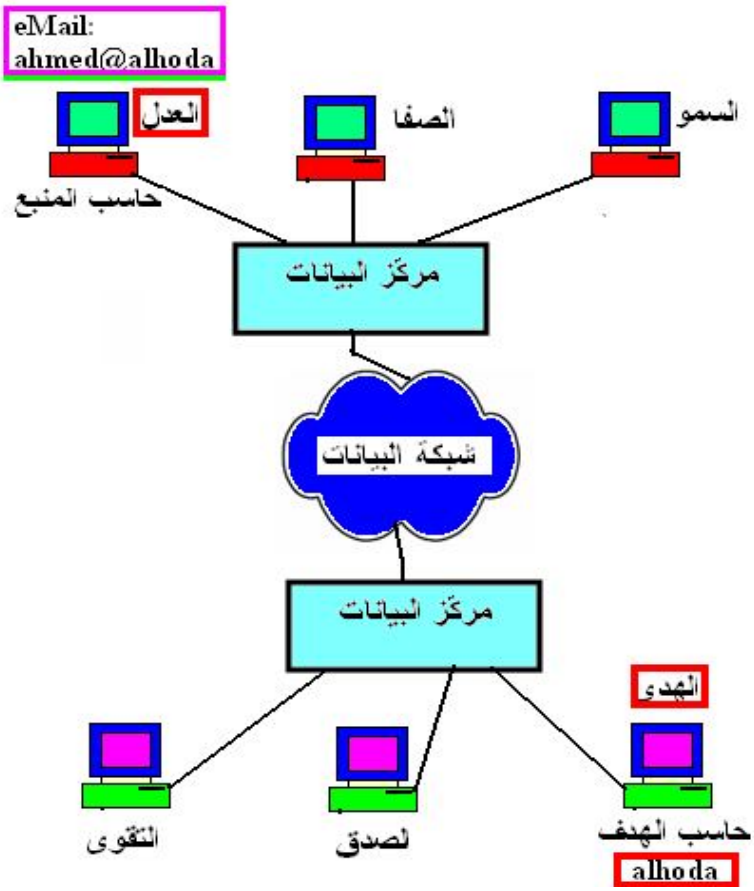
3.5 أدوات المتقدمة لإدارة الأعطال

عزيزي الدارس، إن الأداة المركبة التي تم شرحها سابقا، تحقق إدارة الأعطال إلى حد ما، ولكنها لا تحقق الخطوة الأخيرة، وهي تصليح المشكلة. في المثال التالي سنشرح كيف تستطيع أداة إدارة العطل التغلب على هذا الضعف في الاتصال بين الحاسبين المضيفين. إن كثيراً من أعطال شبكات البيانات تنتج من أعطال أجهزة الشبكة، ولكن المشكلة ليست دائما تقع من خلال عتاد الشبكة.

نفترض الوضع الذي يوجد فيه نظامان لا يستطيعان الاتصال من خلال الشبكة. في شبكة ميجانت، الموضحة في شكل 8–3، يوجد مستخدم على الحاسب المسمى "العدل" هو نظام المنبع، والذي قام بمحاولات عديدة غير ناجحة لإرسال رسالة بريد الكتروني إلى نظام الهدف المسمى "الهدى". تبين أداة إدارة الأعطال كل أجزاء أجهزة الشبكة التي يمكن أن تعمل، دون أن ترسل هذه الأجهزة أي أحداث حرجة، ولكن من الواضح أن هذا الجزء من الشبكة به تلف (معطل).

- **حل مشكلة الشبكة:**

لحل مشكلة الشبكة، يتم فصل الوظائف إلى وحدات صغيرة يمكن تميزها. في هذا الوضع يتم أولا، تحديد الأجهزة التي توفر الوصلة الحالية بين حاسب "العدل" وحاسب "الهدى". بعد ذلك نقوم بفحص كل خطوة عبر المسار، بداية من المنبع. إذا وجد خطأ عند أي خطوة، نقوم بفحص هذا الجزء بالقرب من هذه الوحدة أكثر حتى يتم إيجاد هذه المشكلة. وسوف نشرح هذه الطريقة بالتفصيل تباعا.



شكل8-3

لا يستطيع المستخدم في حاسب "العدل" إرسال بريد الكتروني إلى حاسب "الهدى". تستخدم أداة إدارة الأعطال المتطورة بروتوكول إدارة الشبكة. وذلك لفحص كل جهاز موجود بالمسار حتى يتم الوصول للجهاز الموجود قبل حاسب "الهدى". نفترض أن كلا الحاسبين يستطيعا الاتصال بكل جهاز موجود على المسار بينهما، ولكن لا يستطيعان الاتصال مع بعضهما. بناء على بروتوكول الشبكة المستخدم، فإن طريقة الفحص تتم بواسطة الاستفسار من جدول المسارات Routing Table

عن كل جهاز موجود بالمسار، بداية من المنبع حتى الوصول إلى حاسب الهدف. وبالعودة إلى المشكلة، نجد أن الأداة اكتشفت عدم وجود عطل على أي من هذه الأجهزة الموجودة في المسار. ولكن المستخدم مازال لا يستطيع إرسال بريد الكتروني خلال الشبكة. عند هذه النقطة، سوف تقوم الأداة بتشغيل مجموعة جديدة من الاختبارات على كل جهاز بين الحاسبين. على الرغم من أن ذلك قد يستغرق وقتا، لكنه سوف يتم فحص للمشاكل الكثيرة الممكنة.

فحص وتحديد سبب المشكلة:

- **الطريقة الأولى: استخدام وحدة النقل العظمى:**

أحد هذه الاختبارات هو فحص معدلات الخطأ على كل نظام وسيط (Intermediary) وأجهزة الشبكة. ولإجراء ذلك يتم إرسال حزم بيانية ذات أطوال مختلفة من حاسب المنبع إلى حاسب الهدف لمعرفة إذا ما حدث خطأ. أحد الطرق الجيدة لمعرفة ذلك، هو أن نجد وحدة إرسال عظمى MTU (Maximum Transmission Unit) على المسار. ونجري الاختبار بإضافة 100 بايت زيادة كل مرة حتى نصل إلى حجم حزمة البيانات العظمي التي يسمح بها وسط الشبكة. ويوجد في بروتوكولات عديدة مثل IP طرق ديناميكية لاكتشاف المسار عبر وحدة MTU.

- **الطريقة الثانية: فحص أخطاء الدخول:**

إذا أثبت اختبار وحدة الإرسال العظمى، عدم حسم (Inconclusive)، فإن الأداة بعد ذلك سوف تفحص عملية البريد الإلكتروني في كلا النظامين بواسطة محاولة إرسال رسائل من "العدل" إلى "الهدى" وبعد ذلك يتم فحص أخطاء الدخول (Error Logs). إن معظم نظم البريد الإلكتروني مثل نظام بريد لوتس cc:Mail أو نظام بروتوكول نقل البريد البسيط SMTP(Simple Mail Transport Protocol)

يوجد بها رسائل أوشفرات خطأ قياسية تستطيع أداة إدارة الأعطال إعادة برمجتها ليتم فهمها. أو تستطيع الأداة محاولة استخدام خدمات شبكة أخرى لتحقيق الاتصال، مثل نقل ملف بين الحاسبين.

- **اختبار وعزل منبع المشكلة:**

إن حاسب "العدل" متصل بالشبكة بوحدة التوصيل Hub بواسطة زوج أسلاك مجدولة. بإجراء هذا الاختبار الإضافي، فإن الأداة تكتشف أن حزم البيانات الضخمة التي تنتقل من خلال وحدة التوصيل Hub تتعطل عند أكثر من 55 % من الزمن. تكون رسالة البريد الإكتروني التي يحاول المستخدم إرسالها ضخمة إلى حد بعيد، وأن التطبيق الذي قام بتقسيم هذه الرسالة إلى حزم بيانية قد استخدم طول حزمة بيانية ضخم. وبذلك تقوم الأداة بعزل منبع المشكلة. وتحديد أن منفذ وحدة التوصيل Hub، ربما يكون هو المشكلة. تستطيع الأداة نقل المنفذ المتصل به حاسب "العدل" إلى شبكة البيانات (إذا كان البرنامج الموجود في وحدة التوصيل Hub يسمح بذلك العمل).

- **إصلاح المشكلة:**

إن كثيراً من أجهزة Hub الجديدة المتوفرة في الأسواق، تسمح برامجها بإعادة تهيئة منافذ معينة داخل وحدة Hub (وتسمى هذه الخصائص أحيانا: الشبكة المحلية الوهمية). بعد ذلك سوف تقوم الأداة بإعادة تشغيل الاختبار مع استخدام أطوال حزم بيانية ضخمة. في هذه المرة، فإن الوصلة من جهاز وحدة Hub إلى حاسب "العدل" سوف ترسل 100% من البيانات بدون خطأ. وبذلك تكون الأداة قد قامت بإصلاح المشكلة. كخطوة أخيرة، فإن الأداة تستطيع إنتاج سجل بالطريقة التي استعملتها في إيجاد المشكلة كي يستطيع مهندس الشبكة إصلاح المنفذ الذي لا يعمل.

أسئلة تقويم ذاتي

ارسم خريطة تدفق توضح كيفية تشغيل أداة إدارة الأعطال لبعض فحوصات اختبار العتاد الفيزيقي للشبكة.

اشرح مع الرسم كيف تستخدم الخريطة الهرمية في تتبع الأعطال وعزل العطل في شبكة البيانات.

6. تأثير الأعطال على الشبكة

عزيزي الدارس، يجب أن تكون أداة إدارة العطل قادرة على تحليل كيف يستطيع العطل أن يؤثر على المناطق الأخرى في شبكة البيانات. بعد ذلك فقط يمكنه تزويدنا بتحليل كامل عن العطل. على سبيل المثال: نفترض الوضع الشائع الذي يقوم فيه القمر الاصطناعي بتوصيل بعض مراكز شبكات اتصال مؤسسة "ديكنت" في مصر وشبكات "سنا SNA" في فرنسا. إذا تعطلت هذه الوصلة، فإن الأداة سوف تخبرنا عن العطل. وأن الأداة سوف تحاول أيضا تصليح المشكلة، ربما بتدوينها إلينا في عبارة مثل التالية:

"الوصلة معطلة بين "مركز اتصال" مصر و "مركز اتصال"

هذه المعلومات مفيدة، ولكنها لم تخبرنا أن هذا العطل قد قطع الاتصال بين شبكات "ديكنت" في مصر وبين شبكات " سنا " في فرنسا. بهذه المعلومات الإضافية، فإن هذا العطل يتطلب إجراء اهتمام فوري. ولهذا فإن عبارة أخرى بديلة عن السابقة يمكن أن تكون كما يلي:

"الوصلة" معطلة بين "مركز اتصال" مصر و "مركز اتصال" فرنسا .
"توقفت" حركة مرور الرسائل بين شبكة ديكنت وشبكة سنا.

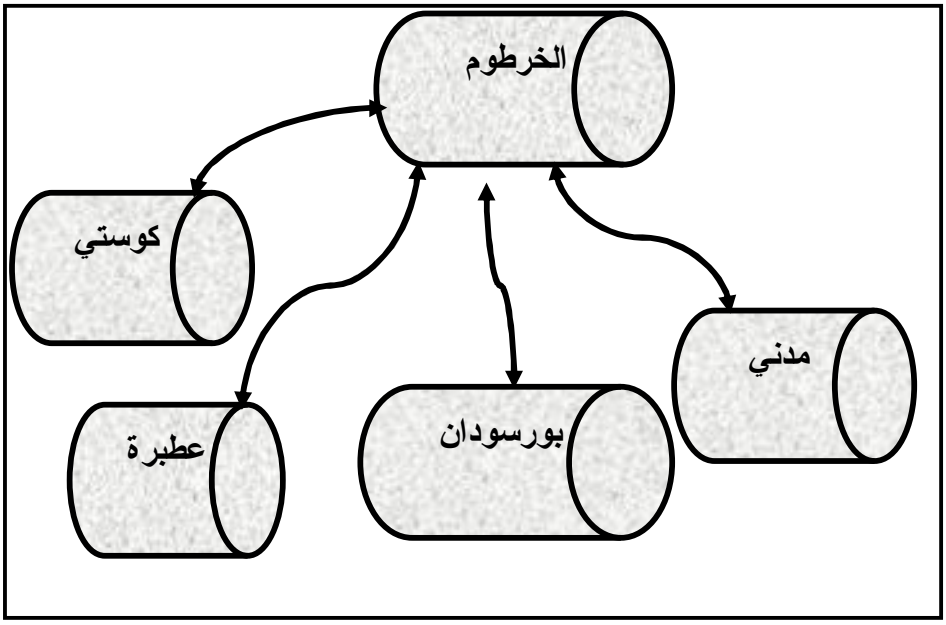
ولكن الآن، دعنا نقول إن شبكة بيانات المؤسسة بها وصلة أرضية Terrestrial بين مصر وفرنسا بالإضافة إلى وصلة القمر الاصطناعي. وأن كلا من هاتين الوصلتين تخدم حركة نقل الرسائل بين شبكة "ديكنت" وشبكة "سنا". والآن عندما تجد أداة إدارة العطل أن وصلة القمر الاصطناعي معطلة، فإن الرسالة قد تأخذ هذا الشكل:

"الوصلة" معطلة بين شبكة "مركز اتصال" مصر و "مركز اتصال" فرنسا
وقد أثر ذلك على حركة مرور الرسائل بين شبكة "ديكنت" بمصر وشبكة "سنا" بفرنسا

في هذه الحالة، فإن حركة مرور الرسائل سوف تتأثر، ولكن لن تتوقف تماما.
وبفرض أن شبكة الخرطوم بها شبكة فرعية تعمل ببروتوكول الاتصال X.25 و بها مفتاح ضخم في الخرطوم يقوم بتوصيل المدن مدني، عطبرة بورسودان، كوستي ، سيناء، المنصورة مع بقية الشبكة، كما هو مبين في شكل 9-3. إذا تعطل المفتاح X.25 عند نقطة ما، فإن أداة إدارة العطل قد تعطي رسالة مثل:

مفتاح الاتصال x.25 قد تعطل في شبكة اتصال الخرطوم .
لايوجد اتصال بين الخرطوم، مدني، بورسودان، عطبره، كوستي

في هذه الحالة نعرف أنه ليس فقط يوجد عطل، ولكن نعرف أيضا كيف يؤثر هذا العطل على شبكة الاتصال.



شكل9-3 استخدام مفتاح X.25 لتوصيل الخرطوم مع بعض المدن الأخرى.

إن تصميم أداة إدارة العطل يكون لها المقدرة على تدوين هذه الأنواع من الأخطاء، وكذلك تأثيراتها، فليس ذلك عملا مستحيلا. حيث سنجد عند دراسة إدارة الأداء، أن معلومات عن نوع البيانات التي تنتقل من أجهزة الشبكة يمكن تخزينها عن طريق نظام إدارة الشبكة، لكي يمكن استعمالها من قبل أدوات إدارة الأعطال.

7. أشكال تدوين الأعطال

عزيزي الدارس، إن الشكل الذي تدون به الأعطال قد يكون على درجة من الأهمية بقدر عملية إدارة الأعطال. إن معظم أشكال الرسائل المألوفة قد تكون على شكل: رسائل نصية – رسائل جرافيك – أو رسائل صوتية.

تعتبر الرسائل النصية أحد الخيارات المقبولة لأنه يصلح استعمالها في كل أنواع الطرفيات سواء أكانت ملونة أو غير ملونة. ولكن الرسالة المصورة تكون أكثر فاعلية وتأثيراً. ولكن لإرسال هذا النوع من الرسائل، فإن أداة إدارة العطل سوف تحتاج أن توصل بوحدة عرض ملونة. من الناحية المثالية، فإن أداة إدارة العطل تكون مقيمة في نظام إدارة الشبكة. وبذلك فإن هذا لا يعتبر مشكلة حتى بدون ألوان، فإن أحد طرق جذب اهتمام مهندس الصيانة هو عرض صورة متلألئة (Flashing) للجهاز الذي يوجد به العطل.

وتمتاز الرسائل التي على شكل إشارات مسموعة، بأنها تجذب انتباه مهندس الصيانة بسرعة إلى الأداة، وخاصة إن كان يعمل في منطقة أخرى. ربما تكون هذه الطريقة غير ملائمة، ولكن قد تعمل الأداة في مركز عمليات مشغول بكثير من العاملين ونظم الرصد. في مثل هذه الحالات، ربما يكون من الأفضل دمج أكثر من شكل معا. على سبيل المثال: في حالة عطل المفتاح X.25، فإن صورة للعطل ربما تظهر العطل الموجود بشبكة الخرطوم كموقع معطل، وأن المواقع الخارجية الأخرى تظهرها كمواقع متأثرة بهذا العطل. ويمكن أن توضح صورة العرض هذه بإضافة رسالة نصية.

سؤال تقويم ذاتي

قارن بين نظام استخدام الرسائل النصية ورسائل الجرافيك عند تدوين الأعطال التي تحدث في شبكة البيانات، وذلك من حيث المزايا والعيوب.

1.7 مميزات استخدام الرسومات الملونة

وعلى الرغم من أن التطبيقات الأخرى في نظام إدارة الشبكة ربما لا تحتاج رسومات ملونة لمخرجاتها، فإن هذه الرسومات الملونة تكون مفيدة جدا خاصة في إدارة الأعطال. على سبيل المثال، إن عرض متوسط زمن حدوث الأعطال للأجهزة قد لا يعتمد على استعمال الألوان، فإن عرض رسالة نصية ربما تكون كافية في هذا التطبيق التحليلي للشبكة. وبالمثل، في إدارة الحسابات وإدارة الأمن فإن عرض رسائل نصية بسيطة عادة يكون كافيا لتدوين النتائج. على الرغم من ذلك، فإن الرسومات، حتى بدون ألوان، سوف تساعد في تبيان حالة أجهزة الشبكة. إذ أن إضافة الألوان للتطبيق يمكن أن يوضح حالة أجهزة الشبكة بكفاءة. فمثلا: إن وحدة المواجهة الرسومية يمكن أن توضح كل جهاز مرسوم على الخريطة بواسطة إدارة الشبكة.

2.7 استخدام الخريطة الهرمية لتتبع أعطال الشبكة

في الشبكات الأكثر تعقيدا، قد يتطلب الأمر وجود خريطة هرمية بها كل مراكز الاتصال التي تعبر عن بناية، مدينة، أو حتى مدن كثيرة. كل مركز اتصال من هذه المراكز يمكن أن يؤدي إلى خريطة أخرى بها مراكز فرعية أصغر، كما هو موضح في شكل 3–10. وأخيرا ربما من خلال خطوات متعددة، فإن كل جهاز

محدد في الشبكة يمكن إظهاره. لبيان حالة كل جهاز في شبكة البيانات، يمكن استخدام نظام ألوان كما هو مبين في جدول 1-3.

بناء على نظام الألوان السابق، فإن الجهاز الأخضر يكون هو الجهاز الذي لم يعانى من أي أحداث شبكة حرجة. وأن الجهاز الأحمر يكون به عطل. ربما يكون الجهاز الأحمر هو أحد الأجهزة التي لم تجيب على عمليةالانتخاب، لأنه لم يسمع التصويت أم أنه يرسل إجابات غير ذكية. يستخدم اللون الأصفر لبيان الأجهزة التي لا تستجيب إلى تصويت متتالي وحيد، ليبين أن هذا الجهاز به خطأ.

في هذه الحالة فإن أداة إدارة الخطأ سوف تظهر حالة الجهاز باللون الأصفر، حتى حدوث فترتين تصويت دون استجابة الجهاز. تحت هذا الشرط، فإنه في حالة

جدول3.1 استخدام نظام الألوان لبيان حالة كل جهاز في شبكة البيانات.

اللون	المظهر	حالة الجهاز في شبكة البيانات
الأخضر		إظهار الجهاز بدون خطأ
الأصفر		الجهاز ربما يكون به خطأ
الأحمر		الجهاز في حالة خطأ
الأزرق		الجهاز يعمل ولكن في حالة خطأ
البرتقالي		الجهاز غير مهيأ
الرمادي		لا يوجد معلومات عن الجهاز
الأرجواني		الجهاز تم أخذ تصويته Polled

الجهاز الذي تغير لونه إلى الأصفر، سوف ينتظر فترة التصويت الثانية، فإذا أخفقت، سوف يتم تغيير لون الجهاز إلى الأحمر. أما إذا تحول لون الجهاز من الأخضر إلى الأحمر في كل مرة يتم فيها إجراء انتخاب منفرد، ولا يوجد استجابة، فإن هذا يشير إلى أن الأجهزة تعمل وتقف عدة مرات. يستخدم اللون الأصفر أيضا عندما يوجد إمكانية إجراء عمل نسخ احتياطي آلي (Automatic Backup) لبعض المكونات التي تعطلت والتي قام الجهاز بتعويضها.

اسئلة تقويم ذاتي

يبين الجدول التالي اللون المستخدم في نظام إدارة الأعطال وبيان حالة الجهاز. وفق اللون الصحيح مع ما يقابله من حالة بيان الجهاز.(رتب القائمة صحيحاً)

رقم اللون	لون الجهاز	بيان حالة الجهاز	رقم بيان الحالة
1	اخضر	الجهاز غير مهيأ	أ
2	اصفر	لا يوجد معلومات عن الجهاز	ب
3	احمر	الجهاز بدون خطأ	ج
4	ازرق	الجهاز ربما يكون به خطأ	د
5	برتقالي	الجهاز في حالة خطأ	و
6	رمادي	الجهاز يعمل ولكن في حالة خطأ	ل
7	ارجواني	الجهاز تم أخذ تصويته	ع

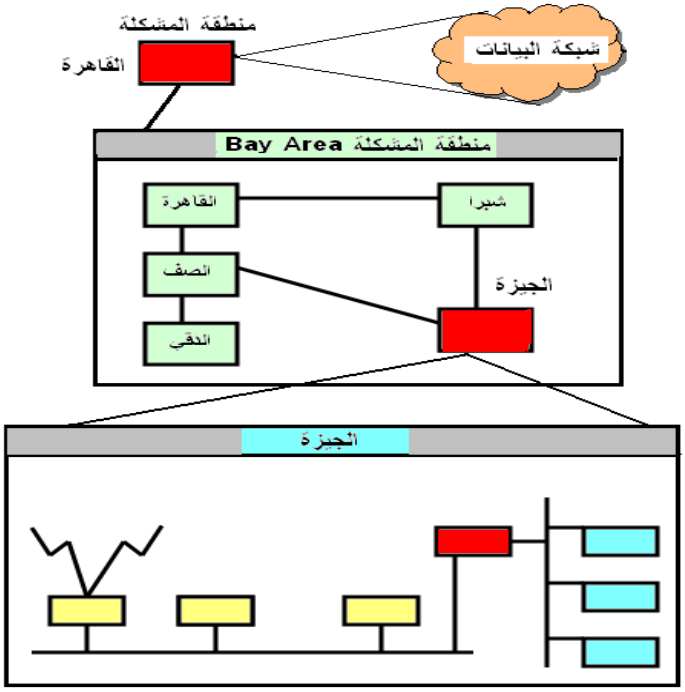
- **الاتصال الاحتياطي Dial Backup**

مثال: يوجد أجهزة عديدة مثل: المجمع – الموجهات – وصلات الشبكة ويكون لها منبع جهد كهربي احتياطي، عندما يتعطل أحدهما فإن الثاني يعمل بدلا منه آليا. بالمثل يوجد في بعض الأجهزة الأخرى خصائص مشابهة من مكونات العتاد، مثل: المعالجات، ووحدات المواجهة. إن اللون الأصفر قد يعني أن الجهاز ليس به خطأ ولكن حالته لم تصل للحد الحرج بعد. على الرغم من أن اللون الأصفر قد يعني أن الجهاز قد قام بتصليح مشكلة الشبكة بدون تدخل يدوي. بعض الأجهزة لها المقدرة على إجراء ما يسمى بالاتصال الاحتياطي "Dial Backup" لرصد وصلة Link وإذا فشلت، فإنها تشغل وصلة أخرى بديلة آليا. ويتطلب ذلك وجود جهاز مودم متوافق مع نظام V.24. إذا كان الجهاز في حالة خطأ وعاد بعد ذلك إلى حالته العادية، فإن الجهاز يتغير لونه إلى الأزرق. ليبين لنا أنه الآن يعمل في حالة عادية بعد أن كان يعاني من عطل حديث سابق.

الجهاز الذي كان لونه برتقالياً، يظهر أنه كان غير مهيأ، وهذا ربما ينتج عن أن له (كلمة سر Password غير صحيحة – عنوان شبكة غير صحيح – عدد الوحدات البينية غير صحيح – أو ما يشابه ذلك). كذلك ينبغي فحص خصائص التهيئة الخاصة لهذه الأجهزة البرتقالية اللون. إذا لم يوجد أي معلومات عن أحد هذه الأجهزة، فيجب تلوينه باللون الرمادي، لبيان أنه ربما لم يتم إجراء عملية التصويت عليه، أو ربما لم يجيب مطلقا على عملية الانتخاب. وأخيرا فإن الأجهزة الملونة باللون الأرجواني، تكون هي الأجهزة التي تم إجراء عمليات الانتخاب عليها حاليا، ويجب على مهندس الشبكة متابعتها ليرى مدى تقدم عملية الانتخاب.

- **استخدام الخريطة الهرمية لعزل الأعطال**

إن الأحداث التي تؤثر على الأجهزة، يمكن أن تغير لون مراكز الاتصال Nodes ذات المستويات العليا في الخريطة الهرمية، وسوف يتم تحديدها بواسطة نظام إدارة الشبكة. من الناحية العملية، فإن المستويات الفوقية المباشرة للأجهزة التي تم إظهارها، سوف يتم تغير لونها تبعا لاستجابة الأحداث الحرجة بالشبكة.



شكل10-3 استخدام الخريطة الهرمية لعزل الأعطال.

لبيان كيفية عمل الخريطة الهرمية مع تخصيص الألوان، يتم تلوين صورة شبكة البيانات بكاملها مثل سحابة (a Cloud). يعبر لون السحابة الخضراء على أنه لم تقع أي أحداث حرجة داخل الشبكة. إذا تغير لون السحابة إلى الأحمر، فإن هذا يجعل مهندس الشبكة يقوم بفحص الوحدة البينية الرسومية الهرمية لإيجاد الجهاز المعطل. ربما تنتشر السحابة إلى خريطة العالم التي يوجد بها مدينة واحدة محددة قد تم تلوينها باللون الأحمر. يمكن الوصول بعد ذلك إلى تبولوجي شبكة هذه المدينة، والوصول إلى الجهاز ذي اللون الأحمر. ثم يتم تدوين التفاصيل إلى مهندس الشبكة لبيان الخطوات التي قد قام النظام باتخاذها فعلا لتصليح الخطأ.

الخلاصة

عزيزي الدارس ، تعرفنا في هذه الوحدة على إدارة الأعطال و عرفنا انها هي المسئولة عن تحديد مكان العطل أو المشكلة في الشبكة والقيام بتصليحها. إذ تعتبر عملية إدارة الأعطال هي الأكثر أهمية من بين الأعمال الكثيرة الواقعة على عاتق إدارة الشبكة. كذلك تناولنا متطلبات عملية إدارة الأعطال من خلال مراحلها الثلاثة :تحديد مكان العطل في شبكة البيانات.

عزل سبب العطل.تصليح العطل (إن أمكن).

واستعرضنا في هذه الوحدة فوائد عملية إدارة الأعطال، و الخطوات الثلاثة المتعلقة بإتمام صيانة الأعطال في شبكة البيانات. ووقفنا على ثلاثة احتمالات ممكنة للأدوات التي يمكن استخدامها. و بعض الطرق المتاحة لحصر الأعطال في نظام إدارة الأعطال.

لمحة مسبقة عن الوحدة القادمة

عزيزي الدارس، في الوحدة القادمة نتناول إدارة التهيئة، وكيفية الحصول على البيانات من الشبكة، واستخدام هذه البيانات في إدارة وتنصيب كل أجهزة الشبكة. سنتناول كذلك تجميع معلومات عن التهيئة الحالية للشبكة، واستخدام هذه البيانات في عملية تعديل تهيئة أجهزة الشبكة، وتخزين البيانات، والاحتفاظ بقائمة حديثة، وتدوين تقارير مبنية على البيانات. في الوحدة الدراسية القادمة سوف نشرح أيضاً فوائد إدارة التهيئة بالنسبة لمهندس الشبكة. ونناقش الخطوات اللازمة لإدارة عملية التهيئة.. كما نعرض التقارير المختلفة التي يمكن الحصول عليها من بيانات التهيئة. كن معنا في الوحدة القادمة وستجد الكثير المفيد إن شاء الله

مسرد المصطلحات

أحداث الشبكة الحرجة Critical Network Events

هي التي يتم إرسالها بواسطة جهاز الشبكة عندما يحدث شرط العطل.

حركة الحدث Event Traffic

من الاعطال التي يجب إدارتها وبها نستطيع تقليل عمليات الإرسال الزائد أو المعلومات الغير مفيدة وتقليل الفقد في سعة نطاق الشبكة

رسائل صدى ICMP Echo

تسمى "Pings" إلى كل حاسب مضيف وجهاز شبكة البيانات لاختبار إن كان متصلا بمستوى IP الشبكة. وتوجد هذه الأداة في بروتوكولات شبكات كثيرة مثل نوفيل IPX وبرتوكول أبل توكِ AppleTalk حيث بها رسائل من نوع Echo.

الإدارة المحلية Local Administration

لإدارة فقط الأعطال على الأجهزة و المعالجات المضيفة الخاصة بهم.
وهذه الأحداث هي التي ربما تؤثر على الشبكة بأكملها. وبذلك يتم تفرغ

المصطلح بالإنجليزية	معناه بالعربية

المصطلح بالإنجليزية	معناه بالعربية
Automatic Backup	نسخ احتياطي آلي
Buffer Storage	مخزن مؤقت
Burst of Traffic	حركة مرور بيانات زائدة
Carrier Signal	إشارة حمل
Congestions	اختناقات
Concentrator	مركّز بيانات
Correlations	علاقات الارتباط
Critical Network Events	أحداث الشبكة الحرجة
Dial Backup	الاتصال الاحتياطي
Default Configuration	التهيئة المتوفرة من قبل المصنع
Event Traffic	حركة الحدث
Extraneous Events	الأحداث الدخيلة
Fault management	إدارة الأعطال
Filter	مصفي أو مرشح
Inconclusive	عدم حسم
Irrelevant Event	حدث غير مفيد
Logical Alarms	الإنذارات المنطقية
Local Administration	الإدارة المحلية
Loop Back	عروة رجوع
Overflow	طفح

المصطلح بالإنجليزية	معناه بالعربية
Pager	جهاز استدعاء
Polling	التصويت
Physical Alarms	الإنذارات الفعلية
Pings	أمر بروتوكول الصدى
Trap	تصيد
Valid Events	الأحداث الصالحة
Virtual Circuit	دائرة وهمية
SMTP(Simple Mail Transport Protocol	بروتوكول نقل البريد البسيط
Reliability	اعتمادية
Redundant Alarms	الإنذارات الزائدة (الإنذارات المتكررة)

المراجع

[1] Douglas Comer, Automated Network Management Systems, Pearson, ISBN13: 9780132393089, Jan 2007.

[2] Douglas E. Comer, Automated Network Management Systems: Current and Future Capabilities, Cisco Systems San Jose, ISBN-10: 0-13-239308-5, Publisher: Prentice Hall, 2006.

[3] Allan Leinwand, Karen Fang, Network Management: A Practical Perspective, 2nd Edition, Addison Wesley Professional, ISBN-10: 0-201-60999, 1996.

[4] Alexabnder Clemm, Network Management Fundamentals: A Guide to Understanding How Network Management Technology Really Works, Cisco Press Fundamental Series, 2006.

[5] Paul L. Della Maggiora, Christopher E. Elliott, Robert L. Pavone Jr., Kent J. Phelps, James M. Thompson, Performance and Fault Management, Cisco Press, ISBN-10: 1-57870-180-5, 2000.

[6] M. Natu and A.S. Sethi, ``Active Probing Approach for Fault Localization in Computer Networks" Proc. End-to-End Monitoring Workshop, Vancouver, B.C., Canada (April 2006).

[7] M. Steinder and A.S. Sethi, ``A Survey of Fault Localization Techniques in Computer Networks" Science of Computer Programming, Special Edition on Topics in System Administration Vol. 53, 2 (Nov. 2004).

[8] M. Steinder and A.S. Sethi, ``Distributed Fault Localization in Hierarchically Routed Networks." In Management Technologies for E-Commerce and E-Business Applications} (M. Feridun, P. Kropf, and G. Babin (eds.))

Lecture Notes in Computer Science Vol. LNCS-2506, (2002), pp. 195-207, Berlin: Springer-Verlag.

[9] M. Steinder and A.S. Sethi, ``The Present and Future of Event Correlation: A Need for End-to-end Service Fault Localization," Proc. SCI-2001, 5th World Multi-conference on Systems, Cybernetics, and Informatics, Orlando, FL (July 2001), pp. 124-129.

[10] Fault management (internet sites):-

www.micromuse.com/downloads/pdf_lit/istt_case_study.pdf

www3.ca.com/Solutions/SubSolution.aspx

www.networkgeneral.com/Consulting_NER.aspx

www.networkdictionary.com/networking/nfm.php

www.tavve.com/EW_White_Paper.pdf

www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm


الوحدةالرابعة
إدارة التهيئة

محتويات الوحدة

مقدمة

تمهيد

عزيزي الدارس، مرحبا بك إلى هذه الوحدة التي تتناول إدارة التهيئة بالحصول على البيانات من الشبكة، واستخدام هذه البيانات في إدارة وتنصيب كل أجهزة الشبكة. سنتناول تجميع معلومات عن التهيئة الحالية للشبكة، واستخدام هذه البيانات في عملية تعديل تهيئة أجهزة الشبكة، وتخزين البيانات، والاحتفاظ بقائمة حديثة، وتدوين تقارير مبنية على البيانات. في هذه الوحدة الدراسية سوف نشرح أيضاً فوائد إدارة التهيئة بالنسبة لمهندس الشبكة. ونناقش الخطوات اللازمة لإدارة عملية التهيئة. ونشرح ثلاثة مستويات من أدوات إدارة التهيئة. كما نعرض التقارير المختلفة التي يمكن الحصول عليها من بيانات التهيئة.

أهلا بك مرة أخرى إلى هذه الوحدة، وعسى أن تنتفع بها، وأن تفيد منها، وأن تساعدنا في نقدها وتطويرها .

أهداف الوحدة

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

- تعدد فوائد إدارة التهيئة في نظام إدارة الشبكة.
- تعرف كيفية تحقيق عملية إدارة التهيئة في نظام إدارة الشبكة.
- تفهم طرق تجميع بيانات تهيئة أجهزة الشبكة يدويا وآليا.
- تقارن بين طرق التجميع اليدوي والآلي لبيانات تهيئة أجهزة الشبكة.
- تعرف وظيفة الرسام الآلي لإنشاء خريطة الشبكة ودورها في عملية التهيئة.
- تفرق بين طريقة تخزين ملفات التهيئة بشفرة أسكي ونظام قواعد البيانات.
- ترسم خريطة التدفق التي تحدد الأداء الوظيفي للأداة المركبة لإدارة التهيئة.
- تفهم كيفية تقييم تهيئة أجهزة الشبكة بواسطة أداة التهيئة المتقدمة.
- تحدد بعض أعطال الشبكة نتيجة وجود سوء تهيئة لبعض أجهزتها.
- تحسن من أداء الشبكة بواسطة ضبط معاملات تهيئة الشبكة بشكل مثالي.

1. فوائد إدارة التهيئة

عزيزي الدارس، لإدارة التهيئة وظائف متعددة منها ما يلي:

1- تعزز إدارة التهيئة قدرة مهندس الشبكة على التحكم في تهيئة أجهزة الشبكة، وذلك بأن تمكنه من الوصول السريع إلى بيانات التهيئة الحيوية لهذه الأجهزة.

2- تستطيع إدارة التهيئة، في النظم الأكثر تعقيدا، تمكين مهندس الشبكة من عمل مقارنة بين تهيئة التشغيل Running Configuration وبين التهيئة المخزنة في النظام، وإجراء عمليات التغيير اللازمة بسهولة، عند الاحتياج.

ونوضح في الأمثلة التالية فوائد إدارة التهيئة:

- **مثال1: المساعدة في تهيئة برامج تشغيل أجهزة الشبكة:**

على سبيل المثال، يعتبر التنصيب الحالي لكل جهاز من أجهزة الشبكة، هو أحد مظاهر بيان التهيئة. دعنا نفترض أنه توجد وحدات بينية إضافية لجهاز معين ونريد أن نعرف أولاً، عدد الوحدات البينية الفعلية الموجودة في الجهاز، وكذلك عناوين الشبكة المخصصة لهذه الوحدات، وذلك للمساعدة في تهيئة البرامج الموجودة بالجهاز. بمعاونة إدارة التهيئة في هذا المكان، نستطيع تحديد مكان هذه المعلومات بسهولة، وذلك لأننا نعرف المكان الذي سوف تخزن فيه هذه المعلومات.

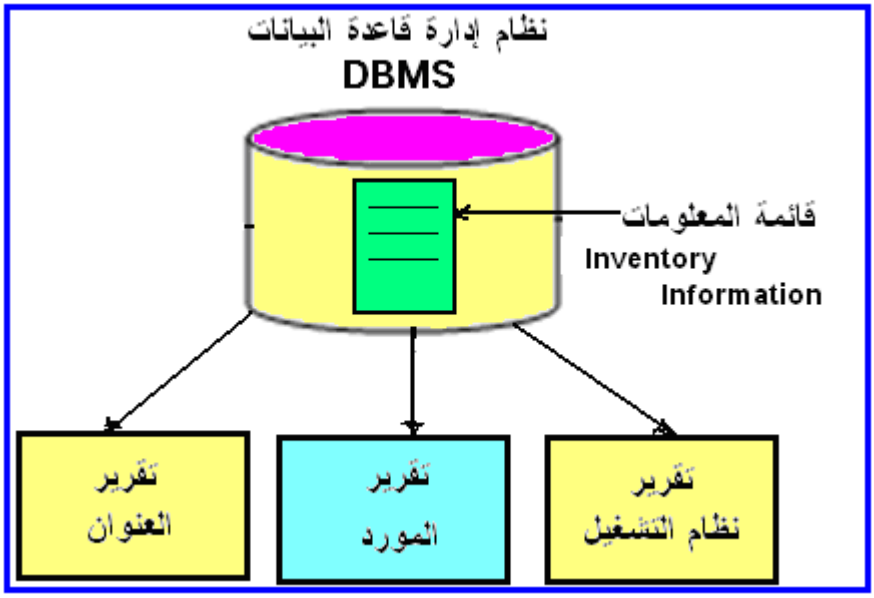
- **مثال2: المعاونة في إجراء تعديلات التهيئة لأجهزة الشبكة:**

في بعض الحالات ربما يحتاج الجهاز إلى إجراء تعديلات. على سبيل المثال، نفترض أن الوحدة البينية لجهاز معين يسبب أخطاء في قطاع من الشبكة المحلية. باستخدام أداة إدارة التهيئة، يستطيع مهندس الشبكة عن بعد، إعادة تهيئة هذا الجهاز لإخماد Deactivate هذه الوحدة البينية. بعد ذلك يتم فحص تهيئة الوحدة البينية لإيجاد المعاملات Parameters غير الصحيحة والتي تسبب الأخطاء. إن أداة إدارة التهيئة

تمكننا من تغيير المعاملات غير الصحيحة ووضع القيم المناسبة، وبعد ذلك يتم إعادة تنشيط الوحدة البينية.

- **مثال3: توفير قائمة بيانات حديثة لمكونات الشبكة:**

إن أداة إدارة التهيئة تساعد أيضا مهندس الشبكة، وذلك بواسطة توفير قائمة بيانات حديثة لمكونات الشبكة. وهذه القائمة تمكن مهندس الشبكة على سبيل المثال من تحديد عدد نوع معين من الأجهزة موجود بالشبكة، أو المعاونة في إنشاء تقرير عن كل إصدارات نظم التشغيل المستخدمة في الأجهزة المتصلة بالشبكة، كما هو موضح في شكل4.1.



شكل4.1 استخدام قائمة بيانات الشبكة في إنشاء تقارير لمساعدة مهندس الشبكة.

- **مثال4: تحديد قطع غيار الشبكة:**

إن التسهيل الذي تقدمه قائمة بيانات إدارة التهيئة لا نحتاج أن يكون محدوداً فقط لاقتفاء أثر وتتبع أجهزة الشبكة. بل يمكن استخدامه أيضا لتسجيل أشياء أخرى مثل: معلومات الاتصال بالمورد ، عدد دوائر الخطوط المؤجرة Leased Lines، أو عدد قطع غيار

الشبكة، وبالتحديد الأشياء التي لا تستطيع قائمة البيانات الثانوية أن تغالي في توكيدها. وهذه المعلومات تفيد عندما نريد الاتصال بالمورد من أجل توريد قطع غيار أجهزة للشبكة، أو لشراء برمجيات عن إصدارات متطورة من برمجيات تشغيل الشبكة. وأن معرفة عدد دوائر الخطوط المؤجرة يفيد في إمكانية إجراء زيادتها أو نقصانها تبعا لحالة الشبكة.

- **مثال5: سرية قائمة بيانات التهيئة للأجهزة الشبكة:**

ينبغي أن تكون قائمة بيانات الشبكة سرية. فإذا وقعت هذه البيانات في أيدي شخص ماكر Malicious، فإن هذا النوع من البيانات يمكن أن يؤذى الشبكة في عدة نواحي. على سبيل المثال، نفترض أن أحداً ما علم بوجود أخطاء في أحد برامج تشغيل الشبكة، والتي يمكنها أن تجعل بعض أجهزة الشبكة لا تعمل بشكل صحيح. عندما يتم الحصول على قائمة بيانات الشبكة، ومعرفة عدد هذه الأجهزة في الشبكة، يستطيع هذا الشخص الماكر أن يسبب أعطالاً ضخمة بالشبكة، وذلك بأن يدفع وينشر هذه الأخطاء في جميع أجهزة الشبكة.

2. تحقيق عملية إدارة التهيئة

تتكون إدارة التهيئة من الخطوات التالية:

1- تجميع المعلومات عن الوسط المحيط الحالي بالشبكة: إن الفشل في هذه الخطوة يمكن أن يؤدي إلى ضياع وقت مهندس الشبكة في حصر مشاكل الشبكة التي سببتها أخطاء تهيئة بسيطة. ويمكن تجميع هذه المعلومات، إما يدويا بواسطة مهندس الشبكة أو بواسطة نظام إدارة الشبكة.

2- استخدام هذه البيانات لتعديل تهيئة أجهزة الشبكة. بما أن الوسط المحيط بشبكة البيانات يتغير باستمرار، فإن قابلية تعديل التهيئة الحالية في الزمن الحقيقي يكون ضروريا. وتتم عملية تعديل التهيئة إما آليا أو يدويا وذلك حسب طريقة التجميع إن كانت آلية أو يدوية.

3- تخزين البيانات، والاحتفاظ بقائمة بيانات حديثة لكل مكونات الشبكة، وتوليد تقارير مختلفة.

1.2 تجميع البيانات يدويا

يتم غالبا الحصول على المعلومات من الشبكة بمجهود يدوي. حيث يمكن لمهندس الشبكة الدخول إلى الشبكة عن بعد ، للوصول إلى معرفة الأجهزة المتصلة بالشبكة، ثم يتم بعد ذلك تسجيل الرقم التسلسلي للأجهزة، والعنوان المخصص للجهاز في ملف مفكرة، أو ملف مكتوب بشفرة أسكي، أو ملف جدول قاعدة بيانات. وعلى الرغم من أن عملية التسجيل اليدوي للمعلومات سوف يؤدي إلى الحصول على النتائج المطلوبة، لكن استخدام هذه الطريقة للاحتفاظ بسجلات حديثة عن كل تغيير يحدث في الوسط المحيط بشبكة البيانات، يمكن أن يكون صعبا، وعرضه للخطأ، ويستغرق وقتا، ويصبح عملية رتيبة.

أسئلة تقويم ذاتي

أكمل ما يأتي:

تتميز إدارة التهيئة بعدة مميزات منها ما يلي(أكمل):-

أ- تعزيز قدرة تحكم مهندس الشبكة على تهيئة أجهزة الشبكة.

ب- .....

ج- .....

2) اذكر بعض عيوب طريقة التجميع اليدوي لبيانات في نظام إدارة تهيئة أجهزة الشبكة؟ وكيف يتم التغلب على هذه العيوب باستخدام الطريقة الآلية.

مثال1: تتبع جدول العناوين المخصصة لشبكة:

نفترض أننا نحتاج تتبع جدول العناوين المخصصة لشبكة بها 6000 مركز اتصال. وأن هذه المعلومات ربما تم تصنيفها لتسهيل عملية استرجاع العنوان بسهولة. فمع إضافة كل جهاز جديد إلى الشبكة، سوف نحتاج إضافة هذه البيانات إلى الجدول، ثم بعد ذلك يتم إعادة عملية تصنيف البيانات مرة أخرى. من هذا المثال يتضح أن عملية التجميع اليدوي للبيانات يمكن أن تستغرق وقتا وجهدا كبيرين. بالإضافة إلى أن تتبع عمليات التهيئة يدويا، يعمل بشكل جيد فقط، إذا استطعنا إيجاد كل أجهزة الشبكة. لكن النظم الجديدة التي يتم إضافتها إلى الشبكة من قبل مستخدمين غير معلومين لإدارة الشبكة، يصعب اكتشافها، خاصة إذا كانت شبكة البيانات منتشرة جغرافيا وتغطي مساحة واسعة. حتى بالنسبة للنظم الجديدة التي يتم إضافتها للشبكة والتي نعلم عنها، فإن الحصول على معلومات التهيئة يتطلب من مهندس الشبكة السفر والذهاب إلى المكان الجغرافي الذي تتواجد به هذه النظم الجديدة، أو الاستعانة بأحد المساعدين المحليين لتجميع هذه البيانات.

مثال2: استخدام وسائل آلية:

يمكن تجنب مخاطر التجميع اليدوي للبيانات وذلك باستخدام وسائل آلية. على سبيل المثال، يمكن توظيف بروتوكول إدارة الشبكة، للحصول على بيانات عن أجهزة الشبكة بانتظام، وتسجيل هذه البيانات آليا في مخزن داخل الذاكرة.

2.2 الاستكشاف الآلي Auto-discovery

يوجد وسيلة أخرى يمكن استخدامها وهي الاستكشاف الآلي Auto-discovery، والتي تمكننا من الحصول على قائمة البيانات الحالية لجميع أجهزة الشبكة. ويوجد طريقتان شائعتان تستخدمان لتنفيذ عملية الاستكشاف الآلي:

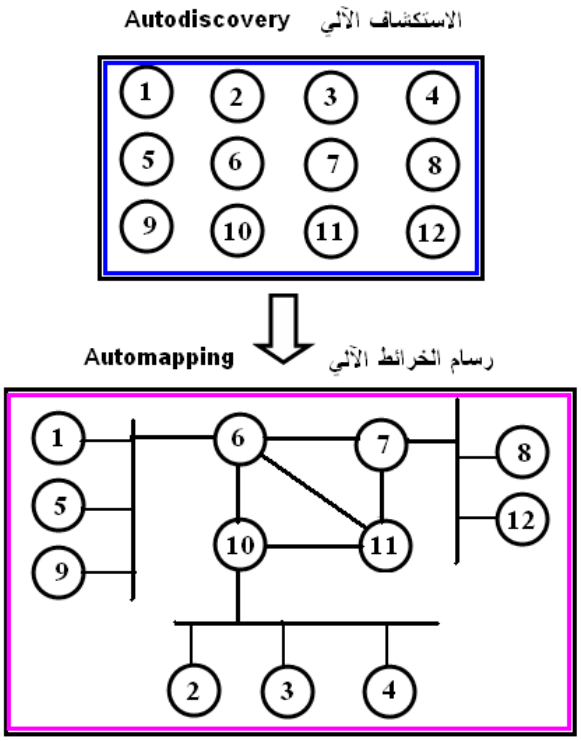
الطريقة الأولى: هي أن يتم إرسال رسالة استفسار Query، وذلك باستخدام أمر الصدى "بنج" ICMP Echo(ping) ، إلى كل عنوان محتمل في الشبكة. عندما يقوم الجهاز بالإجابة على الاستفسار، تتم عملية إجراء استفسار تفصيلي أخرى عن المعلومات

باستخدام بروتوكول إدارة الشبكة. وتتميز هذه الطريقة بأنها تكتشف كل جهاز يعمل في الشبكة، ولكن من عيوبها أنها تقوم بإرسال استفسارات للأجهزة غير موجودة بالشبكة أيضا، وهذا يؤدي إلى ضياع جزء من سعة نطاق الشبكة. وهذه الطريقة أيضا قد تستغرق وقتا لاكتشاف جميع الأجهزة، لأن الاستفسارات التي يتم إرسالها إلى الأجهزة غير الموجودة بالشبكة، يتم انتظارها حيث تستغرق فترة زمنية كي تقوم بالاستجابة، بعد ذلك يتم إعادة محاولة الاتصال بها مرة أخرى بعد مرور فترة زمنية محددة تسمى Timeout.

الطريقة الثانية للاستكشاف الآلي: هي إيجاد جهاز واحد في الشبكة، وإجراء الاستفسار عنه باستخدام بروتوكول إدارة الشبكة، لاكتشاف كل الأجهزة التي قامت بالاتصال به حديثا. ويتم إجراء هذه العملية على كل أجهزة الشبكة، وتتم عملية اكتشاف الأجهزة بنظام البحث العرضي Breadth-first Search لكل أجهزة الشبكة. تستطيع الأداة استخدام بروتوكول الشبكة لإيجاد كل المعلومات ذات العلاقة بهذه الأجهزة. تتميز هذه الآلية، بأنها سريعة في الاستكشاف عن أجهزة شبكة البيانات، ولكن من عيوبها أنها تتطلب استخدام بروتوكول إدارة الشبكة، كما أنها تفشل في الاستكشاف عن الجهاز الذي لم يقم بالاتصال بأي أجهزة أخرى خلال الفترة الزمنية المخصصة لعملية الاستفسار.

3.2 رسام الخرائط الآلي Automapping

تستطيع طريقة الاستكشاف الآلي إنشاء خريطة رسومية لشبكة البيانات الحالية، وذلك باستخدام عملية يطلق عليها اسم " رسام الخرائط الآلي Auto-mapping "، كما هو مبين في شكل4.2 . وعلى الرغم من أننا قد نحتاج إلى مراجعة وتعديل الخريطة التي يتم رسمها بواسطة رسام الخرائط الآلي، وذلك لتمثيل المنطقة الجغرافية للشبكة، وهذه التعديلات للخريطة تكون مفيدة من أجل توضيح التهيئة الإجمالية للشبكة.



شكل4.2 الاستخدام الاستكشافي الآلي لإيجاد أجهزة الشبكة،
واستخدام رسام الخرائط الآلي لإنشاء خريطة للشبكة.

إن قيمة سعة النطاق التي تحتاجها عملية التهيئة الآلية، سوف تؤثر بالطبع على اتخاذنا قرار الاستعانة بهذه الطريقة، على الرغم من أن فوائد عملية الأتمتة سوف تغطي بسهولة هذه التكاليف. إن معدل تكرار عملية التصويت لأجهزة الشبكة، سوف يؤثر على قيمة سعة النطاق المستهلكة. وبالتالي، فإننا سوف نحتاج إلى تحديد عدد مرات التكرار التي يتم فيها إجراء تجميع المعلومات. لأن تهيئة الشبكة تتغير عادة بطريقة غير منتظمة نسبيا، وأن عملية الانتخاب ربما تكون أيضا غير منتظمة، فيمكن أن تتم مرة واحدة في الأسبوع، وبذلك يتم الاحتفاظ بقيمة منخفضة لسعة النطاق المستهلكة.

3. تعديل بيانات تهيئة الشبكة

عندما يتم الحصول على معلومات إدارة الشبكة، سوف نحتاج إلى إجراء عملية تحديث. نفترض شبكة بيانات بها 6000 مركز اتصال، التي تم مناقشتها سابقا. فإذا احتاج 1% فقط من مراكز الاتصال تخصيص عنوان، أو تغير كل أسبوع، فسوف نحتاج إلى إجراء 60 تعديل في الأسبوع. وأكثر من ذلك، فإن عناوين الشبكة تكون واحداً من العديد من بيانات تهيئة الشبكة. إن أي جهاز منفرد سوف يتطلب الكثير من التعديلات التي سوف تتم في المعاملات الخاصة به والتي ينبغي تتبعها أثناء عملية التهيئة.

من الواضح أن عملية تجميع البيانات وتعديلها يدويا ، تكون طريقة غير فعالة، إذا لم يقوم مهندس الشبكة الذي أدى عمليات التهيئة يدويا بتسجيل الخطوات، وأن سجل تغيرات التهيئة ربما لم يتم حفظه. يمكن أن يؤدي ذلك إلى حدوث إرباك، خاصة عندما يقم مهندس آخر للشبكة بفحص الجهاز الذي تم تغيير تهيئته ولم يجد سجل حفظ التهيئة السابق. على النقيض من ذلك، إذا سمحت إدارة التهيئة في نظام إدارة الشبكة بإجراء تغيرات تهيئة الجهاز فإن هذه التغيرات يمكن تسجيلها قبل أن يتم إرسالها إلى الجهاز. كميزة إضافية، فإن نظام إدارة الشبكة ربما يكون قادرا على التحقق من أن تغييرات التهيئة كانت مناسبة للجهاز، ويقوم بتنبيه مهندس الشبكة قبل أن يقوم بإجراء تهيئة غير مناسبة للجهاز بدون قصد.

4.تخزين معلومات تهيئة الشبكة

ينبغي على إدارة التهيئة توفير وسيلة لتخزين المعلومات. إن نظام الإدارة الفعال هو الذي يستطيع تخزين كافة تهيئة شبكة البيانات في مكان مركزي. وهذا يجعل بيانات التهيئة متاحة بشكل سريع وفعال ، يمكن الوصول إليها بسهولة بواسطة مهندس الشبكة. يمكن أن يكون مكان التخزين المركزي لبيانات التهيئة عبارة عن ملف مفكرة، أو ملف مكتوب بشفرة أسكي ، أو جدول في مركز تحكم الشبكة. وبغض النظر عن الطريقة

المستخدمة، فإن وجود هذه البيانات بشكل متاح ومنسق سوف يكون ذو فائدة كبيرة لمهندس الشبكة.

1.4 ملفات شفرة أسكي

إن استخدام ملف مكتوب بشفرة أسكي هو أحد وسائط التخزين الشائعة، وله ثلاثة **مميزات هي:**

- أن شفرة أسكي سهلة القراءة.
- يسهل الوصول إليها من أماكن بعيدة.
- ولها هيكل ملف يكون عادة سهل الإدارة والفهم.

ولهذا، فإن معظم البرامج التطبيقية (بغض النظر عن العتاد المستخدم) تستطيع قراءة ملفات أسكي.

من عيوب استخدام شفرة أسكي:

- أن حروف شفرة أسكي تستخدم ذاكرة تشغل حيز كبير في نظام الكمبيوتر.
- وأن كمية كبيرة من البيانات المخزنة بهذه الشفرة يمكن أن يستهلك مساحة ضخمة من حيز قرص التخزين.
- علاوة على أن هياكل ملفات أسكي غير المعقدة يمكن أن يؤدي إلى بطء عملية الوصول للبيانات، أثناء عملية البحث.
- ولكن العيب الأكثر أهمية في ملفات أسكي هو أنها لا تستطيع إنشاء علاقات بين البيانات المركبة.

أسئلة تقويم ذاتي

1) أذكر طريقتين للاستكشاف الآلي لبيانات تهيئة أجهزة الشبكة تستخدمان في إدارة التهيئة؟ وقارن بينهما من حيث الوظيفة، المميزات، والعيوب.
2) ما وظيفة استخدام الرسام الآلي في إدارة التهيئة؟ وضح إجابتك بمثال.
3) اذكر مميزات وعيوب طريقة تخزين بيانات تهيئة أجهزة الشبكة باستخدام ملفات مكتوبة بشفرة أسكي.

2.4 استخدام نظام إدارة قواعد البيانات

عزيزي الدارس، إن الاختيار البديل هو استخدام نظام إدارة قواعد البيانات DBMS(Data Base Management System) ، حيث إنه نظام أكثر فاعلية. إن نظام إدارة قاعدة البيانات توفر مميزات عديدة أكثر مما توفره ملفات أسكي للبيانات المخزنة. **وتشمل بعض هذه المميزات ما يلي:**

- تخزين البيانات بكفاءة، حيث يمكن تخزين كمية ضخمة منها على حاسب منفرد.
- تخزين البيانات حسب الفورمات الخاصة بها، وهذا يسرع من عملية البحث عن بيانات معينة.
- تصنيف البيانات آليا بأشكال متعددة.
- يمكنها آليا استرجاع البيانات المفقودة.
- تمكين المستخدم من ربط أنواع متعددة من البيانات مع بعضها.

ربما تكون الميزة الأساسية لاستخدام قاعدة البيانات هو أنها تمكن المستخدم من ربط أنواع متعددة من البيانات مع بعضها.

مثال: نظام قاعدة بيانات علاقية لإيجاد علاقات بين بيانات الشبكة:

يبين جدول4.1 ،على سبيل المثال، بيانات التهيئة لجهاز معين يقوم بتوجيه مهندس الشبكة إلى مورد الجهاز. وأن بيانات المورد تشير بدورها إلى شخص معين مسئول يتم الاتصال به في المؤسسة الموردة للجهاز عند حدوث مشكلة في الجهاز.

إن تدفق المعلومات ذات العلاقة ليس قاصرا على أجهزة الشبكة، إذ إنه يمكن أن يشمل جميع المعلومات الضرورية لإدارة التهيئة. وبذلك فإن استخدام قاعدة البيانات في التخزين، يمكن أن يساعد مهندس الشبكة في جميع النواحي المتعلقة بعملية إدارة التهيئة.

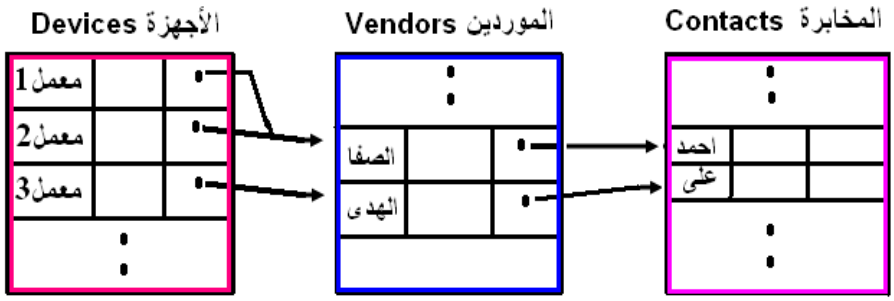
ونلاحظ على الرغم من ذلك **أن نظام إدارة قاعدة البيانات لها بعض العيوب ومنها:**

1- تستخدم غالبا مجموعة مركبة من دوال الإدارة صعبة التحليل.

2- تستخدم لغة خاصة بها، قد لا يعرفها مهندس الشبكة.

3- تحتاج نظام تشغيل وعتاد خاص.

جدول4.1 نظام قاعدة بيانات علائقية لإيجاد علاقات بين بيانات الشبكة.



يوجد صعوبة في عملية نقل ملفات البيانات المخزنة بنظام قاعدة البيانات إلى نظام آخر. ولكن معظم موردي نظم قواعد البيانات قد قاموا بحل هذه المشكلة بواسطة السماح بوضع البيانات المخزنة في قاعدة البيانات على شكل شفرة أسكي، وبذلك يمكن بسهولة نقلها واستخدامها. وبذلك فإن المميزات التي توفرها نظم قواعد البيانات تعوض بشكل جيد عن عيوبها.

5. إدارة التهيئة في نظام إدارة الشبكة

عزيزي الدارس، إن أدوات إدارة التهيئة يمكنها زيادة إنتاجية مهندس الشبكة بواسطة تجميع وتحديث بيانات أجهزة الشبكة آليا، وتوفير مخزن مركزي لبيانات التهيئة، وتمكين إجراء التعديلات في بيانات الشبكة، وتوفير قائمة بيانات، وتوليد التقارير. إن الأداة التي تستطيع تقديم هذه التسهيلات سوف يحدد مدى سهولة وصعوبة هذه الأداة، وهذا ما سوف نشرحه على التتابع في الفقرات التالية.

1.5 الأداة البسيطة لإدارة التهيئة

إن أداة إدارة التهيئة البسيطة، ينبغي على الأقل، أن توفر مخزناً مركزياً لمعلومات جميع شبكة البيانات، وتشمل هذه المعلومات: تخصيص عناوين الشبكة، والأرقام المسلسلة للأجهزة، والأماكن الفعلية للأجهزة، وبيانات الأجهزة الأخرى ذات الصلة. كما ينبغي وجود تقنية الاستكشاف الآلي لإيجاد كل الأجهزة المتصلة بشبكة البيانات، وأن هذه الأداة ينبغي أن تقوم بالاستفسار عن الأجهزة لإيجاد المعلومات ذات الصلة، لتغطية المعلومات التي يتم الاحتياج إليها آليا بقدر الإمكان. إن تحقيق هذه الوظائف يتطلب أن تحقق الأداة عملية الاستكشاف الآلي لإيجاد الأجهزة المتصلة بشبكة البيانات لكل جهاز يتم إيجاده. تقوم الأداة بعد ذلك بمحاولة الاتصال بواسطة استخدام بروتوكول إدارة الشبكة.

إن طلب البيانات آليا يكون مهما بالتحديد لأنه يؤكد أن المعلومات التي يتم الحصول عليها هي المعلومات الحالية. وبذلك فإن مهندس الشبكة سوف يشعر بالارتياح عند إجراء عملية التصويت على الأجهزة في حالة الضرورة فقط، وفي أثناء الفترة التي يكون فيها استعمال الشبكة قليلاً. إن معدل تكرار عملية الانتخاب يكون أحد معاملات التهيئة. من الناحية المثالية، فإن الأداة سوف تستخدم بروتوكول إدارة الشبكة لإجراء عملية الانتخاب للأجهزة، والحصول على البيانات الخاصة بتهيئتها.

على الرغم من أن الأداة البسيطة تحقق عملية الاستكشاف الآلي، فإنه ليس من الضروري أن تحقق عملية رسم الخرائط آليا. إذا كان الجهاز يدعم بروتوكول إدارة الشبكة، فإن الأداة تستطيع بعد ذلك الاستفسار عن الجهاز وتحديد اسم المورد، للحصول على معلومات محددة تكون ذات صلة بالجهاز.

في حالات كثيرة، فإن الأداة البسيطة قد تقوم بالاستكشاف عن الجهاز ولكنها لا تستطيع الحصول على معلومات منه، بسبب أن الجهاز لا يدعم بروتوكول إدارة الشبكة، أو بسبب محاذير أمنية. في مثل هذه الحالات فإنه ينبغي اتخاذ التدابير اللازمة كي يتم إدخال كل البيانات المطلوبة إلى الأداة يدويا. ولتسهيل هذه العملية، فإن الأداة تستطيع إظهار طلب المعلومات التي تحتاجها. إن الأداة البسيطة قد لا توجد بشكلها البدائي في برامج إدارة الشبكات الحالية، فهذه البرامج يكون لها القدرة على كشف الأجهزة في شبكة البيانات وتجميع المعلومات عنها. ولكن من الناحية العملية، فإن برامج إدارة الشبكة، تقوم فقط بتجميع المعلومات التي هي قي غاية الأهمية عن كل جهاز مثل: اسم الجهاز – عنوان الشبكة – أو عدد الوحدات البينية. بالرغم من أن هذه المعلومات تكون مفيدة، لكن هذا يضعف من وظائفها، ويعني هذا أنه يجب على مهندس الشبكة الاستفسار عن كل جهاز بطريقة يدوية وتجميع المعلومات الإضافية اللازمة لإدارة التهيئة.

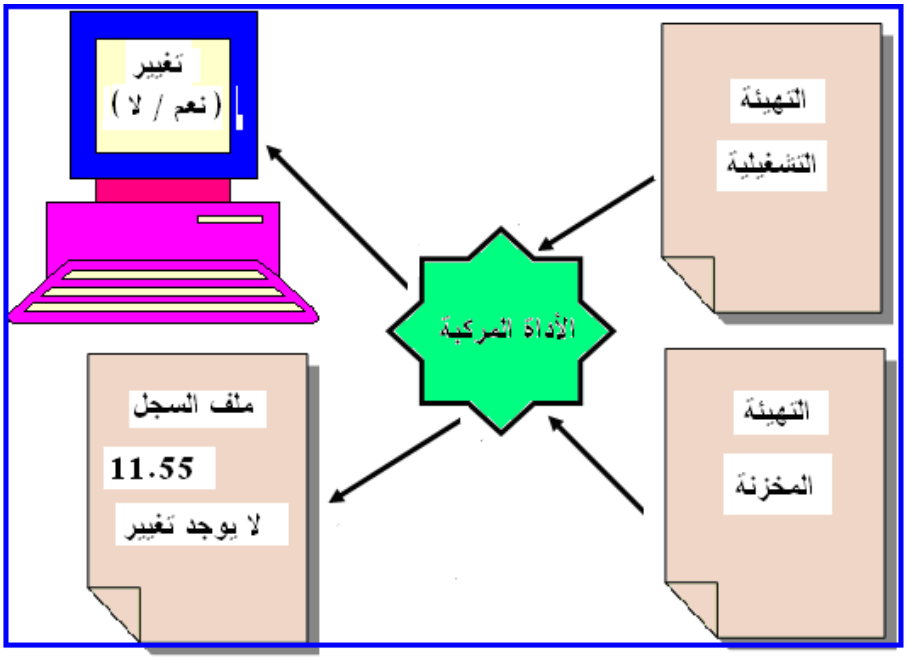
2.5 الأداة المركبة لإدارة التهيئة:

يمكن تطوير أداة مركبة تستطيع مقارنة تهيئة الأجهزة الحالية مع التهيئة المخزنة في قاعدة بيانات النظام. كما تستطيع أن تمكننا من رؤية التهيئة الجغرافية المنصبة، وإجراء عمليات تغيير التهيئة. وأخيرا مثل الأداة البسيطة، فإن إصدار الأداة المركبة يجب أن يوفر مخزناً مركزياً ووسيلة سهلة لاسترجاع البيانات.

وكما هو مبين في شكل4.3 ، فإن الأداة ينبغي أن تمكننا من **إجراء عملية المقارنة بين التهيئة التشغيلية مع التهيئة المخزنة** في قاعدة بيانات النظام. بالإضافة إلى أنه ينبغي للأداة إما أن تبدأ عملية تشغيل التهيئة التي تمكنا من تغيير التهيئة أو أن تحقق هي عملية تغيير التهيئة بنفسها آليا. أثناء إجراء حوار مشترك بين الأداة والجهاز، فإن الأداة

سوف تتحسس الجهاز لمعرفة التشغيل الحالي وبعد أن تتم عملية مقارنته مع التهيئة المخزنة. إذا وجد أي اختلافات، فإن الأداة تقوم بالسؤال عن ما إذا كنا نريد تغيير تهيئة الجهاز ليتوافق مع الإصدار المخزن. ربما يتم تشغيل هذه الخاصية آليا (دون إجراء تغيرات) على فترات، ويمكن إرسال بريد إلكتروني إلى مهندس الشبكة لإحاطته علما عن أي اختلافات تم إيجادها.

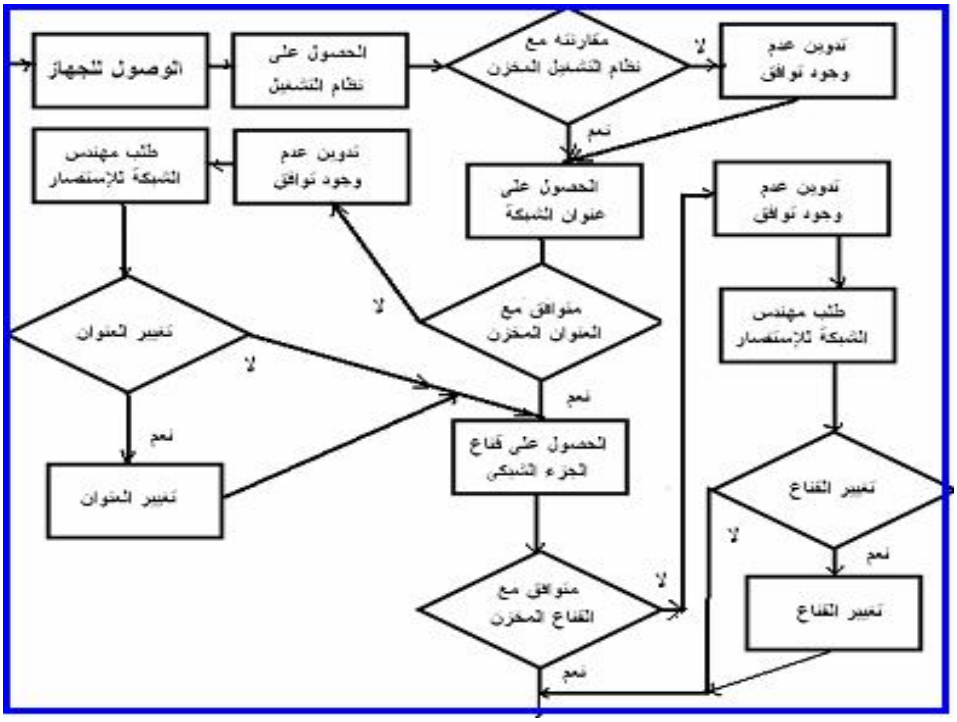
نلاحظ أن جميع تفاصيل التهيئة تكون على درجة متساوية من الأهمية. من أجل العمل الجيد في الوسط المحيط المتنوع في شبكة البيانات، ينبغي على الأداة أن تحتوي على **وسائل لتحديد نوع أخطاء التهيئة**، وأن تقوم بتوليد رسائل تحذير وتعرض إنذارات. على سبيل المثال: نفترض أن أحد اختيارات التهيئة في جهاز خادم الطرفيات هي تهيئة معدل إرسال المعلومة Bit Rate لوصلة القدوم، وهذه التهيئة تكون مفيدة في إجراء الاتصالات في نفس الوقت مع العديد من الأجهزة عند معدلات معلومة مختلف. نفترض أن معلومات التهيئة المخزنة، أوضحت أن كل خط غير متزامن خارج من جهاز خادم الطرفيات تم ضبطه عند معدل معلومة 9600 بايت /ثانية. ولكن عندما تقوم الأداة باستفسار الجهاز وجدت أن أحد الخطوط كان مضبوط عند 2400 بيت/ثانية، في هذه اللحظة ، فإن الأداة ربما تهتم بالتهيئة، ولكنها ببساطة سوف تصدر رسالة تحذير إلى ملف السجل Log File . وعلى النقيض، إذا وجدت الأداة خط آمن Secure Line متصل بخادم الطرفيات بدون وجود كلمة سر له، فسوف تقوم الأداة بالتنبيه عن هذه الحالة بواسطة عرض إنذار.



شكل4.3 استخدام الأداة المركبة لمقارنة التهيئة التشغيلية مع التهيئة المخزنة، وعرض الاختلافات على مهندس الشبكة للموافقة.

- **الأداء الوظيفي للأداة المركبة لإدارة التهيئة:**

توضح خريطة التدفق في شكل4.4 ، كيف تستطيع الأداة فحص نظام التشغيل الحالي، وعنوان الشبكة IP، وقناع جزء شبكي (يحدد عنوان الجهاز) لكل جهاز ومقارنته مع التهيئة المخزنة في الذاكرة.



شكل4.4 الأداء الوظيفي للأداة المركبة لإدارة التهيئة.

في هذه الحالة، إذا كان إصدار نظام التشغيل غير متوافق مع التهيئة المخزنة، فإن الأداة سوف تقوم ببساطة بتدوين الفروق في تقرير. ولكن عندما تجد الأداة عنوان الشبكة IP أو قناع جزء شبكي مختلف، فسوف تقوم بتدوين الاختلاف ثم تضبط التهيئة كي تتوافق مع القيم المخزنة.

إن الأداة المركبة ينبغي أن تعرض مناظر رسومية عن تهيئة الجهاز مع توصيلاته الحالية بالشبكة. يمكن إيجاد معلومات عن الخواص الطبيعية للجهاز بواسطة استخدام بروتوكول إدارة الشبكة. على الرغم من أن المشهد الرسومي لا ينبغي أن يعرض صورة شكل الجهاز فعليا، فإن هذه الصورة للجهاز تساعد غالبا مهندس الشبكة. حيث أن المظهر الفعلي للجهاز سوف يأخذ حيزا كبيرا من مساحة شاشة العرض في نظام إدارة الشبكة، وإن لم يوجد معلومات ذات صلة تغطي هذه المساحة، فإن العديد من مهندسي الشبكات تفضل وجود شكل توضيحي منطقي مختصر للجهاز. إن كلا من

المناظر المنطقية والفعلية للجهاز ينبغي أن تظهر التهيئة للجهاز، وكذلك الوحدات البينية المصاحبة للشبكة.

- **تهيئة الشبكة المحلية التخيلية**

ينبغي للأداة أن تسمح للمستخدم باختيار المعاملات الخاصة بالمناظر المنطقية أو الفعلية، وإيجاد حالتهم الحالية (وهذه غالبا إحدى خواص إدارة الأعطال) أو إجراء تغييرات التهيئة. ربما تشمل تغيرات التهيئة: حالة التشغيل وعناوين الشبكة ومعاملات أجهزة معينة . على سبيل المثال، فإن الجهاز الذي يوجد به وحدات بينية للشبكة، ربما يمكن اختيار طريقة التعبير الرسومية لهذه الوحدة البينية على شاشة العرض، وإيجاد الحالة الحالية للمنفذ الذي يتم اختياره. يمكن للمستخدم بعد ذلك، أن يقدر على أن يغير حالة أدارة المنفذ، إما بتنشيطه أو إخماده.

تقوم الشبكة المحلية التخيلية المنطقية بتوصيل أجهزة الشبكة المحلية عند أماكن فعلية مختلفة، لتكوين شبكة محلية منطقية واحدة، وهذا يسمح للشبكة المحلية التصورية بأن تمتد لأماكن متعددة. يكون التوصيل بين هذه الأماكن عبر خطوط ذات سرعات عالية مثل : نمط النقل غير المتزامن (Asynchronous Transfer Mode) ATM ، أو باستخدام وحدة مواجهة بيانات موزعة مصنوعة من الألياف البصرية FDDI (Fiber Distributed Data Interface) .

إن مبدأ الشبكات المحلية التخيلية ربما يغير كيفية التهيئة الرسومية للجهاز وتوصيلاته بالشبكة، وتقوم بتحديد ذلك الأداة المركبة. في شبكة محلية نوعية، فإن منفذاً منفرداً على الجهاز، يمكن توصيله بقطاع فعلي (مثل منفذ موجود على موجه أو قنطرة). تكون كل الأجهزة المتصلة بهذا القطاع، كل حسب دوره، يتم فهمها بأنها تخص نفس قطاع الشبكة. ربما يوجد حالة مماثلة لموجه متصل بمفتاح توصيل ايثرنيت Hub ، وبعد ذلك يتم توصيل جهاز Hub إلى كل الحاسبات المضيفة في القطاع.

يستطيع الموجه في الشبكة المحلية التخيلية أن يتصل بمفتاح ATM ، الذي يستطيع محاكاة قطاعات شبكة محلية فريدة ومتنوعة من خلال وحدة بينية منفردة. ينبغي على أداة التهيئة الرسومية أن تصف وتكشف هذه المعلومات إلى مهندس الشبكة، ربما بواسطة رسمها منافذ الوحدة البينية المنطقية منفصلة لكل ذاكرة محلية تصورية، وبعد ذلك يتم تجميعهم فعليا تحت عنوان منفرد. إن ألوان التشفير للمنافذ المختلفة في نفس الشبكة المحلية التصورية، تعتبر طريقة أخرى لكشف وتوضيح رسومات التهيئة الحالية للمفتاح. إن التشغيل المبدئي أو تغيير تهيئة الشبكة المحلية التصورية، ربما يتطلب أداة مركبة لتهيئة أجهزة متعددة في نفس الوقت.

إن بعض الأجهزة الموجودة في الشبكة المحلية االتخيلية: ربما تكون متصلة بجهاز التوصيل في مبنى واحد، بينما أجهزة أخرى نريدها أن تكون في نفس الشبكة المحلية التخيلي، ربما تكون متصلة بجهاز آخر في مبنى مختلف. إن الأداة المركبة تسمح لنا بأن نبدأ تهيئة الشبكة المحلية التخيلية، وذلك بأن يتم أولا تحديد المنافذ ذات الصلة بالمشاهد الفعلية أو المنطقية لكل الأجهزة المتأثرة. بعد ذلك يتم إخبار الأداة المركبة لكي تجعل كل منفذ من هذه المنافذ بأن ينتمي إلى نفس الشبكة المحلية التصورية (ربما بواسطة إسقاط المنافذ المعبر عنها بالرسومات إلى أيقونة الشبكة المحلية التصورية). تستطيع الأداة المركبة بعد ذلك تهيئة كلا من الأجهزة المتأثرة والمنافذ.

- **برمجيات الأداة المركبة:**

بعض تطبيقات إدارة الشبكات المتوفرة في الأسواق تقوم بتوفير معظم الوظائف التي تم وصفها بخصوص الأداة المركبة. ويوجد عند بعض الموردين أداة تستطيع فحص التهيئة الحالية للجهاز، ومقارنتها بالتهيئة المخزنة في قاعدة البيانات. أيضا يوجد بعض الموردين، لديهم بعض التطبيقات التي تظهر رسومات تهيئة الأجهزة الخاصة بهذه التطبيقات. تكون هذه المواصفات غالبا محددة من قبل الموردين، ويكون لها وحدات مواجهة بينية للمستخدم مختلفة حسب كل جهاز يتم توريده. ويعنى هذا أن مهندس

الشبكة يحتاج أن يتعلم كيفية تحقيق هذه الوظائف على أساس المعلومات المتوفرة من المورد، وكذلك باستخدام برنامج إدارة الشبكة المناسب.

3.5 الأداة المتقدمة لإدارة التهيئة

بينما الأداة المركبة كما تم شرحه في الفقرات السابقة تسمح بتغيير التهيئة التشغيلية للجهاز، فإن الأداة المتقدمة سوف تكون أكثر فاعلية إذا استخدمت نظام إدارة قاعدة البيانات في تخزين البيانات والاستفسارات ذات الصلة، و تسجيل قوائم معلومات إدارة الشبكة. وتكون قادرة على تقييم تهيئة الجهاز، كي تؤدي عملها في صورة مثالية.

إن قدرة الأداة على إيجاد علاقة بين مجموعات متعددة من البيانات يكون مهما في إدارة التهيئة. على سبيل المثال، إذا كان أحد المهندسين في الشبكة مسئولا عن 150 جهازاً، فإن إسناد اسم هذا المهندس إلى كل هذه الأجهزة مرة واحدة، سيكون أسهل من إدخال وتخزين نفس الاسم في كل مرة لكل جهاز على حدة.

أسئلة تقويم ذاتي

1) أذكر مميزات وعيوب طريقة تخزين بيانات تهيئة أجهزة الشبكة باستخدام نظام إدارة قواعد البيانات .
2) اذكر وظائف تهيئة الشبكة التي تحققها:
   أ- الأداة البسيطة لإدارة التهيئة.
   ب- الأداة المركبة لإدارة التهيئة.
   ج- الأداة المتقدمة لإدارة التهيئة.

استخدام لغة إس كيو إل سكول SQL:

إن نظام إدارة قاعدة البيانات DBMS (Data Base Management System) لا يسمح فقط بالمعالجة المركبة للبيانات ، ولكن يسمح أيضا بالاستفسارات المركبة. وهذه الاستفسارات تكتب عادة باستخدام لغة استفسار هيكلية SQL (Structured Query Language). نستطيع باستخدام لغة "سكول SQL " إيجاد معلومات معينة مخزنة في قاعدة البيانات. نفترض عل سبيل المثال: أننا نريد معرفة نوع إصدار برنامج *Software* موجود في جسر *Bridge* ايثرنيت يسبب وجود أخطاء في الشبكة. لتصليح هذا الوضع، سوف نحتاج إيجاد كل القناطر التي تستخدم هذا النوع من الإصدار البرمجي. نفترض أن كل الأجهزة المحتملة الموجودة بالشبكة تم تخزينها في ملف جدول يسمى "أجهزة". لإيجاد كل الجسور ايثرنيت التي تتأثر بهذا النوع من الإصدار البرمجي فإننا يمكن أن نستخدم أمر لغة "سكول SQL " التالي:

```
SELECT *FROM "DEVICE" WHERE TYPE =BRIDGE AND
  SOFTWARE =A
```

سوف يبين الخرج الناتج عند تنفيذ هذا الأمر، كل أجهزة الجسور في الجدول المسمي "أجهزة"، والذي يعمل بنوع الإصدار البرمجي A ، كما هو موضح في جدول4.2 .

جدول4.2 أحد أشكال الخرج الممكنة ناتج عن تنفيذ أمر استفسار بلغة SQL

المخابرة	المكان	الإصدار البرمجي	النوع	الرقم المسلسل	المورد	اسم الجهاز
احمد	الهندسة	A	قنطرة	01234	الصفا	ج1: مهندس المجموعة
علي	الإدارة	A	قنطرة	56789	الصفا	ج2: مدير الفرع
حسن	التسويق	A	قنطرة	10112	الهدى	ج3: قسم التسويق
...	...	...	...	...	...	...

1- الرقم التسلسلي للجهاز	2- ماركة الجهاز وسنة الصنع
3- نظام التشغيل	4- سعة الذاكرة RAM
5- عناوين الشبكة	6- سعة الوحدة البينية.

تستطيع لغة "سكول SQL " أيضا توليد تقارير مثل تقارير قائمة البيانات، وهذه التقارير قد تحتوي على البيانات التالية:

```
SELECT device, sn FROM "أجهزة", vendors WHERE
vendors. Name = "الصفا" AND devices. months <<= 12
```

مثال: لتوليد تقرير يبين الأجهزة Devices وأرقامها التسلسلية، المستوردة من شركة معينة تسمى "الصفا"، والتي تم إضافتها إلى الشبكة خلال العام الماضي ومازالت في فترة الضمان. يمكن أن نستخدم لغة "سكول SQL " وكتابة أمر الاستفسار التالي:
وبعد تنفيذ هذا الأمر سوف نحصل على التقرير المبين في جدول4.3. والذي يوضح قائمة الأجهزة المستوردة من شركة "الصفا" ومازالت في فترة الضمان.
جدول4.3 قائمة بأسماء أجهزة شركة "الصفا" المتصلة بالشبكة، ولازالت في فترة الضمان السنوي.

الرقم المسلسل	اسم الجهاز
12345	معمل1
67890	معمل2
11123	معمل3
14156	معمل4

- **توليد التقارير:**

يمكن استخدام نظام إدارة قاعدة البيانات لتوليد تقارير أخرى، مثل قائمة الأشخاص الذين يمكن الاتصال بهم في الشركات الموردة وكذلك الحصول على بيانات الدوائر المؤجرة

Leased Circuit . وقد تشمل قائمة البيانات الخاصة بالمورد على: الاسم، والعنوان ورقم الهاتف. وقد تشمل قائمة بيانات الدوائر المؤجرة على: رقم الدائرة والسرعة اسم المورد وعدد نقاط النهايات بالشبكة والمدة المسموحة والمدة التي سوف تتوقف عندها الخدمة.

على الرغم من إمكانية استخدام لغة "سكول SQL " للاستفسار عن أجزاء معينة في قاعدة البيانات، فإنه ليس من الضروري على مهندس الشبكة أن يتعلم لغة "سكول SQL ". لأنه ينبغي على الأداة المتقدمة أن توفر وحدة مواجهة بينية لمساعدة مهندس الشبكة في إيجاد البيانات الحرجة المخزنة داخل قاعدة البيانات دون الحاجة للاستخدام لغة "سكول SQL ". إن الأداة المتقدمة ينبغي أن تسأل مهندس الشبكة عن البيانات المطلوب البحث عنها، وأن توفر له القوائم المناسبة التي يستطيع فهمها واستخدامها في البحث عن البيانات المطلوبة.

على سبيل المثال، لإيجاد جهاز معين عند العنوان AB لا يتطلب من مهندس الشبكة أن يعرف أن هذا العنوان مخزن في جدول قاعدة البيانات المسمى "عناوين". فبدلا من ذلك فإن مهندس الشبكة يستخدم الأداة المتقدمة ويخبرها أنه يريد إيجاد العنوان المسمى AB، وبعد ذلك تقوم الأداة المتقدمة بعرض كل المعلومات المعروفة عن هذا الجهاز، ويشمل ذلك المكان الفعلي الموجود به الجهاز، ومدير الجهاز، ووصف العتاد، ...الخ.

- **تقييم تهيئة أجهزة الشبكة:**

مما سبق يتضح أن الأداة المتقدمة، تستطيع تخزين المعلومات الضرورية، ومقارنتها بالتهيئة الحالية، وإجراء التعديلات عليها، وتتعامل مع الاستفسارات. والآن سوف نشرح الخاصية الإضافية الأخرى وهي المتعلقة بعملية تقييم بيانات التهيئة.

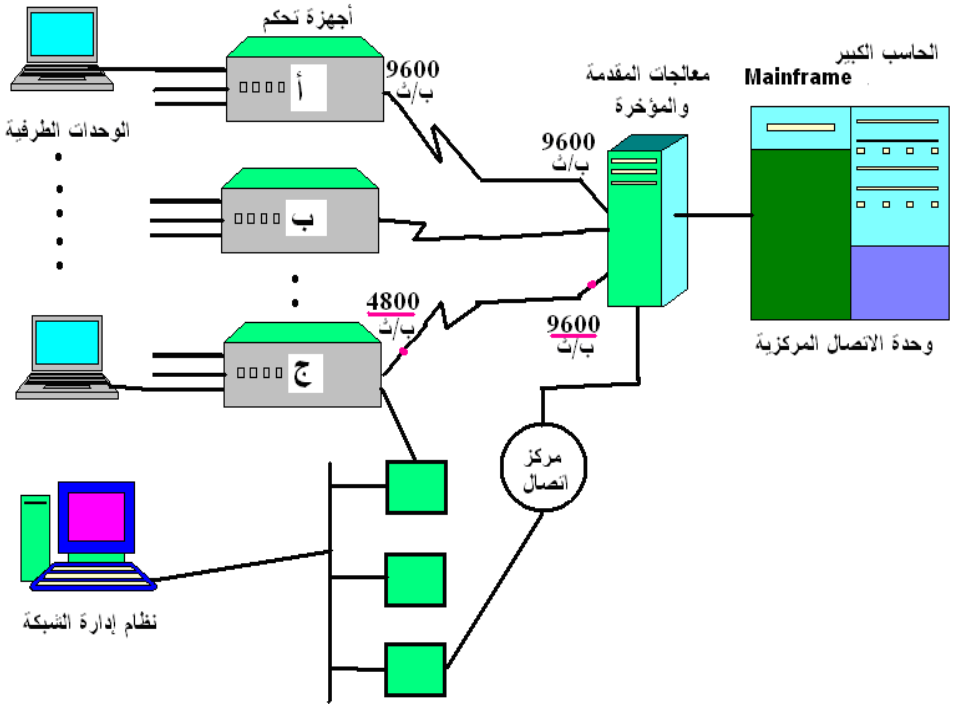
تستطيع الأداة المتقدمة دوريا Periodically، أن تقيم تهيئة كل أجهزة الشبكة وتظهر لنا وجود أي تكرار Duplication(إن وجد)، في عناوين الشبكة أو أسماء الأجهزة أو الوظائف. نفترض على سبيل المثال، شبكة محلية يتم توسعتها بدون إدارة، ويوجد العديد من خوادم ملفات الحاسبات الشخصية بهذه الشبكة. فينبغي على أداة إدارة الشبكة أن

تخبرنا أنه يوجد اثنان من أجهزة الخادم بهذه الشبكة يقومان بتأدية نفس الوظائف إلى المستخدمين. وهذا ربما يعبر عن وجود فائض Redundancy ، أو ربما يعبر عن وجود مشكلة في إدارة التهيئة تحتاج معالجة.

تستطيع الأداة المستخدمة **تقييم تهيئة الشبكة لتحديد قدرتها الاتصالية**. على سبيل المثال، نفترض أن الشبكة الموضحة في شكل4.5 ، تحتوى شبكة إقليمية WAN ، تتكون من أجهزة تحكم وحاسبات مقدمة ومؤخرة Front–End Hosts. والمطلوب تهيئة وحداتها البينية كي تقوم بإجراء عمليات الاتصال عند سرعات مناسبة. نفترض أن زمن الاستجابة من الوحدات الطرفية لأحد أجهزة التحكم أبطأ من زمن الاستجابة الناتج من الوحدات الطرفية لأجهزة التحكم الأخرى. لتقييم هذه الحالة عند بدء التشغيل، فإن أداة إدارة التهيئة سوف تدرك أن سرعة إرسال مجموعة أجهزة التحكم قد تم ضبطها عند القيمة 4800 بايت/ثانية، وأن سرعة حاسبات أجهزة المقدمة والمؤخرة عند الجانب الآخر قد تم ضبط سرعة الاستقبال بها بحد أقصى 9600 بايت/ثانية. وهذا ينتج عنه أن تصبح السرعة القصوى تكون 4800 بايت/ثانية. وعلى النقيض من ذلك، فإن مجموعة أجهزة التحكم الأخرى في نفس الجانب والمتصلة بنفس حاسبات المقدمة والمؤخرة كان قد تم ضبط سرعتها لتعمل عند 9600 بايت/ثانية في كلا الجانبين. سوف تستنتج الأداة أن هذا الاختلاف في معدلات سرعة أجهزة التحكم هو الذي سبب بطء زمن الاستجابة. وكخطوة أخيرة في عملية التقييم، سوف تقوم الأداة باستخدام قاعدة البيانات العلائقية لتحديد سرعة وصلة الشبكة الإقليمية WAN. وبذلك فإن الأداة تكون قد وجدت مشكلة تهيئة الشبكة آليا بواسطة تقييم معلومات إدارة التهيئة.

تعتمد الأداة المتقدمة على مجموعة الخصائص الوظيفية التي تقوم بها على وجود نظام إدارة قواعد البيانات. إن الأدوات المتقدمة المتوفرة في الأسواق، تقوم بتخزين المعلومات في قواعد بيانات أيضا، كما تساعد في بناء استفسارات باستخدام لغة "SQL".

معدل سرعة الإرسال والاستقبال، يتم كشفه بواسطة الأداة المتقدمة لإدارة الشبكة. ويوجد بعض المنتجات توفر لمهندس الشبكة إمكانية توليد تقارير متنوعة عن أجهزة الشبكة وأسماء الموردين. وبعضها يوفر وسائل لتوليد تقارير يمكن للمستخدم أن ينشئها بحسب احتياجاته. أما خاصية تقييم إدارة تهيئة الشبكة، فيمكن أن تتم من خلال بناء أداة تستطيع تقييم تهيئة الشبكة بشكل إجمالي. حيث أن المتوفر حاليا في الأسواق أن كل مورد ينتج برمجيات تختص بإيجاد أو وصف تهيئة أجهزة معينة خاصة بمنتجاتهم.



شكل4.5 شبكة إقليمية يوجد بها خطأ تهيئة ناتج عن عدم توافق

6. توليد تقارير التهيئة

عزيزي الدارس، كما شرحنا في الفقرات السابقة، أنه ينبغي على الأداة المتقدمة لإدارة التهيئة أن تقوم بتوليد التقارير اللازمة، التي تمكن مهندس الشبكة من معرفة التطورات الجديدة حول التهيئة الإجمالية للشبكة.

على الرغم من أن هذا النوع من الأداة غير مطلوب أن يرحل المعلومات بسرعة –مثل أداة إدارة الأعطال– فإنه في أحيان كثيرة يكون عرض هذه التقارير ضروريا، وخاصة عندما تجد الأداة تكراراً في العنوان أو تكراراً في أسماء أجهزة الشبكة. على عكس أداة إدارة الأعطال، فإن أداة إدارة التهيئة لا تعتمد على استخدام الألوان أو وحدات بينية رسومية لكي تعمل بشكل متكامل. فإذا استطاع مهندس الشبكة الدخول إلى البيانات من خلال وحدة طرفية تعمل بشفرة أسكي، فإن كل التسهيلات المتعلقة بإدارة تهيئة الشبكة سوف تكون متاحة أمامه. بالطبع، كلما كانت الأداة سهلة جعل ذلك مهندس الشبكة يستطيع توليد التقارير الضرورية بسهولة.

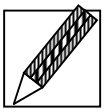
يمكن أن يحتوي التقرير على تفاصيل عن التهيئة الإجمالية لأجهزة الشبكة، وقدراتها ويشمل ذلك: أسماء الأجهزة، وعناوين الشبكة، والأرقام المسلسلة، أسماء الموردين ونظام التشغيل، الاسم المحلي للشخص المسئول عن الشبكة. إذا كان الجهاز موصل بوصلة توالى، فإن التقرير يمكن أن يشمل أيضا، أرقام الدوائر، وهي تكون مفيدة عندما يتم كتابة تقرير عن أعطال الوصلة، خاصة عندما يتم إرساله إلى مورد الدوائر. يوجد بعض البيانات الإضافية الاختيارية الأخرى، يمكن أن تحتوي على اسم الشخص المسئول في الشركة الموردة للأجهزة للاتصال به عند الحاجة، والمكان الفعلي لوجود الجهاز. وهذه المعلومات تمثل الحد الأدنى الذي يمكن أن يعبر عن أجهزة الشبكة.

إن معدل التكرار الذي يتم عنده توليد هذا التقرير يتغير حسب حالة كل شبكة. يمكن على سبيل المثال، أن يتم توليد هذا التقرير أسبوعيا، إذا كانت الشبكة تتغير بمعدل سريع، أو شهريا إذا كانت الشبكة مستقرة.

يمكن الاستعانة بهذا التقرير في تشغيل الشبكة الحالية، وربما نحتاج بعد ذلك إلى ملخص بكل التعديلات المطلوبة لتحديث الشبكة. إن هذا التقرير يحتوي على قائمة التغيرات المطلوبة للشبكة، مصنفة ومذكور بها اسم الشخص الذي يطلب التغيير، والمكان الذي سوف يحدث به التعديل. يمكن أن يشمل المصنف على الأجهزة الجديدة المطلوبة، والعتاد المطلوب تغييره، والبرمجيات والإدارات. إن تقسيم المعلومات المذكورة في التقرير إلى مصنفات يجعلنا نحصل على المعلومات المهمة بسرعة.

إن معدل إنشاء هذا التقرير يتغير حسب معدل التغيرات التي تحدث بالشبكة. وأخيرا فإنه على أداة إدارة التهيئة إنشاء تقرير ملخص بقائمة البيانات الإجمالية للشبكة. وهذا التقرير يتم الاحتفاظ به لبيان الجهود اللازمة لأي شبكة بيانات، وينبغي أن يركز التقرير فقط على أجهزة الشبكة. ويتضمن هذا التقرير: كل جهاز يتم شراؤه، الرقم المسلسل، والمكان الفعلي، وتاريخ وضع الجهاز في الخدمة، ومدة ونوع الضمان، وتاريخ شامل وحديث . وبناء على الوسط المحيط للشبكة، فإن إضافة معلومات عن كل جهاز يكون مطلوبا. بسبب أن ذلك عادة يكون ضروريا . ويمكن إنشاء هذا التقرير بشكل دائم شهريا.

تدريب (1)



أجب بعلامة صح أو خطأ مع تصحيح الخطأ في كل مما يلي:

أ- ينبغي أن تكون قائمة بيانات التهيئة في الشبكة سرية.

ب- تتعاون إدارة التهيئة في إجراء تعديلات تهيئة الأجهزة.

ج- يتميز ملف التهيئة المخزن بشفرة أسكي بأنه يمكننا من إنشاء علاقات مركبة بين البيانات المخزنة.

د- يتميز ملف التهيئة المخزن في نظام إدارة قاعدة البيانات بأنه يمكننا من إنشاء علاقات مركبة بين البيانات المخزنة.

هـ- من عيوب نظام إدارة قاعدة البيانات في نظام إدارة التهيئة أنه يستخدم لغة خاصة به.

و- تستطيع الأداة البسيطة لإدارة التهيئة عمل مقارنة بين التهيئة التشغيلية والتهيئة المخزنة.

ز- تستطيع الأداة المتقدمة لإدارة التهيئة تقييم تهيئة أجهزة الشبكة كي تؤدي عملها بصورة مثالية.

ح) تستخدم لغة SQL للاستفسار عن أجزاء معينة في قاعدة البيانات الخاصة بتهيئة أجهزة الشبكة.

ط) يمكن أن تساعد إدارة التهيئة مهندس الشبكة في تحديد قطع غيار أجهزة الشبكة.

ك) يستخدم رسام الخرائط الآلي لإيجاد أجهزة الشبكة التي سيتم تهيئتها آليا.

الخلاصة

عزيزي الدارس، تعرفنا في هذه الوحدة على إدارة التهيئة بالحصول على البيانات من الشبكة واستخدام هذه البيانات في إدارة وتنصيب كل أجهزة الشبكة. تناولنا تجميع معلومات عن التهيئة الحالية للشبكة، واستخدام هذه البيانات في عملية تعديل تهيئة أجهزة الشبكة، وتخزين البيانات، والاحتفاظ بقائمة حديثة، وتدوين تقارير مبنية على البيانات. في هذه الوحدة الدراسية ايضأ تعرفنا على فوائد إدارة التهيئة بالنسبة لمهندس الشبكة. وكما ناقشنا الخطوات اللازمة لإدارة عملية التهيئة. وشرحنا ثلاثة مستويات من أدوات إدارة التهيئة. كما عرضنا التقارير المختلفة التي يمكن الحصول عليها من بيانات التهيئة.

لمحة مسبقة عن الوحدة القادمة

عزيزي الدارس في الوحدة القادمة نتناول **إدارة الأمن** والتي تختص بحماية المعلومات الحساسة للأجهزة المتصلة بشبكة البيانات بواسطة التحكم في نقاط الوصول لتلك المعلومات وستناول أيضاً خصائص إدارة الأمن الأربعة .

وسنفرق بين إدارة الأمن وبين أمن التطبيقات، مثل أمن نظام التشغيل أو الأمن الفعلي. يتم تحقيق إدارة الأمن من خلال تهيئة حاسبات مضيفة محددة بالشبكة ، وذلك للوصول إلى نقاط الاتصال داخل شبكة البيانات. قد تشتمل نقاط الاتصال على: خدمات برمجية ، مكونات العتاد، ووسائط الشبكة. إن وسط الشبكة بالتحديد هو منطقة غير محصنة، عندما يتم اتصال شخص بوسط يحمل معلومات حساسة، فإن القياسات المأخوذة لتأمين المعلومات الحساسة في الحاسبات المضيفة أو أجهزة الشبكة تكون غير مفيدة. ،كن معنا في الوحدة القادمة وستجد الكثير المفيد إنشاء الله .

مسرد المصطلحات

الاستكشاف الآلي Auto-discovery

كيفية تمكننا من الحصول على قائمة البيانات الحالية لجميع أجهزة الشبكة. ويوجد طريقتين شائعتين يستخدمان لتنفيذ عملية الاستكشاف الآلي

بيانات الدوائر المؤجرة Leased Circuit

تشمل قائمة البيانات الخاصة بالمورد على: الاسم – العنوان – رقم الهاتف. وقد تشمل قائمة بيانات الدوائر المؤجرة علي: رقم الدائرة – السرعة – اسم المورد – عدد نقاط النهايات بالشبكة – المدة المسموحه و المدة التي سوف تتوقف عندها الخدمة.

ملف السجل Log File .

وعلى النقيض، إذا وجدت الأداة خط آمن Secure Line متصل بخادم الطرفيات بدون وجود كلمة سر له، فسوف تقوم الأداة بالتنبيه عن هذه الحالة بواسطة عرض إنذار.

المصطلح بالإنجليزية	معناه بالعربية
ATM (Asynchronous Transfer Mode)	نمط النقل الغير متزامن
Autodiscovery	الاستكشاف الآلي
Automapping	رسام الخرائط الآلي
Breadth-First Search	نظام البحث العرضي
Bit Rate	معدل إرسال المعلومة
Configuration Management	إدارة التهيئة
DBMS(Data Base Management System)	نظام إدارة قواعد البيانات
Deactivate	إخماد
Duplication	مضاعفة
FDDI (Fiber Distributed Data Interface	وحدة مواجهة بيانات موزعة مصنوعة من الألياف البصرية
Front –End Hosts	حاسبات مقدمة ومؤخرة
ICMP Echo(ping)	أمر الصدى "بنج"
Leased lines	دوائر الخطوط المؤجرة
Log File	ملف السجل
Malicious	ماكر
Parameters	معاملات
Periodically	دوريا
Query	استفسار
Secure Line	خط آمن
SQL (Structured Query Language)	لغة استفسار هيكلية

المصطلح بالإنجليزية	معناه بالعربية
Timeout	انتهاء الزمن
Redundancy	فائض
Running Configuration	تهيئة التشغيل

المراجع

[1] Network Configuration and Management, www.delmarlearning.com/companions/content/0766835197/ppt/Ch16.ppt

[2] Network Configuration Management via Model Finding , http://alloy.mit.edu/papers/NetConfigAlloy.pdf

[3] Configuration management - Wikipedia, en.wikipedia.org/wiki/Configuration_

[4] Web-based network configuration management system, ieeexplore.ieee.org/iel5/7138/19245/00889251.pdf

[5] Network Configuration Manager overview and features, www.openview.hp.com/products/ovncm/index.html.

[6] Configuration Management, www.aperture.com/ enterprise_strategies/ configuration _management.php

[7] Adaptive Network Configuration Management, whitepapers.techrepublic.com.com/whitepaper.aspx

[8] Network Configuration Management In Heterogeneous ATM Environments, www.springerlink.com/index/**QP3MXY948YWH56XY.pdf**

[9] Intelligent Network Configuration Management, www.nal.utoronto.ca/met/pdffiles/Intelligent

[10] Simplifying Network Management with EPICenter, www.extremenetworks.com/apps/whitepaper/

[11] Allan Leinwand , Karen Fang , Network Management, Addison Wesley 1992.

[12] Allan Leinwand, Network Management - A practical Perspective, 1999.


الوحدة الخامسة
إدارة الأمن

محتويات الوحدة

مقدمة

تمهيد

عزيزي الدارس مرحبا بك الى هذه الوحدة والتي بعنوان إدارة الامن.

تحتوي هذه الوحدة على **أربعة أقسام** رئيسة، تتناول أهم المفاهيم التاسيسية في إدارة الأمن تبدأ **بتعريف فوائد إدارة الامن.** ثم اختصاصات إدارة الأمن الأربعة وهي: تحديد المعلومات الحساسة من أجل حمايتها، و إيجاد نقاط الاتصال، والعمل على تأمين نقاط الاتصال، ثم الحفاظ على نقاط الاتصال.

وفي القسم الثاني تتناول ادوات إدارة الأمن من خلال التعرف على أمن الحاسب وأمن المستخدم ثم أمن المفتاح السري .

. وأخيراً نناقش في هذه الوحدة مميزات سجلات الفحص التي يمكن الحصول عليها من تقارير حوادث الأمن.

أهلا بك مرة أخرى إلى هذه الوحدة، عسى أن تنتفع بها وأن تفيد منها، وأن تساعدنا في نقدها وتطويرها .

أهداف الوحدة

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

- تُعرّف فوائد إدارة أمن شبكة البيانات.
- تشرح كيفية تحقيق إدارة أمن شبكة البيانات.
- تفرق بين طرق إيجاد نقاط الاتصال وتأمينها والحفاظ عليها آمنة.
- تحدد وظائف توثيق المستخدم والحاسب ومفتاح الدخول.
- تحلل معاني تشفير المفتاح الخاص والعام ووظائفهما لحماية المعلومات.
- تعدد استخدامات الجدار الناري وترشيح الحزم في أمن شبكة البيانات.
- تبرر استخدم الأدوات البسيطة والمركبة لإدارة أمن شبكة البيانات.
- تصف المتطلبات اللازمة لبناء شبكة بيانات آمنة، وكيفية إدارتها.
- تنصب بعض برامج إدارة أمن الشبكة وتهيئتها عمليا.

1. فوائد إدارة الأمن لشبكة البيانات

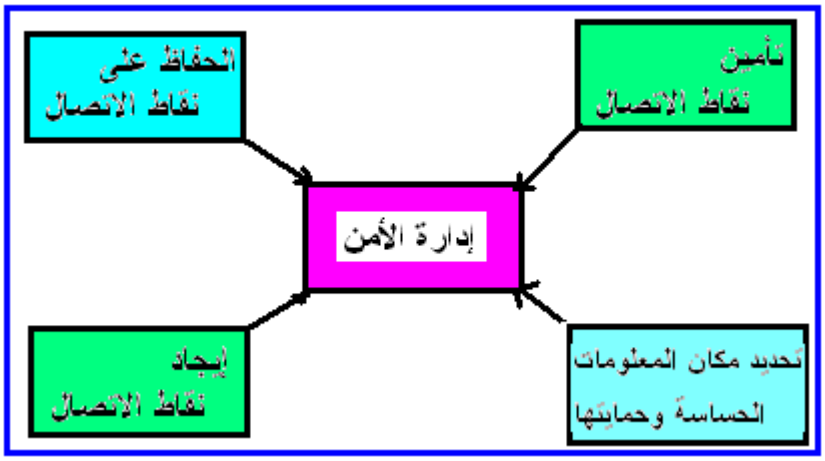
عزيزي الدارس إن الاهتمام المبدئي للعديد من المستخدمين عند توصيل حاسبات مضيفة إلى شبكة البيانات يكون ضعف الجهد المبذول في أمن المعلومات الحساسة الموجودة في الحاسب المضيف. وللتغلب على هذه المشكلة، يمكن **للحاسب المضيف** الذي يحفظ المعلومات الحساسة **منع الوصول للشبكة ومنع نقل المعلومات على وسط متنقل،** ويشمل هذا الوسط: الشرائط الممغنطة أو الأقراص الضوئية. بهذه الطريقة، يستطيع فقط المستخدمون الذين لهم اتصال فعلى بالحاسب المضيف الوصول إلى المعلومات الحساسة. ولكن هذه الطريقة برغم الأمن، ليست ذات كفاءة، فهي تزيح بفاعلية الاحتياج إلى شبكة البيانات.

يستطيع التنصيب الملائم وصيانة إدارة الأمن، توفير أكثر من بديل عملي يحقق اهتمامات أمن المستخدمين ويزيد من رضاهم في فعالية وأمن الشبكة. إن بناء الرضا وأمن المعلومات الحساسة هما الفوائد الأساسية من إدارة الأمن. إن الانعكاسات من عدم وجود إدارة أمن للشبكة من الممكن أن نتصوره بسهولة. على سبيل المثال، بفرض أن شبكة بيانات خاصة بأحد المؤسسات تم توصيلها بشبكة البيانات العامة، وأن أحد أجهزة الحاسب في شبكة المؤسسة يحتوي على معلومات الرواتب، ويوفر أيضا طلبات تأدية خدمة معلوماتية لأي مستخدم. كما نلاحظ، فإن عاقبة هذا الاتصال غير المحكوم والمباح يمكن أن يضر المؤسسة.

2. تحقيق إدارة الأمن في شبكات البيانات

عزيزي الدارس، تتطلب إدارة الأمن الفعالة من مهندس الشبكة أن يوازن بين الاحتياج إلى معلومات حساسة آمنة، وبين احتياجات المستخدمين من الوصول إلى المعلومات ذات الصلة لتأدية وظائفهم. لضمان تحقيق ذلك في إدارة الشبكة ينبغي اتباع أربع خطوات، كما هو مبين في شكل5.1، وهي:

- تحديد المعلومات الحساسة.
- إيجاد نقط الاتصال.
- تأمين نقط الاتصال.
- والحفاظ على نقط اتصال آمنة.



شكل5.1 وظائف إدارة الأمن.

1.2 كيفية تحقيق وظائف إدارة الأمن

يوضح شكل5.2 كيفية تحقيق وظائف إدارة الأمن. حيث تمثل قائمة رواتب الموظفين قاعدة بيانات المعلومات الحساسة المتصلة بالحاسب الكبير.تعتبر نقاط الاتصال هي: الدخول عن بعد، ونقل الملف. يقوم مهندس الشبكة بتأمين نقاط الاتصال بواسطة تهيئة النظام من خلال وحدة الإظهار (وحدة طرفية) للسماح فقط بتشغيل المستخدمين المفوضين (Authorized). يقوم نظام الرصد بضمان صيانة الأمن بواسطة تسجيل محاولات الدخول غير المفوضة.

أولا: تنصيب الوسائل الأمنية:

مثال: نفترض جهاز حاسب يقوم بتخزين رواتب الموظفين لأحد المؤسسات، وهو الذي يحتفظ بمعلومات حساسة عن المؤسسة، وله نقطة اتصال واحدة، من خلال شبكة البيانات، وذلك باستخدام برنامج الدخول عن بعد. والمطلوب هو إجراء عملية التحكم في الدخول لهذا البرنامج.

الحل

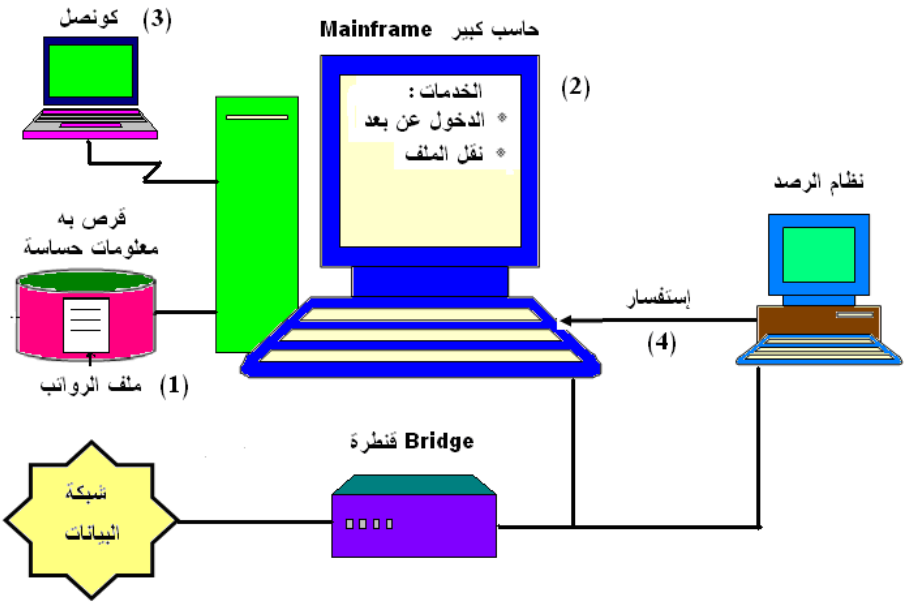
ولإجراء ذلك نتبع الخطوات التالية:

أولا: نستطيع أن نكفل للموظفين الذين لديهم تفويض تام بالاطلاع على المعلومات، وذلك بأن يخصص لهم فقط أرقام حسابات كمستخدمين.

ثانيا: ضمان تخصيص كلمات سر (Passwords) يتم طلبها من برنامج الدخول لكل رقم حساب مستخدم.

ثالثا: لتحسين عملية الأمن أكثر، نستطيع استخدام برنامجاً لتوليد كلمات السر بشكل عشوائي، ويتم تجديدها دوريا.

وهكذا، بعد أن يتم تنصيب هذه الوسائل الأمنية، يمكن أن نطمئن أننا قد قمنا بتأمين المعلومات الحساسة.



شكل5.2 متطلبات تحقيق الخطوات الأربعة المستخدمة في إدارة الأمن.

ثانيا: استخدام الحاسبات المضيفة المفوضة:

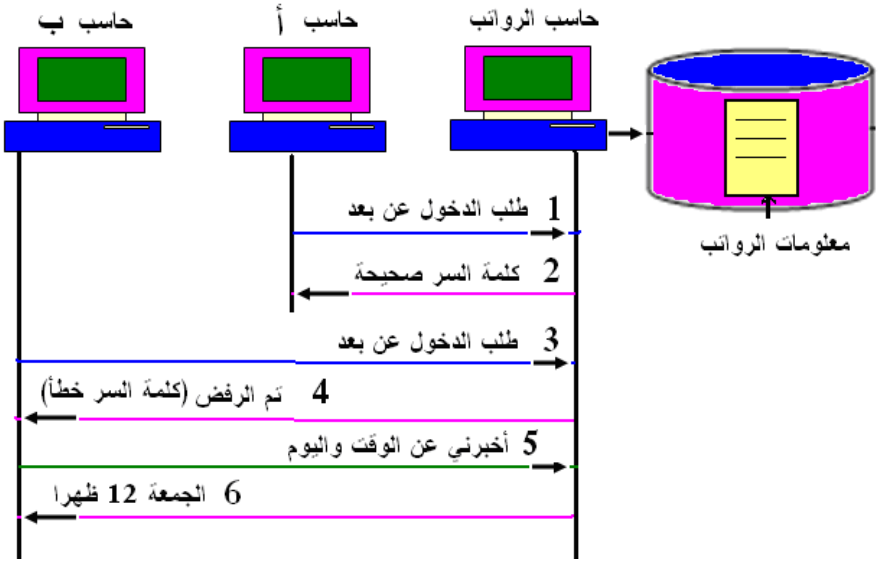
إن مستوى الحماية السابق شرحه، ربما لا يكون كافيا. بالإضافة إلى وجود كلمات سر لكل حساب. ربما نريد توفير طلبات دخول عن بعد إلى الحاسبات المضيفة الخاصة بقوائم الرواتب، وأن تأتي فقط عن بعد من قبل حاسبات مضيفة مفوضة (Authorized Remote Hosts). ولكي يتمكن المستخدم من الوصول إلى بيانات الرواتب، يجب أن يدخل أولا عن بعد إلى الحاسبات المضيفة المفوضة، ويوثق إذن الدخول بواسطة كلمة السر. بعد ذلك يمكن أن يسمح للمستخدم بأن يواصل الدخول إلى جهاز الحاسب المخزن عليه الراتب، مرة أخرى من خلال سلسلة متعاقبة من كلمات السر الموثقة.

لاحظ في هذا المثال أننا لم نحاول تأمين المعلومات الحساسة نفسها. على الرغم من أن المعلومات الحساسة تكون آمنة داخل جهاز الحاسب، سوف نجد بعد ذلك أنه من الضروري، أن يتم تأمينها بين الأماكن الآمنة. أيضا ينبغي أن نكون على دراية بأنه في بعض الحالات لا يتطلب الوضع تأمين نقط الدخول كلها. على

سبيل المثال، نفترض أن حاسب الرواتب، يمكن الوصول إليه بواسطة الدخول عن بعد، لتوفير خدمات لإبلاغ مستخدمي الشبكة عن الوقت، وهذا لا يعتبر معلومات حساسة عادة. في مثل هذه الحالات يمكن أن يسمح بالدخول بحرية إلى خدمات الوقت، كما هو موضح في شكل 5.3.

لكي نقنن عملية الدخول إلى معلومات الرواتب، يتم اتباع الخطوات التالية:

- يطلب المستخدم الموجود على جهاز الحاسب_"أ" طلب الدخول عن بعد إلى حاسب الرواتب.
- إذا كانت كلمة السر صحيحة، يتم السماح له بالدخول.
- يحاول مستخدم موجود على جهاز الحاسب_"ب" الدخول عن بعد إلى حاسب الرواتب.
- يتم رفضه لأن كلمة السر غير صحيحة.
- يقوم المستخدم الموجود عند الحاسب_"ب" بالسؤال عن اليوم والوقت من حاسب الرواتب.
- يقوم حاسب الرواتب بإخباره عن اليوم والوقت، حيث أن معلومات الرواتب هي معلومات حساسة، لكن المعلومات عن اليوم والوقت ليست معلومات حساسة.



شكل5.3 طريقة الوصول للمعلومات الحساسة.

1.2 تحديد المعلومات الحساسة

إن الخطوة الأولى لتحقيق إدارة الأمن تتم بواسطة تحديد الحاسبات المضيفة المتصلة بالشبكة، والتي يوجد بها المعلومات الحساسة. إن معظم المؤسسات يوجد بها نظام يعرف جيدا المعلومات الحساسة، وهي غالبا **المعلومات التي تحتوي على: الحسابات، الماليات، العملاء، التسويق، الهندسة، ومعلومات الموظفين**. لذلك من الوهلة الأولى، فإن هذه العملية تظهر مباشرة، ولكن ما يتم تعريفه بأنه معلومات حساسة يمكن أن يختلف من مؤسسة لأخرى، ويعتمد على الوسط المحيط. إن الجزء الصعب في تحديد المعلومات الحساسة هذه، هو إيجاد مكان على الحاسب المضيف لتخزين هذه المعلومات.

أسئلة تقويم ذاتي

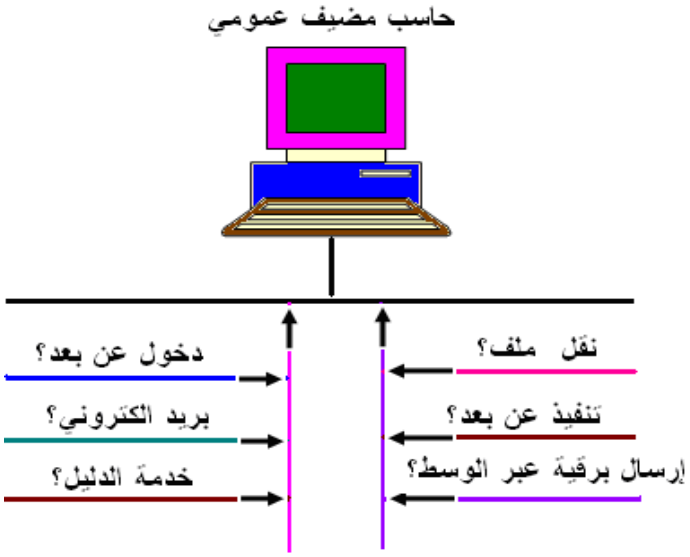
أكمل ما يلي: تختص إدارة أمن شبكة البيانات بأربعة خصائص هي:

1- ..... 2-.....

3- ..... 4-.....

إيجاد نقاط الاتصال

بعد أن يتم معرفة المعلومات الحساسة ومكانها، بعد ذلك يتم تحديد كيفية وصول مستخدمي الشبكة من الوصول إليها. مع الأخذ في الاعتبار أن نقط الاتصال الأولى لأي شبكة بيانات هي الأسلاك الفعلية. إن إيجاد نقط اتصال أخرى في شبكة البيانات يكون غالبا وظيفة صعبة، وهذا سوف يتطلب عادة فحص كل جزء من البرنامج الذي يقوم بتأدية خدمة في الشبكة. ويوجد العديد من الحاسبات تمتلك الكثير من مثل هذه البرامج. إن الوصول لهذه البرامج يجبر شبكة البيانات على أن تساهم في الوصول من خلال نقط الاتصال إلى المعلومات الحساسة على الحاسب، كما هو موضح في شكل 5.4. لحسن الحظ، فإن بعض أجهزة الحاسبات تمكننا من تبسيط مهمة إيجاد نقط الاتصال، بواسطة عزل طريقة توفير الدخول عن بعد ونقل الملف.



شكل5.4 تحديد نقاط الاتصال لكل حاسب.

تدريب (1)

1. ضع علامة صاح أمام الجملة الصحيحة وعبارة خطأ أمام الجملة الخطأ
2. يختص الأمن الفعلي للمؤسسة غلق أبواب غرف الحاسبات.
3. يختص الأمن الفعلي للمؤسسة تنصيب بطاقات اتصال بالنظم
4. يختص الأمن الفعلي للمؤسسة توفير وحدات مفاتيح للأقفال
5. من فوائد إدارة أمن شبكة البيانات تحقيق اهتمامات امن المستخدم.
6. من فوائد إدارة أمن شبكة البيانات تحقيق امن المعلومات الحساسة.
7. يتحقق إدارة امن شبكة البيانات بواسطة: تحديد المعلومات الحساسة.
8. يتحقق إدارة امن شبكة البيانات بواسطة: إيجاد نقاط الاتصال بالشبكة.
9. يتحقق إدارة امن شبكة البيانات بواسطة تنصيب بطاقات اتصال بالنظم.

- **الاتصال بالشبكة بطريقة غير رسمية (Anonymous Method):**

عزيزي الدارس، تقم معظم أجهزة الحاسبات المتصلة بشبكة البيانات بتوفير الدخول عن بعد للمستخدمين. وإذا لم تقم وسيلة الدخول هذه بتحديد المستخدمين المنفردين (Unique) وتقنين حركتهم من خلال النظام إلى المناطق المفوضة لهم، مع إمكانية فحص نقط الاتصال بقدر الاستطاعة وجعلها آمنة (تستطيع كثير من الحاسبات أيضا، تحقيق عملية نقل الملفات عبر شبكة البيانات. مثل وسيلة الدخول عن بعد.) فإن استخدامها سوف يكون محدودا. كمثال على خدمة نقل الملفات، الذي يتطلب تدقيق إدارة الأمن هو عملية دخول المستخدم كضيف (Guest) في نظام غير رسمي (مجهول المصدر Anonymous) في بروتوكول نقل الملفات FTP، وهو نظام يسمح للمستخدم بالدخول لمواقع محددة في الشبكة كزائر، ويسمح للمستخدم بنقل ملفات محددة.

يستخدم بروتوكول FTP في العديد من الحاسبات المضيفة التي تستخدم بروتوكول TCP/IP. ويوجد العديد من الإصدارات التي تسمح للمستخدمين بالدخول من خلال نظام غير رسمي، وهذا النظام لا يستخدم كلمة سر، لذلك فإن المستخدمين يمكنهم كتابة أي حروف لكلمة السر والدخول إلى حساب خاص في النظام عن بعد. إن التوفير الذي يوفره الدخول من خلال نظام غير رسمي هو أن الملفات التي يستطيع المستخدم استرجاعها من هذا الحساب عادة تكون محدودة لبعض أجزاء صغيرة من المجلدات. وتستخدم عملية تهيئة بروتوكول نقل الملفات غالبا في توزيع الوثائق والبرمجيات العامة. يمكن استخدام هذا التطبيق أيضا، عندما لا يهتم مدير جهاز الحاسب بمن سوف يستطيع الدخول إلى الملفات الموجودة في هياكل المجلدات المحددة. وبهذا، إذا قام جهاز حاسب بتوفير خاصية الدخول "غير رسمية" لخدمة بروتوكول نقل الملفات، فإنه ينبغي على مهندسي الشبكة المتصلة بها الحاسب أن يقوموا بتنظيم المعلومات الموجودة بهذه المجلدات بعناية.

- **طريقة إظهار ومعرفة الملفات المطلوبة:**

ربما تكون عملية الدخول عن بعد ونقل الملفات، هي من أكثر أنواع البرامج شيوعا، والتي توفر نقاط اتصال إلى جهاز الحاسب. لكن يوجد برامج أخرى مثل: البريد الإلكتروني، وتنفيذ العمليات عن بعد، وملفات ومجلدات أجهزة الخادم، وأسماء أجهزة الخادم، يمكن أن تخصص نقاط اتصال إلى جهاز الحاسب، والتي تحتاج أن تكون آمنة بواسطة إدارة الأمن. على سبيل المثال، إن جهاز الحاسب الذي يعمل بنظام التشغيل يونيكس، تكون الخدمات التي يوفرها الجهاز، ممكنة رؤيتها بواسطة أمر تنفيذ حالة العملية (Process Status: ps)، والتي يمكن أن تظهر كافة العمليات التي تعمل على جهاز الحاسب.

- **نظام ملفات الشبكة NFS(Network File System):**

يسمح نظام ملفات الشبكة NFS(Network File System)، الموجود في أنواع مختلفة عديدة لأجهزة الحاسب، لأحد أجهزة الحاسب من الوصول إلى ملفات نظام آخر كما لو أنه موجود على الحاسب المحلي باستخدام شبكة البيانات. كما أن النظام أيضا يفيد في مشاركة المصادر، حيث يستطيع فتح نقاط توصيل إلى الملفات الحساسة. بالمثل، يوجد الكثير من الحاسبات الشخصية يوجد بها ملفات أو تطبيقات توضح قائمة الخدمات التي يستطيع جهاز الحاسب تقديمها. يمكن أن يكون هذا الملف شائعا، مثل ملف تهيئة الشبكة NET.CFG ،أو ملف مخبأ مثل الملفات ذات الامتداد INI. إن إيجاد التطبيقات الموجودة على الحاسب الشخصي، التي ربما تستخدم الشبكة يمكن أن تكون عملية صعبة. وقد نحتاج استخدام محلل بروتوكول الشبكة، للمساعدة في تحديد نوع بروتوكول الشبكة الذي يجب أن يستخدمه الحاسب الشخصي.

- **استخدام بروتوكول NetBIOS:**

مثال: إن الحاسب الشخصي الذي يعمل كمدير في وسط شبكة محلية لميكروسوفت، يستخدم بروتوكول NetBIOS لإجراء عمليات الاتصال بين العملاء وأجهزة

الخادم. وهذا الوسط له خاصية ميدانية (Domains)، وهي منطقة في الشبكة يوجد بها جهاز الخادم. يقوم الخادم بإذاعة اسمه والمقاطعة التي يوجد بها على فترات دورية. على العملاء أن تصغي إلى التحديثات من خلال اسم ميداني خاص، قبل أن تستطيع رؤية أجهزة الخادم في هذه المقاطعة (وتقوم بعد ذلك بالاتصال بهم). وعلى الرغم من أن المنطقة الميدانية (المقاطعة) في هذا السياق، تعني وجود وسيلة إدارية لتقسيم حركة مرور الرسائل، فهي غالبا تستخدم كمقياس للأمن (Security) Measure أيضا. يستطيع مدير الشبكة المحلية المتطور أن يغير أسماء المقاطعة (Domain Names) التي يصغي إليها العملاء، بعد ذلك من المحتمل أن يتصل بأي جهاز خادم في المقاطعات المعروفة. بالطبع، يحتاج المستخدم أن يدخل على الخادم قبل أن يتمكن من الوصول إلى البيانات، ولكن لإيجاد المقاطعات الأخرى في الشبكة ربما يؤدي إلى اختراق الأمن (Security Breach). على الرغم من ذلك، يقوم الخادم بإذاعة مثال من نقط الاتصال التي تدل على وجود خدمة الشبكة، وربما تحتاج أن تدار بعناية. في هذا المثال، تتم عملية ***إدارة الأمن بواسطة إخفاء المعلومات*** عن أنظمة العميل. إن عملية تحقيق الأمن بواسطة إخفاء المعلومات عموما لا تعتبر صحيحة من الناحية العملية، ولكنها تستخدم غالبا. إن ***مرشحات الحزم البرمجية*** التي ترفض إذاعة الخادم من خلال قطاعات العميل، ربما توفر إدارة أمن أكثر فاعلية في هذا التنصيب. إن أحسن طريقة، على الرغم من التهيئة المكثفة، ربما تكون مرشحات الحزم التي تسمح فقط لمجموعة من العملاء المفوضين، بأن ترسل حزم بيانات إلى أجهزة خادماتهم الخصوصية.

- **استخدام البروتوكول ZIP:**

إن فكرة منطقة الشبكة التي تحتوى على خدمات معينة تخصص إلى المستخدمين، بخلاف الطريقة التي تستخدم NetBIOS، توجد في العديد من بروتوكولات الشبكات الأخرى. على سبيل المثال، في شبكة أبل Appletalk توجد مناطق في الشبكة تسمى (Zones)، يستطيع مستخدم شبكة أبل أن يكتشف

مناطق في الشبكة بواسطة إرسال طلب يسمى بروتكول معلومات المناطق ZIP (Zone Information Protocol). وعندما يتم إيجاد المناطق، يستطيع المستخدم اختيار المنطقة التي يريد الاتصال بها ونوع الخدمة الموجودة في المنطقة بواسطة استخدام تطبيق يسمى "Chooser". وإذا استطاع أحد المخترقين (Crackers) للشبكة إيجاد منطقة، فقد يمكنه إيجاد الحاسبات المضيفة للمعلومات الحساسة خلال مناطق.

أسئلة تقويم ذاتي

أذكر ثلاثة أنواع (طرق) لتأمين نقاط الاتصال في إدارة أمن شبكة البيانات.

اشرح مع التوضيح بالرسم كيف تتم عملية الوصول للمعلومات الحساسة عن بعد؟ وكيف يتم الاستفسار عن الوقت واليوم، في نظام إدارة أمن الشبكة؟

أذكر باختصار دور (وظائف) المكونات التالية في إدارة أمن شبكة البيانات:

- بروتوكول ZIP.
- استخدام وحدة NetBIOS.
- المحلل البروتوكولي.

استخدام المحلل البروتوكولي:

عزيزي الدارس، إن التسهيلات التي تسمح للمستخدمين ***برصد حزم البيانات*** أثناء سيرها عبر وسط الشبكة، يمثل نقطة اتصال أخرى للمعلومات الحساسة. نحتاج في بعض الأحيان تجميع حزم البيانات لفحص كيفية أداء سلوك معيب للشبكة. ويتم هذا غالبا باستخدام محلل البروتوكول، أو حاسب مضيف. إن الاحتياج لهذه الوظيفة أو العمل غالبا يفوق أي تصورات أمنية، لأنه إذا لم تعمل الشبكة بشكل صحيح، فإنه

سوف لا يوجد بيانات حساسة تستطيع المرور في الشبكة. ولكن على مهندس الشبكة أن يكون على دراية بأن المستخدمين لديهم هذه المقدرة وتستطيعون تجميع حزم البيانات، واحتمالية اكتشاف كلمات السر، والمعلومات الحساسة الأخرى. كما سوف يتم شرحه تباعا في الفقرات التالية. إن ***تشفير البيانات*** في الحزم ربما يساعد على منع تجميع المعلومات الحساسة بواسطة محللي الشبكة.

وبسبب أن محلل الشبكة يستطيع أن يرصد كل حزم البيانات في الشبكة، فإنها تعتبر أداة ممتازة لإيجاد أية حاسبات مضيفة في الشبكة بالتحديد. كما تستخدم أنواع بروتوكولات في إجراء عمليات الاتصال. غالبا لا يعرف المستخدمون البروتوكولات التي تستخدمها تطبيقاتهم، وأن محلل الشبكة يستطيع منع أي شك لمهندس الشبكة. ويوجد العديد من المؤسسات التي تستطيع تقديم المساعدة للمستخدمين كي يقوموا بتحديد أنواع البروتوكولات التي تستخدمها الحاسبات المضيفة في إجراء الاتصالات.

- **استخدام بروتوكول إدارة الشبكة:**

إن الكثير من أجهزة الحاسبات توفر معلومات غير حساسة ظاهريا من خلال بروتوكولات إدارة الشبكة. ولكن عند الفحص من قرب في هذه المعلومات، ربما نكتشف أن الاتصالات المحظورة ينبغي أن يتم التأكيد عليها. على سبيل المثال، إن كل بروتوكول إدارة شبكة تقريبا يكون له قدرة على سؤال الحاسب عن المعلومات الأساسية، مثل عناوين الشبكة، ونوع إصدار نظام التشغيل، ومدة التشغيل، والمعلومات العامة غير الضارة. نفترض على الرغم من ذلك، أن الحاسب الذي يقوم بتشغيل بروتوكول إدارة الشبكة، يقوم بفحص إصدار نظام تشغيل جديد من المورد. عندما يقف في طابور الانتظار من قبل مورد مضارب، فإن إصدار نظام التشغيل العائد، يكون هو النظام غير المعروف للعامة بعد. هذا النقص من المعلومات، على الرغم من صغره، ربما يؤثر على سوق منتجات المضاربين.

- **استخدام نظام إدارة الشبكة:**

عامل آخر، غالبا نغفل عنه هو المكان الذي يحتوى على المعلومات الحساسة في شبكة البيانات، وهو نظام إدارة الشبكة نفسه. إن نظام إدارة الشبكة يوفر طرقاً كثيرةً للمستخدمين للكشف عن المعلومات الحساسة، الموجودة على الشبكة، والموجودة في قاعدة البيانات العلائقية. عندما يتم تحديد نقاط الاتصال بشبكة البيانات، ينبغي أن نأخذ في الاعتبار نظام إدارة الشبكة كحاسب مضيف يحتاج الى اهتمامات أمنية خاصة.

- **توحيد معايير نقاط الأمن:**

تخصص كثير من المؤسسات مصادر مادية، لتوحيد نقاط الأمن لجميع أجهزة شبكاتهم والحاسبات المضيفة. ويعمل توحيد أمن الشبكة كقاعدة للتعامل مع الطرق العديدة للوصول إلى المعلومات الحساسة. يمكن تحقيق هذه المعايير من خلال أي عدد من المعاملات. على سبيل المثال، نستطيع تعريف نقاط الاتصال بواسطة مصنعي الحاسب المضيف، أو نوع نظام التشغيل. في هذه الحالات، فإن المؤسسة تستطيع أن تقرر أن كل الحاسبات المضيفة من مصنع معين به معلومات حساسة لا يمكن الدخول إليه بواسطة بروتوكول نقل الملفات عن طريق نظام غير رسمي (Anonymous)، أو يستطيع تحديد أن حزم برامج الشبكة للحاسبات الشخصية لا توفر أمناً كافياً، وبذلك تمنع من استخدامها. المبدأ الرئيسي هنا يكون للمستخدم في وضع معايير مصنع الحاسبات المضيفة التي تستطيع حفظ المعلومات الحساسة والتطبيقات التي تستطيع تشغيل هذه الحاسبات المضيفة دون تسوية الأمن.

3.2 تأمين نقاط الاتصال

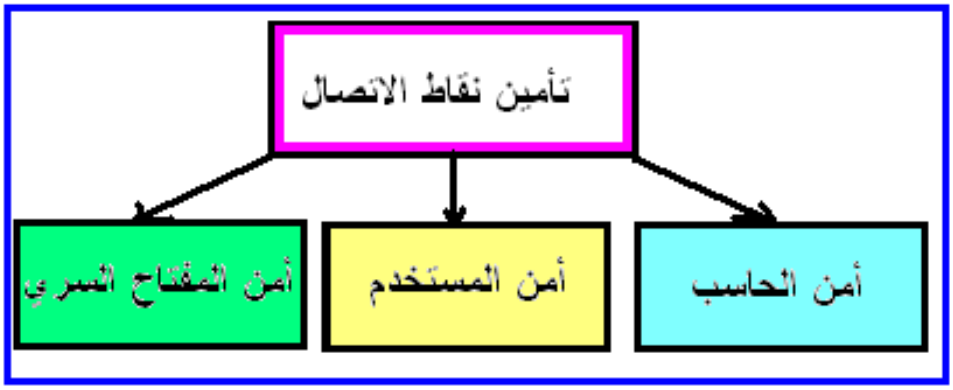
إن الخطوة التالية في إدارة الأمن، هي تطبيق تقنيات الأمن الضرورية. ويمكن استخدام الأمن في مستويات عديدة في شبكة البيانات، كما يلي:

- يمكن استخدام التشفير في مستوى وصلة البيانات.
- يمكن استخدام مرشحات الحزم لتأمين تدفق حركة البيانات في أجهزة مستوى الشبكة.

1.3.2 وسائل تأمين نقاط الاتصال في الشبكة

يوجد بكل حاسب مضيف خدمات مصاحبة، وهذه الخدمات توفر الوصول إلى المعلومات الحساسة التي تستطيع توفير واحد أو أكثر من بين ثلاثة أنواع للأمن، هي موضحة في شكل5.5، وتشمل على ما يلي:

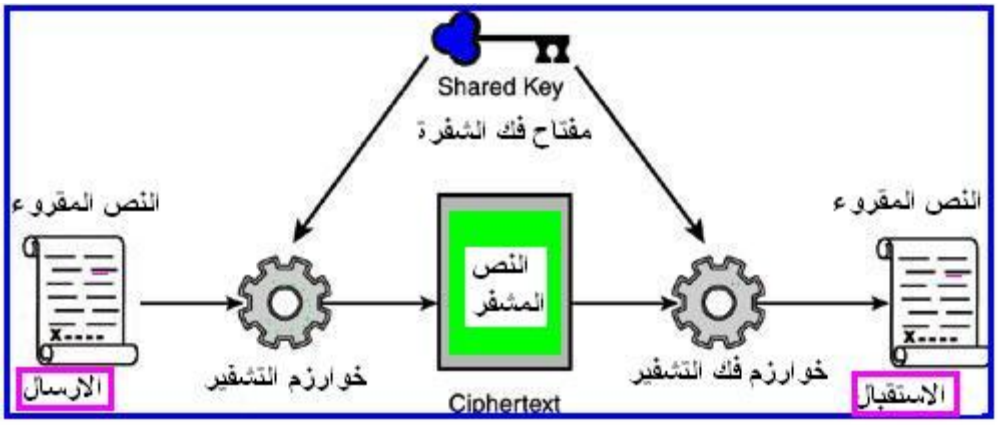
- أمن الحاسب المضيف بواسطة التوثيق.
- أمن المستخدم بواسطة التوثيق.
- أمن المفتاح السري بواسطة التوثيق.



شكل5.5 وسائل تأمين نقاط الاتصال.

2.3.2 التشفير

إن تشفير البيانات التي تنتقل من خلال الشبكة المحلية LAN أو من خلال الشبكة الإقليمية WAN، يمكن أن تمنع المستخدمين غير المصرح لهم بدخول الشبكة من الوصول للمعلومات الحساسة. والتشفير يعني عملية التكويد، وفي هذه الحالة، فإن الجهاز المشفر يستخدم خوارزم لمزج أو تشفير المعلومات المقروءة (plaintext) لإرسالها. عندما تمرر المعلومات المقروءة إلى خوارزم التشفير، يسمى خرج هذه العملية النص المشفر (Cipher-text). بعد إرسال النص المشفر، يتم فك الشفرة عند نهاية الاستقبال بواسطة تحقيق العملية الخوارزمية العكسية لاسترجاع النص الأصلي، ويبين شكل5.6 مراحل عملية التشفير.



شكل5.6 مراحل عملية التشفير.

إن مفتاح التشفير هو عبارة عن برنامج أو عتاد مخصص لذلك، ويستخدم للتحكم في خوارزم التشفير. كل نظام متتابع منفرد من المعلومات (Bits) في مفتاح التشفير يقوم بتوليد نص مشفر مختلف عن النص الأصلي. يجب أن يقوم خوارزم التشفير بتوليد مفتاح المشفر. لا يستطيع المستخدم فك شفرة النص المشفر بدون معرفة كلا من خوارزم التشفير ومفتاح الشفرة. ويكون التشفير مفيدا جدا عندما يتم إرسال

البيانات عبر الأقمار الاصطناعية، ووصلات موجات الميكروويف، التي تقوم بإرسال المعلومات عبر الأثير، حيث تكون عرضة لأن يتم استقبالها من أي أحد سواء أكان مفوضا بذلك أو غير مفوض. تستخدم بعض المؤسسات تشفير القطاعات (Segments) في الشبكات المحلية، لضمان أن الأسلاك الفعلية للشبكة المحلية لا تمثل نقاط اتصال. لكن لسوء الحظ أن هذه الطريقة مكلفة، لأنها تحتاج وجود عتاد مشفر أو برنامج لكل جهاز متصل بالشبكة المحلية. أيضا، إن تشفير الشبكة المحلية يجعل عملية فحص أعطال الشبكة مشكلة صعبة.

تقنيات التشفير الشائعة:

يوجد نوعين من تقنيات التشفير الشائعة، هما:

1- طريقة استخدام المفتاح الخاص (Private Key).

2- طريقة استخدام المفتاح العام (Public Key).

- **أولا: طريقة استخدام المفتاح الخاص:**

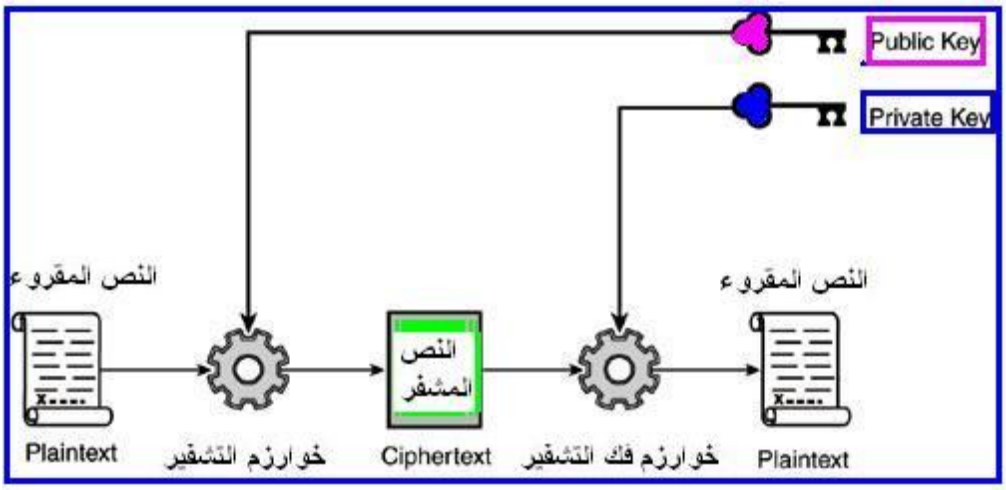
تعتمد طريقة التشفير باستخدام المفتاح الخاص على حقيقة أن كلا من المصدر والهدف يستخدمان نفس مفتاح التشفير، لتشفير وفك تشفير معلومات النص. وهذا يجعل خوارزم التشفير بسيطاً طالما تم معرفة مفتاح التشفير. وبسبب أن مفتاح التشفير ربما يتم كسره (معرفته)، لذلك يمكن تغيير المفتاح عند كلا من المصدر والهدف على أساس منتظم بواسطة إرسال فعلي لمفتاح جديد (إما باستخدام العتاد أو البرامج)، لكل جهاز يحقق تشفير. إن الإرسال الفعلي للمفتاح يمكن أن يستهلك جزءاً من وقت ومصادر الشبكة، لكنها تكون الطريقة الأكثر أمانا لنقل المفاتيح. وعلى الرغم من أن تشفير الأجهزة بطريقة المفتاح الخاص يمكن أن يكون الاحتفاظ به صعب، لكن كثير من المؤسسات تفضل استخدام هذه الطريقة لتأمين المعلومات الحساسة.

- **نظام التشفير القياسي** DES(Data Encryption Standard):

نظام التشفير القياسي هو أحد نظم التشفير الشائعة التي تستخدم المفتاح الخاص. وباستخدام DES يتم تشفير النص المقروء باستخدام قطاعات حزمية طولها 64 بيت. عند نظام المصدر، كل قطاع نصي مقروء يتم تشفيره باستخدام مفتاح تشفير طوله 56 بيت. إن أي انحراف بسيط مكمل للمفتاح 56 بيت ينتج عنه تشفير نصي مختلف تماما. يستخدم الخوارزم المركب دخل نص مقروء طوله 64 بيت، ويتم تشفيره إلى 64 بيت نص مشفر. عند نظام الهدف، تتم العملية العكسية، ويحول النص المشفر إلى نص مقروء.

- **ثانيا: طريقة استخدام المفتاح العام:**

إن استخدام طريقة المفتاح العام في التشفير لا تعتمد على مشاركة كل من نظام المصدر والهدف لنفس مفتاح التشفير. حيث تمنع هذه الطريقة مشكلة الاحتفاظ بمفاتيح تشفير متزامنة. في الواقع، تستخدم بعض النظم، مفتاح التشفير الخاص البسيط في البيانات، ومفتاح التشفير العام لتبادل قيمة المفتاح الخاص. يستخدم تشفير المفتاح العام خوارزم يقوم بتقسيم المفتاح الواحد إلى جزأين. الجزء الأول يكون المفتاح الخاص، والجزء الثاني يتم جعله متاحاً وعاماً. وبواسطة معرفة الجزء العام من المفتاح فقط، نستطيع تشفير الرسالة التي يمكن أن يتم فك شفرتها بواسطة الجزء المكون للمفتاح الخاص. ببساطة، إن معرفة جزء المفتاح العام لا يمكننا من فك الرسالة المشفرة من النص المشفر إلى النص المقروء. إن عملية فك الشفرة، تتطلب معرفة الجزء الخاص من مفتاح التشفير، ويبين شكل5.7 طريقة التشفير باستخدام المفتاح العام.



شكل5.7 يبين عملية التشفير باستخدام المفتاح العام.

وباستخدام طريقة تشفير المفتاح العام، إذا أراد نظام المصدر أن يرسل رسالة مشفرة إلى نظام الهدف، سوف يحتاج معرفة خوارزم التشفير الذي يستخدمه كلا النظامين وكذلك الجزء العام من مفتاح التشفير في نظام الهدف. يقوم المصدر بفك شفرة الرسالة باستخدام الجزء العام من مفتاح تشفير الهدف (بفرض أن المصدر يعرف الجزء العام من مفتاح تشفير الهدف، وإلا سوف يتم إجراء استفسار). يقوم الهدف بفك شفرة الرسالة باستخدام الجزء الخاص من مفتاح التشفير.

نلاحظ مما سبق أنه، عندما يريد النظام تغيير مفتاح التشفير عند أي وقت. فإنه يقوم بتغيير كل من الجزء العام والخاص. ويحتاج تشفير المفتاح الخاص لتوزيع نفس مفتاح التشفير في نفس اللحظة إلى كل من مصدر وهدف يتم حذفه. ومن عيوب نظام التشفير باستخدام المفتاح العام، أن كل نظام يريد أن يرسل نصاً مشفراً إلى الهدف، يجب أولا أن يستفسر عن الجزء العام من مفتاح التشفير في الهدف. أيضا، عند إرسال التشفير في اتجاهين، فإن كل نظام يحتاج معرفة الجزء العام من مفتاح التشفير. يستخدم بروتوكول إدارة الشبكة البسيط (الإصدار الثاني) طريقة التشفير باستخدام المفتاح العام.

4.3.2 ترشيح الحزم

إن العديد من أجهزة الشبكة مثل: الجسور، والمفاتيح، والموجهات، يمكنها تحقيق ترشيح الحزم المبني باستخدام عناوين الوصول لوسط الشبكة MAC (Medium Access Control). إن عملية ترشيح الحزم، توقف الحزم من الوصول إلى الحاسبات المضيفة غير الآمنة، قبل أن تصل إلى نقطة اتصال ربما تحتوي معلومات حساسة. لكن على الرغم من ذلك، فإن هذه الطريقة، ربما تساعد في توفير الأمن، إلا أنها تتعرض لبعض المشاكل.

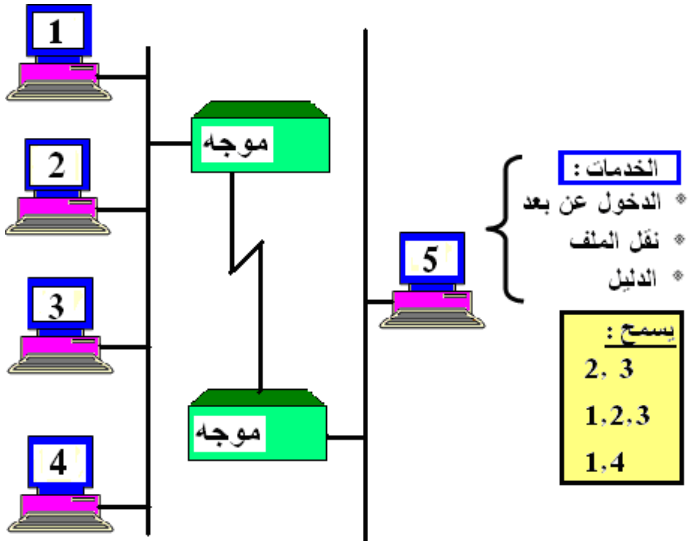
أولا: إن مرشحات الحزم يجب أن تهيئ من خلال كل أجهزة الشبكة. وهكذا لكل عنوان جديد يتم إضافته أو يتم تغييره، سوف نحتاج تغيير المرشحات.

ثانيا: باستخدام مرشح لا يعمل، إذا قام الحاسب المضيف غير الآمن بتغيير العنوان دون أن يخبرنا بذلك.

على سبيل المثال، بفرض أن جسر إثرنيت تقوم بترشيح الحزم بين قطاعات مؤسسة بناء عنوان MAC. بسبب أن عناوين الوصول الشبكية تكون نوعيا مخزنة في شريحة ذاكرة قراءة فقط ROM متواجدة في وحدة مواجهة قنطرة ايثرنيت، فإذا كانت لوحة وحدة المواجهة موضوعة في حاسب مضيف غير آمن، لكي يتم تغييره، فإن اللوحة الجديدة سوف لا تحتوي على نفس عناوين الوصول الشبكية، وأن مرشحات الحزم سوف لا تستطيع على أية حال وقف المعلومات من والى الحاسب المضيف غير الآمن. يمكن أن تنتج هذه المشكلة، ليس فقط بواسطة مستخدمين ماكرين (Devious) ولكن أيضا بواسطة مهندس الشبكة الذي يغير وحدة المواجهة بسبب أن بها عيوباً أو تحتاج إلى تحديث، بدون أن تحقق له اللوحة الجديدة عناوين وصول الشبكية جديدة. يوجد بعض الحاسبات المضيفة توفر معاملات تهيئة برمجية تسمح لمهندس الشبكة بتنصيب عناوين الوصول الشبكية لهم، و احتمال تجنب هذه المشكلة أو جعلها أسهل عندما يريد إحباط (توقيف) مرشح.

5.3.2 توثيق الحاسب المضيف

تسمح طريقة توثيق الحاسب المضيف الوصول إلى الخدمة بناء على عنوان محدد موجود بجهاز حاسب مضيف يعمل كمصدر، وهذا المحدد هو عبارة عن عنوان شبكة شائع مثل الذي يستخدم بواسطة IP، X.25، أو Dec _Net، أو حتى بواسطة عناوين الوصول الشبكية. ويوضح شكل 5.8 مثالاً لتنصيب شائع لتوثيق حاسب مضيف. إن خدمات الحاسب المتعددة، تستخدم نظام توثيق الحاسب المضيف.



شكل5.8 يستخدم الحاسب"5" طريقة تفويض الحاسب المضيف ليقرر الخدمات المسموحة.

مثال1: الحاسب الذي يستخدم بروتوكول X.25:

إن الحاسب الذي يستخدم بروتوكول X.25 في الاتصالات من خلال وصلة توالي، ربما لا يقرر قبول أو رفض المكالمات بناء على عناوين منبع X.121 (نظام تخصيص عناوين). أو ربما لا يسمح لكل حاسب من الوصول إلى الخدمة، بل يسمح فقط لجزء من مجموعة كل احتمالات عناوين شبكة المصدر.

بسبب أن توثيق الحاسب المضيف مؤسس بناء على عناوين الشبكة، فإن العديد من أجهزة الشبكة أيضا تستطيع المساعدة في تحقيق هذه الوظيفة. إذ تستطيع قنطرة

شبكة حلقة توكين (Token Ring) عمل ذلك بواسطة تشغيل ***الوصول المحظور***، للسماح فقط لنظم مصدر معينة لإرسال بيانات إلى أجهزة الحاسب إلى الجانب الآخر من الجسر. تستطيع ***مرشحات الحزم*** أيضا، المساعدة في تحقيق توثيق الحاسب المضيف، على الرغم من أنه لا ينبغي الاعتماد على أن هذه الطريقة هي المثلى لتأمين الحاسب المضيف.

مثال2: نظام إدارة شبكة مركزية:

نفترض نظام إدارة شبكة مركزية، به وحدة عرض ملونة كبيرة، يمكن أن يستخدمها العاملون بالشبكة. على الرغم من أن العديد من المهام يمكن أن يتم تشغيلها بنظام إدارة الشبكة، بواسطة حاسبات متعددة في شبكة البيانات، فإن كل عملية إدارية للشبكة يمكنها عرض نتائجها على وحدة العرض المركزية للنظام. يمكن للنظام المركزي أن يستخدم توثيق الحاسب المضيف، كي يتحقق من أن الحاسب الذي يطلب العرض هو حاسب مضيف مفوض. تستخدم هذه الطريقة نظام النوافذ القياسي الشائع (X11 Window). في هذه الحالة فإن أجهزة الخدمة تستخدم أسماء الحاسب المضيف، التي يتم ترجمتها إلى عناوين الشبكة، لتفويض الحاسبات بالوصول إلى وحدة العرض المحلية. في نظم عديدة، يمكن تحديد الحاسبات المضيفة التي تستطيع استخدام وحدة العرض المحلية، باستخدام بعض أوامر نظم التشغيل (مثل الأمر: <host name> x host).

- **خادمات ملف الحاسب الشخصي:**

تستخدم غالبا خادمات ملف الحاسب الشخصي حاسباً مضيفاً مفوضاً في تحديد الحاسبات التي سوف يسمح لها بالوصول إلى نظم الملف. على سبيل المثال، عندما يتم تشغيل حاسب شخصي بدون قرص تخزين، فإنه ربما يطلب نظام الملف من أي خادم ملفات متاح. إذا كان خادم ملف معين يحتوي معلومات حساسة، فإننا قد لا نرغب أن يتم استخدام نظام الملف هذا من قبل جميع الحاسبات الشخصية. يكون تفويض الحاسب المضيف مفيدا لتوفير الأمن لبعض نقاط الاتصال، ولكنه ليس متقنا.

عندما توجد خدمة على جهاز حاسب توفر اتصال إلى المعلومات الحساسة، فإن معرفة هوية الحاسب المضيف المصدر ربما لا يكون مؤهلا بدرجة كافية لإعطاء هذه المعلومات.

مثال3: استخدام حاسب مضيف مفوض (Authorized):

نفترض حاسباً مضيفاً يسمى"الأمانة"، يوفر الخدمة التي تسمح للموظفين بنسخ البرامج لتستخدم داخل المؤسسة فقط. ولحماية هذه البرامج، فإن حاسب "الأمانة" يستخدم ***حاسباً مضيفاً مفوضاً*** ليسمح فقط لحاسب مضيف آخر يسمى "البريء" للوصول إلى البرامج. لكن نفترض أن أحد المستخدمين قرر نسخ – للاستخدام الشخصي– البرامج الموجودة على حاسب "الأمانة". لإجراء ذلك، فإن المستخدم يستطيع إيقاف تشغيل الحاسب "البريء" ويقوم بتهيئة حاسب يسمى "الماكر" كي يمتلك نفس عنوان الشبكة مثل الحاسب "البريء". بعد ذلك، عندما يقوم الحاسب "الماكر" بالدخول إلى البرامج الموجودة على حاسب "الأمانة"، وبذلك يعمل الحاسب "الماكر" في هذه الحالة كأنه هو حاسب "البريء".

مثال4: طريقة تفويض الحاسب المضيف:

نفترض حاسباً مضيفاً يسمى "السيد" يقدم خدمة تسمح للمستخدمين بتنفيذ البرامج عن بعد، والتي تكون تحت التطوير. وأن هذه البرامج موجودة في الحاسب المضيف "السيد" لا يتم مشاركتها مع كل مستخدم داخل المؤسسة. نستطيع استخدام طريقة الحاسب المفوض للسماح فقط للمستخدمين الموجودين على حاسب مضيف آخر يسمى "الخادم" بتنفيذ هذه البرامج. دعنا نفترض أن مدير نظام حاسب "الخادم" أكد لنا أن الشخص المفوض فقط هو الذي يستطيع الدخول لهذه البرامج الجديدة، وله حسابات على حاسب "الخادم"، ولكنك لم تقتنع. أنت تدرك الآن، أن الاعتماد على طريقة تفويض الحاسب المضيف، تعني أن أي شخص يمتلك طريقة دخول شرعية إلى حاسب "الخادم" يستطيع تنفيذ البرامج الموجودة على حاسب "السيد". بذلك يمكننا

أن نقرر تعزيز الأمن للبرامج الموجودة على حاسب "السيد"، بواسطة اتخاذ إجراء إضافي، مثل توظيف طريقة توثيق المستخدم User Authentication.

6.3.2 توثيق المستخدم

تمكن طريقة توثيق المستخدم خدمة تحديد كل مستخدم قبل أن يسمح لهذا المستخدم من الدخول. إن توثيق المستخدم توفر مدى دقيقاً من التحكم في إعطاء خدمة أكثر من التي توفرها طريقة توثيق الحاسب المضيف، لأنها تسمح لكل خدمة أن تحدد المستخدم بالضبط.

من الطرق الشائعة لتمييز المستخدمين هي استخدام ***كلمة السر***. وعلى الرغم من أنها فعالة، فإن استخدام كلمات السر ليست متقنة، لأنها ليست دائما آمنة، كما نأمل. إن أحد مشاكل استخدام كلمات السر، هي أن بعض خدمات الشبكة تستخدم ***نص واضح*** (Clear Text) يمكن بسهولة أي شخص من اكتشاف كلمة السر، بواسطة الاستيلاء على الحزم البيانية بكل بساطة. أحد حلول هذه المشكلة، هو إرسال كلمات السر ***مشفرة***، ولكن هذه الطريقة تفشل إذا تم كسر مفتاح التشفير.

ويوجد مشكلة أخرى هي أن المستخدمين يميلون إلى جعل كلمات السر سهلة التذكر، وهذا يعني أنه يمكن كشفها بسهولة. غالبا، إن كلمات السر التي يتم اختيارها تكون كلمات شائعة، يمكن اكتشافها من خلال محاولات تكرارية. الحل البديل هو توفير كلمات سر لا تستخدم كلمات شائعة، إما بواسطة توليد كلمات السر ***عشوائيا***، أو بواسطة تضمينها حروفاً خاصة أو أرقاماً. على الرغم من أن إجراء كهذا، يمكن أن يجعلها صعبة التذكر، إلا أنه ينتج عن ذلك أن يقوم المستخدمون بكتابتها عادة قرب الحاسب المضيف. وعلى الرغم من هذه العيوب، فإن كلمات السر ما تزال تستخدم تكرارا في توثيق المستخدمين. وأن على مهندس الشبكة ببساطة معرفة نقاط الضعف وإجراء الحماية حولها.

خادم ومولد كلمة السر لمرة واحدة:

يوجد عامل آخر متعلق باستخدام كلمات السر، وهو تخصيص خادم كلمة السر، ومولد كلمة السر لمرة واحدة (One Time Password Generator). إن خادم كلمة السر هو نظام يستطيع توثيق المستخدم، باستخدام قاعدة بيانات بها أسماء المستخدمين، وكلمات السر الخاصة بهم. يقوم مولد كلمة السر لمرة واحدة، بتوليد كلمات السر للمستخدم. وهو عبارة عن جهاز صغير متصل بوحدة مفاتيح يحتفظ به المستخدم. وتوجد طرق متعددة في خادم كلمة السر، لمعرفة كلمات السر الصحيحة لمستخدم معين، بعضها بواسطة تتبع كلمات السر الصحيحة، والبعض الآخر يعتمد على فترات تزامن بين مولد كلمة السر لمرة واحدة وخادم كلمة السر.

إن المستخدم الذي يريد الحصول على كلمة سر لمرة واحدة يتبع الخطوات التالية:

- إنشاء جلسة في نظام الهدف.
- إدخال مفتاح مميز إلى مولد كلمة السر، الذي يشغل المفتاح من خلال خوارزم لإنتاج كلمة السر.
- كتابة كلمة السر ذي المرة الواحدة.

بعد ذلك يتم إرسال كلمة السر ذي المرة الواحدة مع اسم المستخدم إلى خادم كلمة السر من أجل التوثيق. وتتميز طريقة كلمة السر مرة واحدة، بأنه إذا قام أحد الأشخاص الماكرين بالاستيلاء على كلمة السر أثناء انتقالها عبر الشبكة، فإن الاتصال المتعاقب لمستخدم كلمة السر سوف لا يوفر توثيقاً صحيحاً للمستخدم. والميزة الأخرى في هذه الطريقة أن المستخدم من غير المحتمل أن يكتب كلمة السر، لأنها فقط مفيدة لتوثيق واحد فقط. العيب الواضح لهذا النظام، أنه يحتاج من المستخدم أن يحمل مولد كلمة السر وأن يقوم بإدخال المفتاح إليه في كل مرة يحتاج فيها التوثيق.

- **بروتوكول تاكاكس TACACS:**

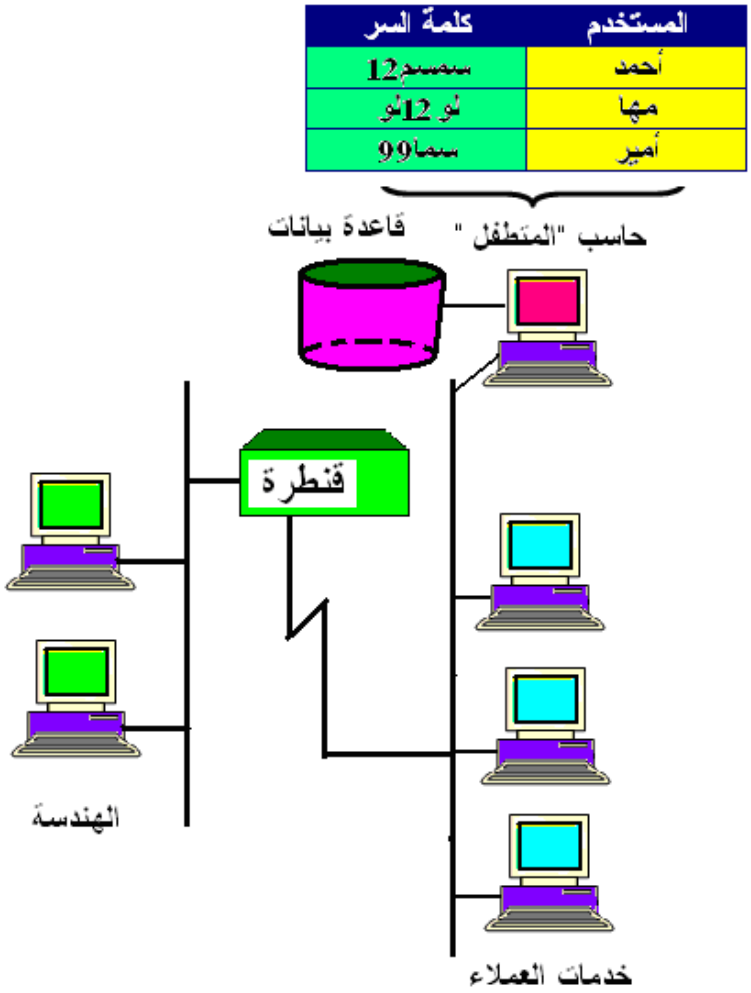
عزيزي الدارس، من أمثلة البروتوكولات القياسية التي تحدد طريقة الاتصال بين نظام الهدف وخادم كلمة السر التي يتم تنفيذها، هو بروتوكول TACACS (Terminal Access Controller Access Control System)، ومعناه: محكم الاتصال الطرفي لنظام تحكم الوصول. وهو ***بروتوكول مفوض عن بعد*** يستخدم للاتصال بالخادم المفوض لتحديد سماحية دخول العميل إلى شبكة البيانات. وهو عبارة عن برنامج، يوجد منه إصدار حديث يطلق عليه مسمى +TACACS، وهو يستخدم عادة في شبكات البيانات التي تعمل بنظام التشغيل يونيكس.

في المثال الذي تم شرحه سابقا، باستخدام حاسب "السيد" وحاسب "الخادم"، لتوضيح كيفية تنصيب إدارة أمن فعال. فبدلا من السماح لكل مستخدم له حساب على "الخادم" بالوصول إلى البرامج الموجودة على حاسب "السيد"، يمكننا فقط استخدام الخدمة التي تمكن الوصول إلى هذه البرامج مع حساب صحيح على "السيد". بهذه الترتيبات، ولتشغيل البرامج من "السيد"، فإن المستخدم، أولاً ينبغي أن يبدأ بأستخدام حاسب مفوض، وثانياً أن يدخل كلمة سر فريدة (Unique).

مثال: خدمة عميل مفوض من خلال كلمات سرية:

نفترض حاسباً يسمى "المتطفل"، يقدم الخدمة التي تسمح للمستخدمين الدخول إلى قاعدة بيانات تتكون من معلومات عملاء مؤسسة، كما هو موضح في شكل5.7. يسمح فقط للموظفين العاملين في قسم خدمة العملاء للمؤسسة المفوضين بالدخول إلى هذه المعلومات الحساسة. وتبعا لذلك، عندما يحتاج بعض وكلاء خدمة العميل بعض المعلومات عن العملاء، فهي تستخدم برنامجاً موجوداً على حاسباتهم الشخصية متصل بالحاسب "المتطفل". على الرغم من ذلك، قبل أن يقوم الحاسب "المتطفل" بإعطاء المعلومات للوكيل، تقوم قاعدة البيانات بسؤال الوكيل عن كلمة السر التي تحدد أن المستخدم مفوض له استخدام قاعدة البيانات. وبذلك لا يسمح لكل مستخدم

جهاز حاسب، في مكتب وكالة خدمة عميل، بأن يستطيع طلب معلومات عن العملاء.



شكل5.9 يوضح أن الخدمات التي توفرها قاعدة بيانات حاسب"المتطفل" تتطلب عميل مفوض من خلال كلمات سرية.

وعلى الرغم من أن طريقة ***توثيق المستخدم*** بوجه عام أكثر فاعلية من طريقة ***توثيق الحاسب المضيف*** الذي يعمل بمفرده، إلا أن لها عيباً مميزاً. تقريبا فإن كل طرق

توثيق المستخدم تعتمد على التهيئة السليمة لجهاز الحاسب. من الواضح، أنه إذا قام الحاسب بتوفير توثيق المستخدم من أجل الخدمة، وجعل كلمة السر هي نفسها لكل مستخدم، فإن الأمن المطلوب لا يتم تحقيقه.

- **دمج عمليتي توثيق المستخدم وتوثيق الحاسب المضيف:**

إن دمج عمليتي توثيق المستخدم، وتوثيق الحاسب المضيف معا يوفر وسيلة أكثر فاعلية لتأمين نقط اتصال أحسن من استخدام طريقة واحدة منهما فقط. لتوضيح ذلك، نعود إلى مثال الحاسب "المتطفل". تم التخطيط على أن يتم إعطاء كل مستخدم كلمة سر لتوثيق المستخدم. لكن هل ذلك سوف يوفر لنا كل الأمن الذي نحتاجه؟ إن أي مستخدم معه حاسب شخصي وكلمة سر وحساب في قاعدة البيانات يستطيع الوصول إلى المعلومات الحساسة من خلال الحاسب "المتطفل". لتحسين الأمن، نريد تطبيق كلا من توثيق الحاسب المضيف، وتوثيق المستخدم في هذه الخدمة. إن هذه الطريقة ***ذات المستويين*** سوف تكفل أن كلاً من المستخدمين الذين يطلبون الخدمة يأتوا فقط من حاسبات مضيفة مفوضة وأنهم مستخدمون مفوضون.

7.3.2 توثيق المفتاح

يوفر نظام توثيق المفتاح وسيلة لتحقيق كلا من توثيق الحاسب المضيف، وتوثيق المستخدم مع إضافة ميزة دون الاعتماد مطلقا على حاسب الهدف المضيف. وتعمل طريقة توثيق المفتاح بواسطة تخصيص حاسب مضيف على الشبكة يسمى ***خادم المفتاح*** A Key Server .

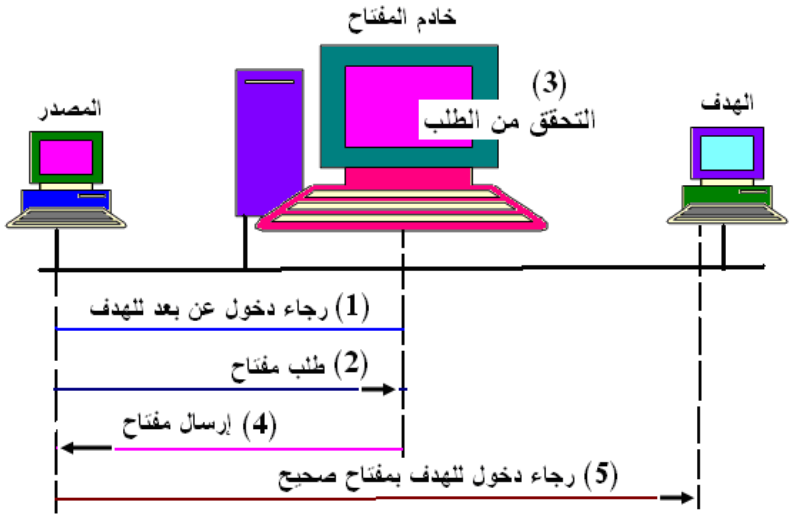
يكون خادم المفتاح مسئولا عن إصدار المفاتيح إلى المستخدمين المفوضين. عندما يتم طلب خدمة، فإن حاسب المصدر يسأل خادم المفتاح عن المفتاح. بعد ذلك، ربما يمتلك خادم المفتاح نوع المستخدم داخل كلمة السر للتفويض. والآن يستطيع خادم المفتاح تحديد كلاً من حاسب المصدر والمستخدم طالب الخدمة. بناء على هذه

البيانات وعلى قواعد الأمن المخزنة داخل خادم المفتاح، فإن الخادم ربما يصدر مفتاحاً صحيحاً.

إن هذا النظام يعمل بسبب أن حاسب الهدف سوف يسمح بالخدمة فقط عندما يكون طلب الدخول مصحوبا بالمفتاح الصحيح. في بعض خادمات تفويض المفتاح تكون المفاتيح الصحيحة غير متاحة في فترات الاستراحة. ويمكن أن يسبب ذلك توقيف جلسة المستخدم، ولكنه أيضا يضمن أن المفتاح الصحيح المنفرد لا يسمح بدخول غير مقنن. كما نرى، بسبب أن خادم المفتاح يقوم بتفويض المستخدم، ويمنع الدخول إلى الخدمات، فإنه يحتاج أن يكون تحت أمن فعلي قوي.

- **مثال: عملية طلب الدخول عن بعد باستخدام توثيق المفتاح:**

يمكن أن تعمل عملية طلب الدخول عن بعد باستخدام توثيق المفتاح، كما هو موضح في شكل5.10 كما يلي:



شكل5.10 يوضح عينة من الخدمة التي يمكن طلبها بواسطة مفتاح التوثيق.

- يقوم حاسب المنبع بطلب رجاء خدمة الدخول عن بعد إلى الحاسب الهدف.
- تقوم عملية الدخول عن بعد بطلب رجاء مفتاح من خادم المفتاح الذي يسمح للمستخدم بالدخول إلى حاسب الهدف.

- يقوم خادم المفتاح بالتحقق من حاسب المصدر، وضمان أن المستخدم مفوض، لاستخدام خدمة الدخول عن بعد للحاسب الهدف.
- عندما يتم فحص كل شيء، يقوم خادم المفتاح بإصدار مفتاح صحيح للحاسب المصدر من أجل الدخول عن بعد إلى حاسب الهدف.
- يتم إرسال المفتاح الصحيح إلى حاسب المصدر.
- يقوم حاسب المصدر بطلب رجاء خدمة الدخول عن بعد إلى حاسب الهدف بواسطة المفتاح الصحيح.

في **طريقة توثيق المفتاح**، يكون خادم المفتاح حرجا للاحتفاظ بتأمين نقاط الاتصال الخاصة بخدمات شبكة البيانات. من المهم أيضا، أن تتم إدارة وتهيئة خادم المفتاح بشكل صحيح. لكي تعمل طريقة توثيق المفتاح، فإن كل خدمة على حاسب المصدر يجب أن تطلب مفتاحاً من خادم المفتاح، قبل بدء العملية. بالإضافة إلى أن الخدمات في حاسب الهدف يجب أن تقبل طلبات الخدمة فقط عندما يصاحب هذه الطلبات المفتاح الصحيح. ويعني ذلك أننا لا نستطيع تنصيب خادم المفتاح وأن نبدأ استخدام توثيق المفتاح ببساطة. يجب أن تتغير وتتهيأ كل التطبيقات والخدمات لاستخدام خادم المفتاح. لقد أصبحت طريقة توثيق المفتاح أكثر شيوعا وخاصة في حاسبات يونيكس. كما يوجد العديد من الموردين توفرون أشكالاً من نظم توثيق المفتاح.

2.4 المحافظة على نقاط اتصال آمنة

تعتبر عملية الصيانة هي الخطوة الأخيرة للحصول على نقاط اتصال شبكة آمنة وفعالة. كما تعلمنا سابقا، إن الاحتفاظ بمعايير أمن حديثة وآمنة في شبكة البيانات مهمة صعبة وتتطلب التزام المؤسسة بتوفير كل من المصادر والوقت. من مهام مهندس الشبكة الحفاظ على الشبكة، بصرف النظر عن كيفية التخطيط والبناء، فعندما تنتهي تكملة مهمة نظام الأمن، فإن الصيانة وتعديل الشبكة سوف يكون مطلبا. إن المبدأ الرئيسي للصيانة هو تحديد مكان الإجهاد أو اختراق الأمن الفعلي. في بعض

الحالات ربما يتم عمل ذلك بواسطة المهندسين المسئولين عن فحص أمن الشبكة. فهم قد يستخدمون مثلا نقاط اتصال الشبكة كأساس للفحص، والتي يقوم مهندس الشبكة بتوثيقها وإجراء الأمن المطلوب لها. لسوء الحظ، فإن حفظ هذه الوثائق وتحديثها باستخدام وفرة برامج الشبكة المتاحة في الأسواق يكون مهمة أخرى كبيرة. لذلك في مثل هذه الحالات، فإن أحسن ما يأمله فاحصو الشبكة هو فهم المسائل المتعلقة بإدارة الأمن والخطوط الإرشادية للمؤسسة المتعلقة بذلك.

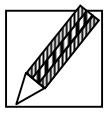
- **برامج محاولات اختراق أمن الشبكة:**

عزيزي الدارس، في حالات أخري، فإن مهندسي الشبكة ربما يوظفوا برامج على الحاسبات المضيفة لفحص مشاكل الأمن المعروفة والشائعة. يمكن للبرامج البسيطة محاولة اختراق الأمن بواسطة محاولة كسر كلمات السر ومفتاح الشفرة بطريقة عشوائية. يمكن للبرامج الأكثر دقة أن تشن هجوما على الشبكة والحاسبات بعدة طرق مختلفة. في كلا الحالتين، فإن كل برنامج سوف يخبر مهندس الشبكة عن نجاحه أو فشله في اختراق الأمن. إن المنطق وراء ذلك أنه، إذا استطاع أحد البرامج كسر معيار الأمن، فإن آخراً سوف يكون قادرا على تحقيق نفس العمل. إن ميزة هذه الطريقة أن المشاكل الموجودة بواسطة برنامج تمكن مهندس الشبكة من غلق نقط الاتصال المتأثرة، ومن الأفضل أن يتم ذلك قبل أن يتم إيجادها ونشرها بواسطة مستخدمين غير مفوضين. ويوجد العديد من الأمثلة لهذه البرامج متاحة في الأسواق، ويمكن أن يتم الاستفسار عنها من موردي نظم الحاسبات لمعرفة أي من هذه البرامج يمكن توظيفها.

ويوجد طريقة أخرى غير عادية، تمت محاولتها بواسطة بعض المؤسسات الأكثر جرأة. حيث تقدم المؤسسة عرضا على الشبكة العامة بجوائز نقدية إذا استطاع أحد من الناس إثبات أنه استطاع اقتحام شبكة المؤسسة، ويوضح الكيفية. على الرغم من أن هذه الطريقة تبدوا عنيفة نوعا ما، فإنها تساعد على ضمان عملية الأمن بواسطة مساعدة مهندسين الشبكة في تحديد أماكن اختراق الأمن. لسوء الحظ، فإن الطرق

التي تم شرحها هنا لا تضمن أن الأمن سوف يتم المحافظة عليه بشكل صحيح. إن الفحص لا يمكن أن يتحقق كل يوم. إن البرامج التي تستخدم في فحص الأمن لا يمكنها فحص كل ثغرة ممكنة. إن مهندسي الشبكة عليهم أن تفهموا معايير الأمن في المكان، وأن يبذلوا مجهودا في تبليغ المؤسسة بإجراء اللازم والمساعدة في صيانته.

تدريب (2)



عرف المصلحات الآتية :

استخدام الحاسبات المضيفة المفوضة: (Authorized Remote Hosts)

نظام ملفات الشبكة NFS(Network File System):

عناوين الوصول لوسط الشبكة MAC (Medium Access Control).

نظام التشفير القياسي DES(Data Encryption Standard):

مولد كلمة السر لمرة واحدة (One Time Password Generator)

3. الاتصال بالشبكة العامة

عزيزي الدارس، تم في الجزء السابق، وصف الخطوات الخاصة بتحقيق إدارة الأمن للخدمات على الحاسب المضيف. إن المؤسسة التي تمتلك شبكة بيانات غير متصلة بالشبكة العامة قد تجد أن هذه الخطوات سوف توفر الأمن اللازم. لكن في المؤسسة التي بها شبكة بيانات متصلة بالشبكة العامة، فإن تحقيق إدارة الأمن يتطلب طريقة مختلفة. ويوجد ثلاثة أنواع ممكنة لتوصيل شبكة البيانات العامة بشبكة بيانات المؤسسة، وهي:

- لا يوجد اتصال.
- اتصال كامل.
- اتصال محدود.

إن شبكة البيانات الخاصة التي تسمح بعدم توصيل الدخول عن بعد، من شبكة البيانات العامة ربما تستخدم ببساطة توصيلته إلى الشبكة العامة كوسيلة لإرسال واستقبال البريد الإلكتروني. على سبيل المثال، ربما يتحقق الاتصال كل بضع ساعات قليلة من خلال جهاز مودم لغرض إرسال واستقبال بريد إلكتروني من شبكة البيانات العامة. وتكون كل العمليات مع شبكة البيانات العامة يتم بدؤها من خلال شبكة بيانات المؤسسة. بهذه الطريقة، فإن المؤسسة لا تحتاج إلى أن تجد نقاط اتصال بشبكة البيانات العامة، بسبب أنه لا يوجد مثل هذه النقاط.

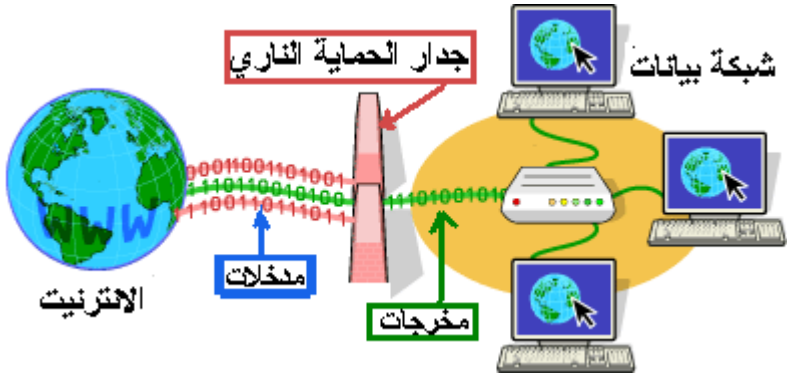
على العكس من ذلك، عندما لا تضع المؤسسة أية محاذير على العمليات بين حاسباتها وشبكة البيانات العامة، فإن كل إدارة أمن يجب أن تحفظ في كل حاسب منفرد موجود داخل المؤسسة. في هذا التركيب، ربما تسمح المؤسسة لأي بيانات أن تدخل شبكتها وأن تعتمد على الحاسبات في توفير توثيق الحاسب المضيف أو توثيق المستخدم قبل إطلاق المعلومات الحساسة.

لكن، بفرض أن المؤسسة تريد إدخال بعض الخدمات من الشبكة العامة، أو عرض بعضها إلى الشبكة العامة، لكن لا يوجد حاسب مضيف، أو مستخدم مفوض على معظم حاسباتها. من الواضح أن فتح شبكة بيانات المؤسسة وتوصيلها بالشبكة العامة، في مثل هذه الحالة سوف يؤدي إلى مخاطر أمنية. إن طريقة التوصيل المحدودة تستطيع مساعدة ونفع الاهتمامات الأمنية في هذه الحالة.

- **الجدار الناري Firewall:**

يتضمن الوصول محدود السماح فقط لمجموعة صغيرة مفوضة من الحاسبات المضيفة لتوفير الخدمة بين شبكة المؤسسة والشبكة العامة. يتم وضع مجموعة من نظم الحاسبات أو أجهزة الشبكة بين شبكة المؤسسة والشبكة العامة لتدعيم إدارة

الأمن، وهذه الطريقة تسمى بناء جدار ناري (Firewall)، ويبين شكل5.11 مثالاً يوضح استخدام جدار حماية ناري بين شبكة بيانات مؤسسة وشبكة الانترنت. وتمكن طريقة استخدام الجدار الناري مهندس الشبكة من التحكم في كل حاسب يوفر خدمة إلى شبكة البيانات العامة. وبذلك يتم تحديد الخدمات المتاحة للشبكة العامة ويوفر نقاط اتصال آمنة بطريقة أحسن لشبكة المؤسسة.

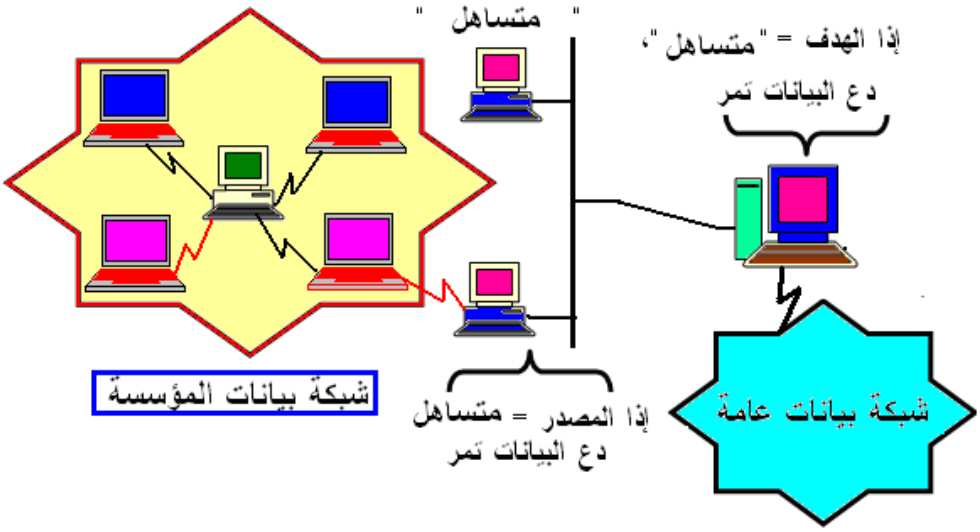


شكل5.11 استخدام جدار الحماية الناري في ترشيح المدخلات لحماية المستخدم والشبكة من القرصنة.

إن جدار الحماية الناري هو عبارة عن طريقة لدمج خصائص إدارة الأمن لسلسة من أجهزة الشبكة تم تصميمها بحيث تسمح فقط لمعلومات معينة بالمرور من مكان لآخر. في هذه الحالة فإن الجدار الناري سوف يسمح فقط لبيانات معينة من الشبكة العامة كي تمر خلال الشبكة الخاصة. ويتم بناء الجدار الناري عادة بواسطة استخدام أجهزة موجهات تقوم بتوفير مستوى شبكي لترشيح الحزم بواسطة استخدام حاسبات تعمل كبوابات سريعة Gateways تتحكم في تدفق البيانات بين التطبيقات.

مثال: ضبط التهيئة للسماح بوصول مقنن:

نفترض أن مؤسسة بها شبكة بيانات متصل بها جهاز حاسب يسمى "متساهل"، وهو عبارة عن تطبيق لبوابة طريق داخل الجدار الناري. يعمل النظام الأمني على ضمان أن أي بيانات خاصة بشبكة المؤسسة يجب أولاً أن ترسل إلى الحاسب "متساهل"، كما هو موضح في شكل 5.12 .



شكل5.12 ضبط التهيئة للسماح بوصول مقنن
من شبكة بيانات المؤسسة إلى شبكة البيانات العامة.

إن الرابط بين قطاع الشبكة– الذي يستخدم الحاسب "متساهل"– يوجد في الشبكة العامة ويتم من خلال جهاز الشبكة مثل الجسر أو الموجه. ويجب تهيئة هذا الجهاز ليسمح بحركة مرور من الحاسب "متساهل" فقط بواسطة ***مرشحات الحزم***. يجب تركيب مرشحات الحزم بحيث إن كل الحزم تدخل عن طريق الشبكة العامة ويكون لها عنوان هدف للحاسب"متساهل".

وباستخدام هذه التقنيات، نستطيع تمكين المؤسسة أن تستخدم الشبكة العامة، دون خوف من تعرض المعلومات الحساسة لمستخدمين غير مفوضين موجودين في شبكة البيانات العامة. لاحظ أن الحاسب المضيف المفوض الذي تم شرحه في هذا المثال سوف يعمل، طالما لم يتم عن طريق الخطأ، تخصيص نفس عنوان الشبكة المخصص للحاسب"متساهل" لحاسب آخر. ويمكن تجنب ذلك بواسطة تخصيص رقم شبكي للحاسب"متساهل" يختلف عن الرقم الذي يستخدم مع باقي حاسبات المؤسسة.

4. تحقيق نظام الأمن في نظام إدارة الشبكة

كما تم توضيحه، فإن إدارة الأمن تمكن مهندس الشبكة من حماية المعلومات الحساسة بواسطة تحديد وصول المستخدم إلى الحاسب المضيف، ومصادر الشبكة، وكذلك بواسطة تبليغ المهندس عن محاولات اختراق الأمن. يتم تحقيق إدارة الأمن في نظام إدارة الشبكة باستخدام أدوات برمجية. وحسب كيفية دقة الأداة المستخدمة والمتاحة لمهندس الشبكة، يتم الحكم على جودة النظام.

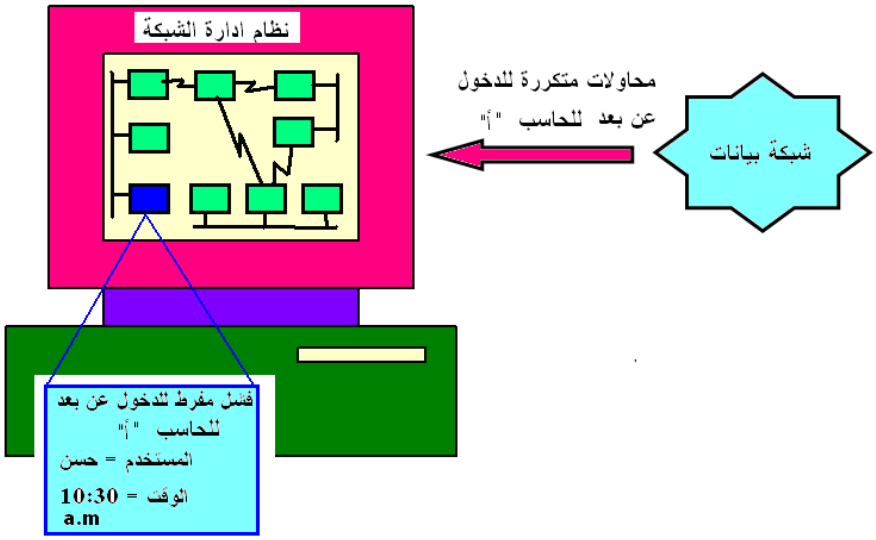
1.4 استخدام الأداة البسيطة لإدارة الأمن

إن الأداة البسيطة التي تستخدم لإنجاز إدارة الأمن في نظام إدارة الشبكة، تحتاج أن تظهر الأماكن التي يتم فيها تنصيب معايير الأمن. بالاعتماد على الدخل من خريطة الشبكة الرسومية، فإن هذه الأداة تستطيع إنشاء شاشة تظهر كل معايير الأمن المطبقة في أي جهاز حاسب مضيف لمستخدم يتم اختياره. بالإضافة إلى تحديد كل الأماكن المحددة لعناوين شبكية أو مستخدم معين في الشبكة. إن الأداة ينبغي أن تكون قادرة على الاستفسار من قاعدة بيانات التهيئة، وإنشاء نافذة لعرض المعلومات الضرورية. كما تستطيع أداة الأمن استخدام معلومات إدارة التهيئة الموجودة في نظام إدارة الشبكة، في حل مشاكل التوصيل المعقدة الموجودة في الشبكة.

تقوم الأداة البسيطة بالاستفسار من قاعدة البيانات العلاقية في نظام إدارة الشبكة، عن تهيئة جهاز تم اختياره من خلال خريطة الشبكة. إذا لم توفر برامج إدارة الأمن في نظام إدارة الشبكة، إمكانية تحقيق خصائص الأمن واستخدامها بواسطة الأداة البسيطة، فإن مهندس الشبكة يستطيع استخدام الأداة لرؤية أجزاء من تهيئة الأجهزة، ويقوم هو بإجراء وتشغيل خصائص الأمن المتاحة يدويا.

2.4 استخدام الأداة المركبة لإدارة أمن الشبكة

يكون للأداة المركبة القدرة على إجراء تطبيقات في الزمن الفعلي، ورصد اتصال المعلومات الحساسة. بعد تحديد مشكلة الأمن المحتملة، فإن هذا التطبيق يستطيع تغيير ألوان الحاسبات المضيفة المتأثرة أو أجهزة الشبكة في خريطة الشبكة الرسومية. أو إذا توفر عدد كبير من الألوان لأحداث مختلفة (ويصبح الأمر مربكا)؛ فإن الأداة تستطيع تدوين ما تم الحصول عليه بوسائل أخرى، مثل قرع جرس النظام (تنبيه صوتي)، أو الدفع بإظهار نافذة على شاشة نظام إدارة الشبكة، تبين ما تم الحصول عليه، كما هو موضح في شكل 5.13 .



شكل5.13 تطبيق إدارة الأمن في الزمن الفعلي، لتدوين محاولات عديدة غير ناجحة من أجل الوصول إلى خدمة الدخول عن بعد للحاسب"أ".

يستطيع مهندس الشبكة، بواسطة استخدام بروتوكول إدارة الشبكة، الاستفسار عن الأجهزة، لمجموعة من حوادث الأمن تم تسجيلها. تستطيع الأداة المركبة أن تجري عملية تصويت (Polling) لطلب هذه المعلومات بشكل دوري(مرة كل ساعة يكون كافيا في معظم الحالات)، وفحص العلاقات بين هذه الأحداث.

على سبيل المثال، يستطيع التطبيق تدوين العملية التي قد يقوم فيها أحد المستخدمين بمحاولات عديدة غير ناجحة، للدخول عن بعد إلى جهاز الحاسب. يمكن إجراء عملية التدوين بطريقتين:

الطريقة الأولى: تعتمد على ذكاء الحاسب بخصوص تدوين الأحداث، فإذا استطاع إرسال الحوادث، المتعلقة بمحاولات الدخول غير الناجحة، إلى نظام إدارة الشبكة، فهذا يعتبر مثاليا.

الطريقة الثانية: إن تطبيق إدارة الأمن، سوف يحتاج بعض الذكاء لفحص ملفات سجل الحاسب المتعلقة بالمحاولات الفاشلة للدخول عن بعد. (تقوم حاسبات عديدة بتسجيل محاولات الدخول في ملف أو سجل إزالة (Audit Trail)، يتم فحصه بعد ذلك). من عيوب هذه الطريقة أنها تحتاج كتابة تطبيق إدارة الأمن بحيث يفحص الأشكال المحددة للملف.

يمكن تطوير هذا التطبيق أكثر، بحيث يستطيع إنشاء معلومات أكثر فائدة، مثل تدوين محاولات إنكار المستخدم من الوصول إلى خدمة معينة، أو الوصول إلى ملف يحتوي معلومات حساسة. ويتم توليد هذا التقرير بطريقة مشابهة للتي تم شرحها سابقا.

- **العلامات الزمنية (Time Stamps):**

يمكن استخدام بعض الحيل الشائعة، لإيجاد ملف تم الوصول إليه، بأن تفحص الأداة العلامات الزمنية في الملف. سوف تبين العلامات الزمنية، في كثير من نظم التشغيل، متى تم إنشاء الملف ومتى تم تعديله آخر مرة.

يمكن تصميم الأداة المركبة أيضا، بحيث تبلغنا عندما يقوم مستخدم غير مفوض، أو محاولات حاسب مضيف، من الوصول إلى الخدمة التي يكون بها نقط اتصال بالمعلومات الحساسة. بإجراء ذلك، فإن الأداة تستطيع أن ترشدنا إلى التهيئة التي يحتاجها الحاسب المضيف. على سبيل المثال، نفترض أن مستخدماً على أحد الحاسبات الشخصية، يطلب خدمة ملف من خادم الحسابات الذي يحتوى معلومات

حساسة. فإن المستخدم لن يحصل على خدمة الملف في خادم الحسابات، ولكن من خادم محلي آخر. وربما أن المستخدم لا يعرف التهيئة اللازمة لإيقاف الحاسب من طلب الخدمات المتاحة على الشبكة. إن هذه الأداة، تقوم برصد وصول الخدمة في خادم الحسابات، وتستطيع ليس فقط بتقديم النصيحة لنا، عن المحاولات المضللة للحصول على الاتصال، ولكن أيضا بتنبيهنا بسوء التهيئة (Misconfiguration).

- **بناء قيود أمنية:**

يمكن للأداة المركبة الآن، إظهار الاهتمامات الأمنية إلى انتباهنا، كما يمكنها أيضا المساعدة في بناء قيود أمنية (Security Restrictions) عند نقاط معينة داخل الشبكة. لتحقيق ذلك، نقوم أولا بتحديد نقطة (أو موضع) في شبكة البيانات، وبعد ذلك نزود الأداة بالدخل عن المستخدمين وعناوين الشبكة المسموحة والممنوعة من المرور بهذه النقطة أو الموضع. بعد ذلك، سوف تقوم الأداة ببناء المرشحات المناسبة، أو إجراء المعايير اللازمة لتنفيذ العمل المطلوب. وأخيرا، تقوم الأداة بطلب التأكيد –من خلالنا– على تنفيذ العملية برمتها.

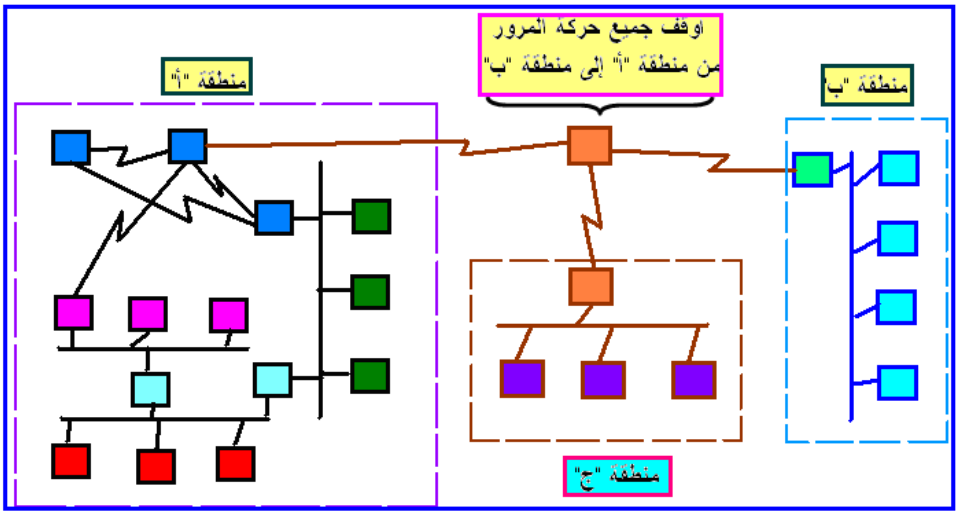
على الرغم من أن المهام المطلوب أن تؤديها هذه الأداة، ليست صعبة، فإنها تحتاج بعض الدقة في إنشاء مثل هذا التطبيق، وذلك بسبب أن كل جهاز شبكة أو حاسب مضيف يكون له طريقة منفردة في تطبيق معايير الأمن (Security Measures). تحتاج الأداة المركبة أولا أن تستفسر عن الحاسب المضيف أو الجهاز في المكان المطلوب تطبيق الأمن عنده، بعد ذلك تستفسر من المستخدم عن المعلومات المستولى عليها. على سبيل المثال، تكون عملية تطبيق الأمن في تحديد مرور عناوين الشبكة، مختلفة تماما عندما يتم تحقيقها على جهاز أو مكرر (Repeater)، أو جسر أو حاسب مقدمة ومؤخرة، أو موجه. بالإضافة إلى أنه لكل جهاز مصنع، يمكن أن يأخذ التطبيق الأمني شكلا مختلفا تماما.

3.4 استخدام الأداة المتقدمة لإدارة أمن الشبكة

تستطيع الأداة المتقدمة تجميع البيانات عن نماذج حركة المرور، لإرشادنا حول الأمن المفروض إجراؤه. وتحتاج إدارة الأمن التام هذه الوظيفة، بالإضافة إلى الخصائص الخاصة بكل من الأداة البسيطة والمركبة. يمكن للأداة المتقدمة فحص نوع الأمن الذي ننوي تنصيبه على الحاسب أو الجهاز، وتنبهنا إلى المحاذير الممكنة عن هذه التنصيبات. يمكن للأداة أن تستقبل مدخلاً من طرفنا، بالإضافة إلى إعطائنا بيانات تاريخية لإجراء تحليلات كاملة عن كيفية تأثير معيار أمني معين على حركة مرور الشبكة.

مثال: توقيف حركة مرور البيانات في الشبكة:

نفترض أننا نخطط لتنصيب نظام مرشح حزمي لإيقاف حركة مرور البيانات بين منطقتين في شبكة البيانات هما أ، ب كما هو مبين في شكل5.14. سوف تقوم الأداة بتحليل نماذج حركة المرور بين المنطقتين أ، ب في الشبكة. بعد ذلك تخبرنا بأن الخطة الأمنية يمكنها وقف 85% من حركة المرور بين المنطقتين أ، ب في الشبكة. إن هذه النسبة من المعدل الفعال ربما تمثل التأثير الذي نريده في النظام. بغض النظر، عن إن الأداة المتقدمة سوف تقوم إما بتعزيز جهودنا، أو بتحذيرنا حول سوء التهيئة.



شكل5.14 يستطيع تطبيق إدارة الأمن، إخبار مهندس الشبكة المعني المتضمن لتشغيل الأمن، كي يوقف جميع حركة المرور بين المنطقتين "أ"، "ب".

تحتاج الأداة المتقدمة أن تعمل بالقرب من معلومات إدارة الأداء المخزنة في قاعدة البيانات في نظام إدارة الشبكة، لإيجاد حركة المرور الكلية بين المنطقتين أ، ب في الشبكة. وينبغي أن تقيم البيانات بدلالة نماذج الحركة، بعد ذلك تنفذ التحليلات اللازمة عن الأمن المقترح.

- **رصد الشبكة عن بعد:**

يمكن استخدام بروتوكول "رصد الشبكة عن بعد" RMON (Remote Network Monitoring) كمجس (Probe) يستطيع تجميع المعلومات حول مصفوفة حركة مرور البيانات بين المصدر والهدف لعناوين الوصول الشبكية. عندما نريد وضع أمن عناوين الوصول الشبكية، فإن هذه المعلومات يمكن تحليلها بسهولة كي تؤدى وظيفة الأداة المتقدمة. مع ذلك، إذا أردنا تنصيب مرشح حزمي مركب في عناوين مستوى الشبكة وأنواع التطبيق، فإن معلومات RMON ربما لا تؤدي الوظيفة.

- **حسابات نماذج حركة مرور البيانات عبر الشبكة:**

توجد بعض التقنيات البرمجية من قبل شركات موردة، تستطيع إجراء حسابات نماذج حركة مرور البيانات عبر الشبكة. تسمح هذه التقنيات النوعية لجهاز الشبكة أن يحسب عدد حزم البيانات والحروف المرسلة بين نظامين في كل مستوى شبكي للبروتوكول المستخدم (مثل بروتوكول IP، بروتوكول IPX). إذا استطاعت الأداة المتقدمة تحديد الجهاز الذي يطبق معايير الأمن، أن به هذه الخصائص، فتستطيع هي الاستفسار عن هذه المعلومات من قاعدة بيانات نظام إدارة الشبكة.

- **تحليل مرشحات الحزم:**

إن المشكلة الأخرى المتعلقة بتنفيذ الأداة المتقدمة، هي عملية تحليل مرشحات الحزم المقترحة المصاحبة لأجهزة الشبكة. إن كل شركة موردة لجهاز، يوجد لها طريقة منفردة لتهيئة مرشحات الحزم، وهذا يجعل أداة تحليل هذه المرشحات الحزمية مهمة صعبة. وتوجد بعض التطبيقات في إدارة الشبكة، بها خصائص لتحليل مرشحات الحزم. ولكن هذه التحليلات ليست مخصصة عادة لفحص حركة نماذج البيانات، وتكون هذه ضرورية ولو لإنشاء إصدار محدود للأداة المتقدمة.

5. تدوين حوادث الأمن في الشبكة

إن سجلات الفحص التي تلخص تدوين معلومات الأمن تكون حرجة في تحقيق إدارة الأمن. لكن بمعاونة التطبيقات التي تجري عمليات الإدخال في سجل الفحص، نستطيع تحديد النماذج (Patterns) التي تبين تهديد نقاط الاتصال، ومن ثم توقيف الاتصالات غير المسموحة. أيضا، مثلما يحدث في تطبيقات الوقت الفعلي، فإن مثل هذه البيانات يمكن أن تساعدنا في إيجاد الطلبات الغير مسموحة التي تنتج عن سوء التهيئة.

مثال: الاحتياطات الأمنية عندما يغادر مسئول إدارة الشبكة المؤسسة:

نفترض أن مهندس الشبكة، المسئول عن إدارة وتهيئة شبكة البيانات يخطط لمغادرة المؤسسة من أجل العمل في مؤسسة منافسة أخرى.

الخطوة الأولى: للتعامل مع هذا الوضع، تكون بإزاحة هذا الشخص فورا من الوصول الفعلي إلى مباني المؤسسة، أو أي مكان يمكنه فعليا الوصول إلى المعلومات الحساسة. وهذه الخطوة قد تحتاج تغيير شفرات المفتاح وتغيير مفاتيح بطاقة الدخول.

الخطوة الثانية: هي إزاحة حسابات هذا الشخص من جميع نظم الحاسب. وبحسب الاعتماد على اتصالات الموظف السابقة، فإن هذه الخطوة يجب أن تتضمن أيضا تغيير كلمات السر ذات الامتياز (مثل: أصل المصدر (Root)، المشرف (Supervisor)، مدير النظام System Manager) في جميع نظم الحاسبات، وأجهزة الشبكة.

الخطوة الثالثة: ينبغي أن يتم تغيير كلمات السر، وشفرات المفاتيح في كل أجهزة الشبكة التي توصل المؤسسة إلى الشبكة العامة (أو تلك التي يمكن أن توصل إلى العالم الخارجي)، مثل جميع أجهزة المودم، أجهزة الشبكة، والحاسبات المضيفة في نظام الجدار الناري.

الخطوة الرابعة: يمكن تنصيب أداة إدارة الأمن، لمراقبة كل الأجهزة المتصلة بشبكة البيانات، عن الأماكن التي يستطيع الموظف السابق الدخول من خلالها.

الخطوة الخامسة:_ يمكن أن يتم تشغيل برنامج يتم تصميمه للبحث في الملفات أو التطبيقات التي ربما قام بتغييرها الموظف السابق، لإنشاء ثغرة أمنية في المستقبل. إن البحث عن ملفات تنفيذية أو ملفات قد تم تغييرها حديثا، هي مهمة يمكن تحقيقها، بواسطة برامج عديدة كجزء من عمل إدارة النظم (على الرغم من أنها ليست طريقة سهلة تماما في جميع الحالات).

1.5 سجلات فحص الأمن

إن المبدأ الرئيسي لضمان إزالة آمنة في شبكة البيانات، يكون بواسطة عمل سجلات فحص مكثفة، وإجراء عمليات توضع في أماكن لرصد الشبكة. في هذا الوضع، فإن سجل فحص الأمن (على ما يبدو في نظام إدارة الشبكة) يكون مهما أيضا. إن إنشاء تطبيق يمكن أن ينشيء سجل فحص، ليس صعبا، حيث يوفر كل تطبيق إدارة أمن الذي يجد محاولات اختراق تدخل نتائج البحث في قاعدة بيانات نظام إدارة الشبكة.
على سبيل المثال، إن التطبيق الذي يكتشف محاولات عديدة غير ناجحة للدخول عن بعد، يستطيع إضافة مدخل إلى قاعدة البيانات عندما يتم تنبيه مهندس الشبكة عن المشكلة. يمكن بعد ذلك، أن تقوم قاعدة البيانات بتوليد تقارير ملخصة. على الرغم من أن هذه التطبيقات يمكن إتمامها ببساطة نسبيا، باستخدام بناء نظام معماري صحيح لإدارة الشبكة، فإنه لا يجب المبالغة في فوائدها.

مثال: تقرير عن محاولات غير صحيحة لنقل ملفات من شبكة مؤسسة:

نفترض عينة من تقرير يومي كما هو موضح في جدول5.1، والذي يوضح كيف يستطيع تطبيق إدارة الأمن، إحضار بيانات مفيدة لمهندس الشبكة. يحدد الجدول اثنين من أغلبية نقاط الاتصال، والمحاولات غير ال صحيحة لنقل ملفات من أحد شبكات المؤسسة، التي وجدت في هذا اليوم، وحاسب المصدر، واسم المستخدم عندما فشلت المحاولة (إذا كان متاحا)، والوقت الذي وقع فيه الحدث. كما يبين جدول5.2 محاولات غير صحيحة لدخول شبكة المؤسسة عن بعد.

جدول5.1: محاولات غير صحيحة **لنقل ملفات** من شبكة مؤسسة.

(ملخص الأمن يوم 5 يناير 2007 ميلادي)

التدوين بواسطة	حاسب المصدر	المستخدم	الوقت
شبكة الأمن	قسم التسويق	حسن	09:10
شبكة التسويق	قسم الوثائق	كريم	10:20
شبكة المكتبة	قسم الهندسة	سمير	12:30

جدول5.2: محاولات غير صحيحة **للدخول عن بعد** لشبكة المؤسسة.

(ملخص الأمن يوم 5 يناير 2007 ميلادي)

التدوين بواسطة	حاسب المصدر	المستخدم	الوقت
شبكة التدريب	قسم الرياضيات	أكرم	15:10
شبكة العلوم	قسم الحاسبات	إسلام	16:00
شبكة المكتبة	قسم الفلك	أمجد	02:30

يمكن إجراء تطبيقات مماثلة تنتج بيانات ذات صلة لفترات أطول (أسبوع أو شهر)، وهذه التطبيقات تكون أيضا حرجة، بالنسبة لإدارة الأمن في نظام إدارة الشبكة. بإجراء مراجعة منتظمة، فإن هذه التقارير يمكن أن تساعد مهندس الشبكة، في الاحتفاظ بأمن الشبكة، وأن يكون على وعي ودراية باحتمالات اختراقات أمنية فعلية.

6. برامج تطبيقية لأمن الشبكة

يوجد حزم برمجية متعددة متوفرة على شبكة الانترنيت يمكن للمؤسسات التي تمتلك شبكات بيانات شراؤها وتنصيبها لتحقيق إدارة أمن الشبكات في المؤسسة كما تم شرحه سابقا. نقدم، في هذا الجزء من الوحدة الدراسية، بعض البرامج المتاحة مجانا على شبكة الانترنيت، التي يمكن للدارس تنصيبها والتدرب عليها وذلك لإكساب الدارس المهارات اللازمة التي تعينه وتمكنه من استخدام بعض وسائل أمن الشبكات والحماية من المخاطر.

وأن يتدرب الدارس على كيفية استخدام هذه البرامج لحماية ملفات العملاء على أجهزة الحاسبات المتصلة بشبكة البيانات. ونعرض هنا مجموعة من أشهر هذه البرامج التطبيقية التي يمكن للدارس أن يقوم بتحميلها من عناوين مواقع شبكة الانترنيت الموضحة تباعا ومن ثم تنصيبها والتدرب عليها. وهذه البرامج مهمة جدا للحماية من مخاطر الفيروسات المدمرة وكذلك من قراصنة الحاسبات.

وتشمل هذه البرامج التطبيقية ما يلي:

1- برامج الحماية من مخاطر الفيروسات وتشمل:

(I) AVG Anti-Virus:
www.grisoft.com/
(II) Norton Anti-Virus:
www.freedownloadscenter.com/Utilities/Anti-Virus_Utilities/Norton_AntiVirus.

2- برامج الحماية من القراصنة بواسطة بناء جدار حماية ناري وتشمل:

(I) *Shield Firewall:*
www.download3000.com/download-Shield_Firewall_2005-count-reg-9171.html
(II) ZoneAlarm Firewall:
www.zonealarm.com/store/content/company/products/znalm/freeDownload.

3- برامج تشفير الملفات: من قبل المستخدمين غير المفوضين.

(I) *Kryptel:*
www.freedownloadscenter.com/Utilities/File_Encryption_Utilities/Kryptel.html
(II) Kryptel Lite:
www.freedownloadscenter.com/Utilities/File_Encryption_Utilities/Kryptel_Lite.html
www.bluesofts.com/download/295/2824/Kryptel.html

4- برامج فك الملفات المشفرة: ويتم ذلك من قبل المستخدمين المفوضين.

(I) *Silver Key:*
www.cleansofts.com/get/35/17527/Silver_Key.html
www.softpedia.com/get/Security/Encrypting/Silver-Key.shtml
www.softjamboree.com/download-Silver-Key.html
(II) DES encryption:
www.pdf995.com/
3d2f.com/tags/storing/triple/des/encryption/data/
www.canadiancontent.net/tech/downloads/Encryption-Software-page-3.
www.canadiancontent.net/tech/downloads/Encryption-Software-page-3.html
www.codec-download.com/misc.-business/crypteon-des-encryption-2308-29.html
www.freedownloadscenter.com/Programming/Components_and_Libraries/CryptoTools.html

5- بعض برامج التشفير باستخدام المفتاح الخاص:

Private Key Encryption:
www.investintech.com/resources/articles/publicprivatekey/
www.instantssl.com/code-signing
QuickCrypt Library symmetric (private-key) encryption algorithms: DES
www.sharewareconnection.com/quickcrypt-library.htm

6- بعض برامج التشفير باستخدام المفتاح العام:

(I) Public Key Authentication:

www.enginsite.com/ssh-webdav-ftp-sftp-client.htm
MDaemon: www.3d2f.com/programs/5-885-mdaemon-download.shtml

Deltacrypt OneClick Public key encryption:
www.freedownloadscenter.com/.../File_Encryption_Utilities/Deltacrypt_OneClick_Public_key_encryption.html
Advanced Encryption Package Public-Private Key:
(II) RSA Public Key Encryption:
www.bytefusion.com/products/ens/cryptoanywhere/rsapublickeyencryption.htm
www.investintech.com/resources/articles/publicprivatekey
www.bytefusion.com/products/ens/cryptoanywhere/rsapublickeyencryption.htm
(III) Key Encryption:
www. shareme.com/showtop/freeware/key-encryption.

7- بعض برامج توثيق المستخدم: لضمان وصوله للمعلومات الحساسة.

user authentication:
www.brothersoft.com/downloads/user-authentication.html
www.hotscripts.com/PHP/Scripts_and_Programs/User_Authentication/index.html

الخلاصة

عزيزي الدارس، تعرفنا في هذه الوحدة على فوائد إدارة الأمن التي تحققت من خلال تحديد المعلومات الحساسة وإيجاد نقط الاتصال ثم من خلال تأمين نقاط الاتصال والحفاظ علي نقاط الاتصال .

ثم حددنا أدوات إدارة الأمن الأدوات البسيطة والمركبة والمتقدمة لإدارة الأمن من خلال التعرف علي أمن الحاسوب وأمن المستخدم، ثم أمن المفتاح السري. وقد تم تناول تقارير حوادث الامن والتعرف على مميزات سجلات الفحص من تدوين حوادث الأمن في الشبكة .

لمحة مسبقة عن الوحدة القادمة

عزيزي الدارس في الوحدة القادمة سنشرح عملية **فوائد إدارة الأداء وكيفية** تحقيق إدارة الأداء ومجالاتها الرئيسية كماسنوضح كيفية تحليل بيانات الشبكة وضبط القيم الحدية **ثم** استخدام محاكاة الشبكة والمحاكي **وسنتناول** إدارة الأداء في نظام إدارة الشبكة **و**وسائل الإدارة البسيطة والمركبة والمتقدمة عن الطرق والإجراءات التي تتعلق بهذه العملية.

كن معنا في الوحدة القادمة وستجد الكثير المفيد إن شاء الله .

مسرد المصطلحات

استخدام الحاسبات المضيفة المفوضة: (Authorized Remote Hosts)
تمكن المستخدم من الوصول إلى بيانات محددة بعيدة بعد أن يدخل أولا عن بعد إلى الحاسبات المضيفة المفوضة، ويوثق إذن الدخول بواسطة كلمة السر .

- **نظام ملفات الشبكة (Network File System)NFS:**

يسمح نظام ملفات الشبكة الموجود في أنواع مختلفة عديدة لأجهزة الحاسب، لأحد أجهزة الحاسب من الوصول إلى ملفات نظام آخر كما لو أنه موجود على الحاسب المحلى باستخدام شبكة البيانات .

عناوين الوصول لوسط الشبكة (Medium Access Control) MAC.
توقف الحزم من الوصول إلى الحاسبات المضيفة غير الآمنة، قبل أن تصل إلى نقطة اتصال ربما تحتوي معلومات حساسة.

- **نظام التشفير القياسي** (Data Encryption Standard)DES:

نظام التشفير القياسي هو أحد نظم التشفير الشائعة التي تستخدم المفتاح الخاص. وباستخدام DES يتم تشفير النص المقروء باستخدام قطاعات حزمية طولها 64 بيت. عند نظام المصدر .

مولد كلمة السر لمرة واحدة (One Time Password Generator)
هو نظام يستطيع توثيق المستخدم، باستخدام قاعدة بيانات بها أسماء المستخدمين، وكلمات السر الخاصة بهم. يقوم بتوليد كلمات السر للمستخدم. وهو عبارة عن جهاز صغير متصل بوحدة مفاتيح يحتفظ به المستخدم

المصطلح بالإنجليزية	معناه بالعربية
Audit Trail	سجل إزالة
Anonymous	طريقة غير رسمية
Authorized	المفوضون
Authorized Remote Hosts	حاسبات مضيفة مفوضة
Ciphertext	النص المشفر
Clear Text	نص واضح
Crackers	مخترفون
Domains	مجالات
Domain Names	أسماء المجال
DES (Data Encryption Standard	نظام التشفير القياسي
Firewall	جدار ناري
FTP(File Transfer Protocol)	بروتوكول نقل الملفات
Gateways	بوابات سريعة
Guest	ضيف
Key Server	الخادم الرئيسي
Misconfiguration	سوء التهيئة
MAC (Medium Access Control)	التحكم بوسط الدخول
Patterns	نماذج
Passwords	كلمات سر
Plaintext	المعلومات المقروءة

المصطلح بالإنجليزية	معناه بالعربية
Private Key	مفتاح الخاص
Probe	مجس
Polling	تصويت
Public Key	المفتاح العام
Process Status: ps	أمر تنفيذ حالة العملية
Unique	فريد
Network File NFS(System)	نظام ملفات الشبكة
NetBIOS	نظام الدخل والخرج الأساسي للشبكة
One Time Password Generator	مولد كلمة السر لمرة واحدة
User Authentication	توثيق المستخدم
TCP/IP	بروتوكول التحكم في النقل
TACACS (Terminal Access Controller Access Control System)	محكم الاتصال الطرفي لنظام تحكم الوصول
Time Stamps	علامات زمنية
RMON (Remote Network Monitoring)	رصد الشبكة عن بعد
Real Time	الوقت الحقيقى
Repeater	المكرر
Security Management	إدارة الأمن
Security Breach	اختراق الأمن
Segments	مقاطع

المصطلح بالإنجليزية	معناه بالعربية
Security Measures	معايير الأمن
Security Restrictions	قيود أمنية
Supervisor	المشرف
System Manager	مدير النظام
X11 Window	نظام النوافذ القياسي الشائع
ZIP (Zone Information Protocol)	بروتوكول معلومات المنطقة

المراجع

[1] Duane De Capite, Self-Defending Networks: The Next Generation of Network Security (Networking Technology: Security), Cisco Press, 2006.

[2] Dale Tesch, Greg Abelar, Security Threat Mitigation and Response: Understanding Cisco Security MARS (Networking Technology), Cisco Press, 2006.

[3] Harold F. Tipton , Micki Krause, Information Security Management Handbook, Fifth Edition, Publisher: AUERBACH, 2003

[4] Sean Convery, Network Security Architectures, Publisher: Cisco Press, 2004

[5] Merike Kaeo , Designing Network Security, Cisco press, 2003.

[6] Alexander Clemm, Network Management Fundamentals, Cisco Press, 2006.

[7] Florent Parent, Oliver Steudler, Jaques Allison, Managing Cisco Network Security, Syngress, 2000.

[8] Moshe Rozenblit, Security for Telecommunications Network Management, Wiley-IEEE Press; 1st Edition ,2006.

[9] Sean Convery, Network Security Architectures, Cisco Press, 2005.

[10] Gert De Laet, Gert Schauwers, Network Security Fundamentals, 2004.

[11] Saadat Malik, Network Security Principles and Practices, Cisco Press, 2002.

[12] Allan Leinwand, Network Management - A Practical Perspective, 1999.

[13] Patrick T.Lane, Network Management, Sybex publish, 2004.

[14] Roberta Bragg, CISSP Certified Information Systems Security Professional, Published by Exam Cram, 2004.

[15] Mani Subramanian, Network Management, Principles and Practice, Addison-Wesley, 1999.

[16] Stephen B. Morris, Network Management, MIBs and MPLS: Principles, Design and Implementation, Prentice Hall, 2003.

[17] William Stallings, Cryptography and Network Security, 2nd Edition, 2007. [17] Robert B. Reinhardt, An Architectural Overview of UNIX Network Security, 2002.

[18] Cryptography and Network Security, McGraw Hill, www.tatmcgrawhill.com/digital_solution/kahate


الوحدة السادسة
إدارة الأداء

محتويات الوحدة

المقدمة

تمهيد

عزيزي الدارس مرحبا بك الى هذه الوحدة والتي بعنوان إدارة الأداء.

تختص إدارة الأداء بضمان أن الخط السريع للشبكة يظل غير مزدحم، ويمكن الوصول إليه. ويتم تحقيق ذلك من خلال:

- رصد أجهزة الشبكة والوصلات المصاحبة لها لتحديد معدل الاستخدام Utilization ، ومعدلات الخطأ Error Rates.
- مساعدة الشبكة في توفير مستوى خدمة متناسقة إلى المستخدمين، بضمان أن سعة الأجهزة والوصلات ليست مرهقة إلى حد غير ملائم يؤثر على الأداء. لتحقيق إدارة الأداء يتم تتبع الخطوات التالية:تجميع بيانات عن معدل الاستخدام الحالي لأجهزة الشبكة والوصلات.وتجميع البيانات ذات الصلة لتبيان اتجاه معدل الاستخدام المرتفع ثم ضبط حدود معدل الاستخدام وأخيرا استخدام المحاكاة Simulation لتحديد كيفية تعديل الشبكة للحصول على أقصي أداء.

في هذه الوحدة ، سوف يتم شرح فوائد إدارة الأداء، ومناقشة الخطوات الأربعة الخاصة بتحقيق هذه الفوائد. بعد ذلك، يتم وصف ثلاثة أدوات لإدارة الأداء، ويشمل ذلك الأداة البسيطة، والمركبة والمتقدمة. وأخيرا سوف نشرح طرق تدوين معلومات إدارة الأداء.

أهلا بك مرة أخرى إلى هذه الوحدة عسى أن تنتفع بها وأن تفيد منها ، وأن تساعدنا في نقدها وتطويرها .

أهداف الوحدة

عزيزي الدارس، بعد فراغك من دراسة هذه الوحـــدة ينبغـــي أن تكون قادرا علي أن :

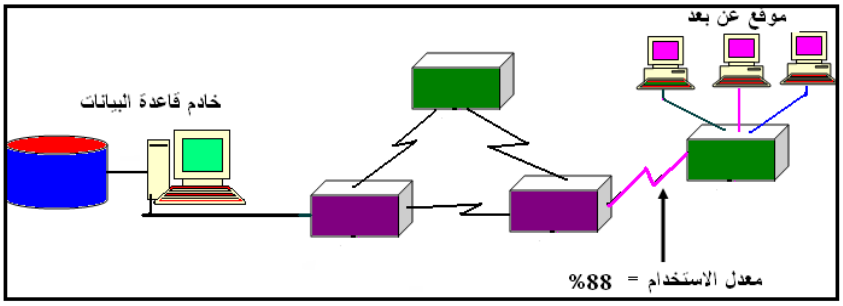
- تعدد وظائف إدارة الأداء في نظام إدارة الشبكات.
- تسرد خطوات تحقيق إدارة الأداء في إدارة شبكات البيانات.
- تتعلم كيفية حساب معدلات استخدام وصلات وأجهزة الشبكة.
- تصف كيفية قياس مستوي الخدمة بواسطة إدارة الأداء.
- تحسب زمن الاستجابة، ومعدل الرفض، والإتاحة للشبكة.
- تحلل بيانات أداء الشبكة باستخدام الرسومات البيانية المتنوعة.
- تضبط القيم الحدية والتأهيلية لتحسين أداء الشبكة.
- تعرف وظائف محاكاة الشبكة في قياس الأداء ووظيفة محاكي الشبكة.
- تفحص أداء الشبكة بالأدوات البسيطة والمركبة والمتقدمة.
- تشرح بعض الطرق المستخدمة لتدوين بيانات الأداء ويقارن بينها.
- تتدرب على بعض البرامج المستخدمة عمليا لقياس أداء الشبكات.

1. فوائد إدارة الأداء

إن الفائدة الأساسية لإدارة الأداء هي أنها تساعد مهندس الشبكة في تقليل الازدحام المكتظ والمتعذر بلوغه لتوفير مستوى خدمة متناسق للمستخدمين. يستطيع مهندس الشب99 –55ة، باستخدام إدارة الأداء، أن يرصد معدل استخدام أجهزة الشبكة والوصلات. وتستطيع هذه البيانات أيضا مساعدة المهندس في تحديد اتجاهات معدل الاستخدام، وعزل مشاكل الأداء، ومن الممكن حتى حل هذه المشكلة قبل أن تنعكس بطريقة غير ملائمة على أداء الشبكة. بهذه الطريقة تستطيع إدارة الأداء أيضا المساعدة في تخطيط سعة الشبكة.

- **رصد معدل الاستخدام:**

تمثل عملية رصد معدل الاستخدام الحالي لأجهزة الشبكة والوصلات نقطة حرجة في إدارة الأداء. تستطيع البيانات التي يتم الحصول عليها معاونتنا في عزل مكونات شبكة البيانات التي استخدمت بكثافة في الحال، كما تساعدنا أيضا في إيجاد أجوبة لمشاكل الإجهاد الأخرى، وربما يعتبر ذلك الأكثر أهمية. على سبيل المثال، في الشبكة الموضحة في شكل 6.1، يشتكي المستخدمين من بطيء الاتصال عن بعد إلى خادم قاعدة البيانات الذي قد ينتج من أسباب متعددة. قد تقع هذه المشكلة في أي جهاز أو وصلة من المصدر إلى الهدف. تستطيع إدارة الأداء مساعدتنا بسرعة في تحديد وصلة بين الموقع البعيد وخادم قاعدة البيانات التي يكون معدل استخدامها فوق 80%، وهذا من المحتمل أن يكون هو سبب بطء الاتصال.



شكل6.1 يسبب معدل الاستخدام المرتفع للوصلة، بطء وصول البيانات من الموقع البعيد إلى خادم قاعدة البيانات.

- **فحص اتجاهات بيانات الشبكة:**

تستطيع تقنيات إدارة الأداء مساعدتنا في فحص اتجاهات الشبكة. نستطيع استخدام اتجاه البيانات للتنبؤ بالقيمة العظمي لمعدل استخدام الشبكة. وبالتالي نتجنب الأداء الضعيف الذي يمكن أن ينتج عن تشبع الشبكة. على سبيل المثال، إذا علمنا متوسط زمن الاستجابة بين الوحدة الطرفية لمستخدم والحاسب الكبير Mainframe ، نستطيع تنصيب إجراءات تجعلنا نعرف متى يكون زمن الاستجابة أطول من اللازم. سوف نتعلم من خلال دراسة هذه الوحدة، أن أجهزة وتطبيقات إدارة الشبكة، يمكن تنصيبها لإرسال تنبيهات عندما يوجد مشكلة أداء محتملة، أو عندما يتم اجتياز حد معرف لمستخدم.

يستطيع بروتوكول رصد الشبكة عن بعد RMON، تجميع معلومات عن قطاع الشبكة في الزمن الفعلي، ويختبر البيانات عند جدول فترات زمنية (ربما كل خمسة دقائق)، ويخزن البيانات التاريخية من أجل استرجاعها فيما بعد بواسطة نظام إدارة الشبكة. وهذه الإمكانية لجهاز رصد الشبكة عن بعد RMON ، هي أحد الأمثلة علي استخدام بيانات الشبكة في الزمن الفعلي من أجل اتجاه تحليلي طويل الأجل.

- **رسم معدل الاستخدام للشبكة مقابل الزمن:**

نستطيع أيضا، رسم معدل الاستخدام للشبكة مقابل الزمن، وذلك لتحديد أوقات ذروة الاستخدام. وبمعرفة ذلك، نستطيع جدولة نقل البيانات الضخمة إلى أوقات عدم الازدحام. في كثير من شبكات البيانات، يقوم المستخدمين بجدولة انتقالات البيانات

الضخمة إلى أوقات يكون عندها؛ على ما يبدو؛ استخدام الشبكة منخفض، مثلا عند منتصف الليل أو وقت تناول الغذاء. على الرغم من أن عدد قليل من المستخدمين ربما تلاحظ وجود مشكلة في هذا التوقيت، فإن استعمال الشبكة يمكن أن يصل في الحقيقة إلى معدل استخدام عالي وعادل بعد ذلك.

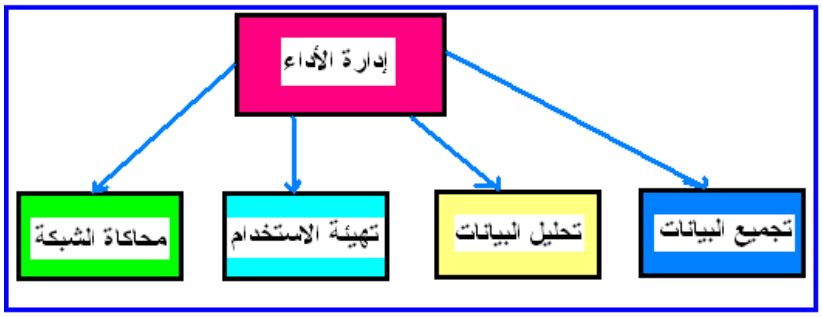
- **تخطيط السعة Capacity Planning:**

يفيد تخطيط السعة كل من المستخدمين ومهندس الشبكة. باستخدام معلومات إدارة الأداء، يستطيع مهندس الشبكة تحديد السعة الحالية للشبكة بواسطة استخدام بروتوكول إدارة الشبكة لتجميع معلومات عن كل الحروف المرسلة والمستقبلة في الوحدة البينية للشبكة. ويعطي إجمالي عدد هذه الحروف حجم الشبكة Network Volume . وعند إجراء هذه العملية، ينبغي تجنب عدم عد نفس البيانات مرتين. في مثل هذه الحالة، يمكن إجراء عملية عد الحروف عند أماكن يكون فيها حركة مرور البيانات متزنة عند نقاط وصول منفردة للهدف (أو الأهداف Destinations). وبعد معرفة السعة الحالية للشبكة، نستطيع تحديد كيفية تأثير إضافة حركة البيانات على الشبكة برمتها.

2. تحقيق إدارة الأداء

تتضمن إدارة الأداء، كما هو مبين في شكل6.2، أربعة خطوات هي كما يلي:

1- تجميع البيانات حول معدل الاستخدام الحالي لأجهزة ووصلات الشبكة.
2- تحليل البيانات ذات الصلة.
3- تهيئة حدود الاستخدام.
4- محاكاة الشبكة.



شكل6.2 الوظائف الواجب تحقيقها بواسطة إدارة الأداء.

1.2 تجميع بيانات معدلات الاستخدام

إن تحديد معدل استخدام جهاز الشبكة ليس عادة مهمة مباشرة، إن كل نوع جهاز ربما يكون له خصائص مختلفة تحدد الاستخدام. على الرغم من أننا نوفر بعض معايير الاستخدام الشائعة، ينبغي علينا العمل مع مورد الأجهزة. على سبيل المثال، إن **معدل استخدام خادم الملفات** ربما من المفضل أن يتم قياسه بواسطة تحميل المعالج، ومعدل الوصول للقرص، ومعدل استخدام كارت الوحدة البينية للشبكة. إن المعالج المشغول ربما يحقق مهام بطيئة للمستخدم، إن القرص الذي يتم الاتصال به باستمرار ربما يقرأ ويكتب ملفات جديدة أكثر بطأ من المطلوب، وأن كارت وحدة بينية مشغول للشبكة ربما يبطئ الوصول إلى الشبكة.

يمكن قياس **معدل الاستخدام لجهاز موجه أو قنطرة** بواسطة معدل تدفق الحزم، حمل المعالج Processor Load، نسبة الأطر Frames المرسلة لكل وحدة بينية، وعدد الحزم المخزنة في الانتظار. إن هذه الأجهزة من الأفضل أن يتم قياسها بواسطة فحص معدلات الإرسال مقابل مقدرتها علي الإرسال في حوار شبكي معطى، بسبب أن هذه الأجهزة يمكنها معالجة الأطر بسرعة أعلى من التي تستطيع توفيرها الوصلات المصاحبة.

إن **معالج الشبكة** عالي التحميل، يبين لمهندس الشبكة أن الجهاز يكون له زمن توقف Idle Time ضئيل. إن الاحتفاظ بمعالج الجهاز مشغولا لا يسبب عادة مشكلة، إلي أن

يصبح الجهاز مشغولا 100% من الوقت ولا يستطيع الاستمرار في معالجة حركة مرور الشبكة. في هذه الحالة، فإن معدل الاستخدام المرتفع لهذا الجهاز ينتج عنه حذف حزم البيانات، وهذا يجبر نظام المصدر على إعادة إرسالها (ومن المحتمل أن يجعل مشكلة الأداء أسوأ). إذا كان الجهاز يستطيع معالجة الحزم ولكنه يحتاج تخزينها في طابور انتظار، فإن هذا أيضا يؤثر على الأداء الكلي للشبكة. إن الجهاز الذي ينتظر عند وصلة شبكة ذات استخدام مكثف، أو وصلة بها عديد من الأخطاء، أو جهاز شبكة آخر، يعاني مشاكل في الأداء.

ويمكن **تحديد معدل استخدام الوصلة** في الشبكة بطريق أسهل ، على الرغم من أن الوصلة ربما لا تستخدم بنسبة 100%، فإن نسبة أقل من معدل استخدام الوصلة ربما يسبب مشاكل في الأداء. على سبيل المثال، تستطيع شبكة إثيرنيت احتواء حركة مرور بيانات بمعدلات استخدام عالية جدا، لكن إذا زاد حمل حركة البيانات العادية 40%، فإن القطاع ربما يسبب أداء رديء وسيء.

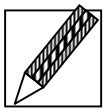
إن معدل استخدام الوصلة هو عبارة عن مجموع كمية المعلومات المرسلة في الثانية والمستقبلة في الثانية مقسومة علي سعة النطاق الكلية المتاحة (التي تكون أيضا بوحدة معلومات في الثانية).

$$\text{نسبة معدل الاستخدام} = \frac{(\text{إجمالي عدد المعلومات المرسلة} + \text{إجمالي عدد المعلومات المستقبلة})}{\text{سعة النطاق}}$$

إن هذه المعادلة لا تستخدم لوصلات التوالي ذات الإرسال في الاتجاهين Full Duplex ، التي تستطيع إرسال واستقبال معدل نطاق الإرسال الكامل في كلا الاتجاهين في نفس الوقت. وهذا يعني أن معدل الاستخدام يستطيع حساب 200%. لهذا ينبغي أن نستخدم المعادلة التالية بدلا من المعادلة السابقة، والتي تحدد القيمة العظمي للمعلومات المرسلة في الثانية والمعلومات المستقبلة في الثانية كما يلي:-

$$\text{نسبة معدل الاستخدام} = \frac{\text{القيمة العظمى/إجمالي عدد المعلومات المرسلة ، إجمالي عدد المعلومات المستقبلة/}}{\text{سعة النطاق}}$$

تدريب(1)



أجب بلا أو نعم

1) لتحقيق إدارة أداء شبكة البيانات نضبط حدود معدل استخدام أجهزة الشبكة والوصلات
2) لتحقيق إدارة أداء شبكة البيانات تجميع البيانات ذات الصلة بمعدل الاستخدام المرتفع.
3) تتميز فوائد إدارة الشبكة بمساعدة مهندس الشبكة في تقليل الازدحام المكتظ في الشبكة.
4) تتميز فوائد إدارة الشبكة بتوفير مستوى خدمة متناسق للمستخدمين.
5) تتميز فوائد إدارة الشبكة برصد معدل استخدام أجهزة ووصلات الشبكة.

- **قياس مستوى الخدمة في الشبكة:**

لقياس مستوي الخدمة في الشبكة، نحتاج تحديد قيم المعاملات التالية:

أولا:- إجمالي زمن الاستجابة Response Time .

ثانيا:- معدل الرفض Rejection Rate.

ثالث:- الإتاحة Availability.

أولا: إجمالي زمن الاستجابة:

يعرف إجمالي زمن الاستجابة بأنه الفترة الزمنية التي تأخذها معلومة استدلالية Datum كي تدخل الشبكة ويتم معالجتها إلي أن يتم الاستجابة وتترك الشبكة. علي سبيل المثال، يمكن قياس إجمالي زمن الاستجابة لجلسة دخول عن بعد، من لحظة أن يقوم المستخدم بكتابة أول حرف من وحدة المفاتيح إلي لحظة انتقال المعلومة إلي حاسب الهدف بالشبكة وعودة الاستجابة إلى الوحدة الطرفية المحلية للحاسب المصدر.

إن العديد من بروتوكولات طبقة النقل، مثل بروتوكول التحكم في الإرسال القياسي بين الشبكات TCP، يمكن أن تقيس زمن دورة الرحلة Round-Trip Time بالملي ثانية لكل معلومة استدلالية ترسل من المصدر إلي الهدف لأغراض التحكم في التدفق. يمكن أن تستخدم هذه القيمة للحصول علي قيمة تقريبية جيدة لإجمالي زمن الاستجابة. إن الفترة الزمنية لدورة الرحلة سوف لا تطابق تماما الفترة الزمنية الإجمالية لزمن الاستجابة، بسبب أن مستوي النقل في الشبكة يستقبل المعلومة الاستدلالية قبل أن يقوم التطبيق بمعالجتها، وأن عملية معالجة التطبيق سوف تضيف وقتا إضافيا. بغض النظر، فإن زمن الرحلة يمثل جزء مهم من إجمالي زمن الاستجابة.

ثانيا: معدل الرفض:

يعرف معدل الرفض بأنه النسبة المئوية للزمن الذي لا تستطيع فيه الشبكة نقل المعلومات، بسبب نقص في المصادر وفي الأداء. لقياس معدل الرفض، يوجد العديد من الأجهزة تسجل عدد المحاولات لإجراء اتصال ، وإجمالي عدد الاتصالات التي تمت ، ونحصل علي النسبة المئوية لمعدل الرفض بواسطة قسمة عدد الاتصالات التي تمت على إجمالي عدد محاولات الاتصال. في حالات كثيرة، عندما تكون قيمة معدل الرفض أكثر من 2% فإن هذه القيمة تمثل حالة مميزة.

ثالثا: الإتاحة:

تعرف الإتاحة بأنها النسبة المئوية للزمن الذي يتم فيه الوصول للشبكة وتكون جاهزة للعمل. وهي تقاس غالبا بالمتوسط الزمني بين الإخفاق MTBF(Mean Time

Between Failure) . وكذلك متوسط زمن اللازم للإصلاح MTTR، و تبين المعادلة التالية طريقة حساب الإتاحة (A):

$$A = \frac{MTBF}{MTBF + MTTR}$$

و يمكن قياس الإتاحة من الناحية النظرية، حيث أن معظم موردين الأجهزة تقوم بتوفير قيم لهذه القياسات. من الناحية العملية، فإن معظم موردين الأجهزة تستطيع أن تخبرنا عن المدة التي تستطيع فيها هذه الأجهزة أن تظل في العمل (العمر الافتراضي للجهاز). بمقارنة هذه القيمة، بالمدة الزمنية الكلية المنقضية منذ كان الجهاز أو الوصلة في الخدمة، يعطينا قيمة الإتاحة. ويوضح الجدول 6.1، أمثلة عددية لحساب قيمة الإتاحة بمعلومية كلا من MTBF، وقيمة MTTR.

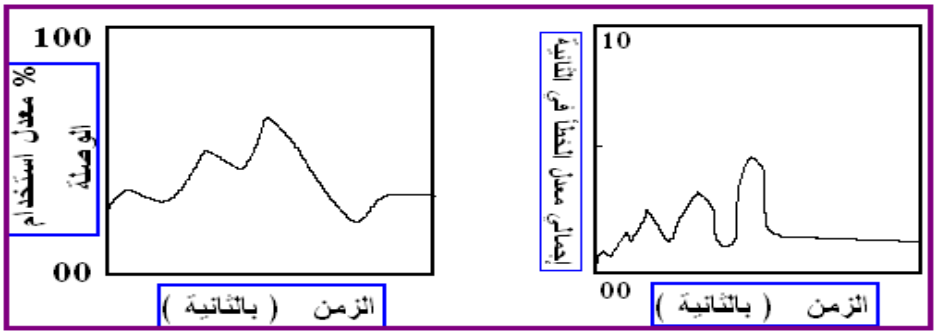
الجدول 6.1: أمثلة عددية لحساب قيمة الإتاحة.

Availab'ty	MTTR	MTBF
0.985	3.5	229.83
0.985	3.5	229.83
0.985	3.5	229.83
0.985	3.5	229.83
0.985	4	262.67
0.985	4	262.67
0.985	4	262.67
0.985	4	262.67
0.985	4.5	295.50
0.985	4.5	295.50
0.985	4.5	295.50

ونستطيع استخدام بروتوكول إدارة الشبكة لتجميع هذه البيانات من الشبكة. وهذه المعلومات ذات أهمية كبيرة من أجل تشخيص الأعطال Troubleshooting وتحليلات تحديد الاتجاهات Trend Analysis.

2.2 تحليل بيانات الأداء

يمكن أن نحصل من نتائج تحليلات بيانات الشبكة على رسومات بيانية (خطية – قضبان) تعبر عن معدل استخدام جهاز الشبكة أو الوصلة في الزمن الفعلي، أو من منظور تاريخي. وهذه الرسومات تكون مفيدة جدا في تحليلات الأداء. يمكن أن توضح الرسومات التحليلية في الزمن الفعلي حالات الاستخدام الحالية للشبكة، وكذلك الأخطاء التي تحدث في الشبكة مقابل الزمن، كما هو موضح في الشكلين 6.3 a,b . علي سبيل المثال، يمكن أن يظهر الرسم الوقت الفعلي الذي يبين العلاقة بين الحزم المرسلة مقابل معدل الأخطاء، ويمكن الاستفادة من هذه الرسومات في تحديد مشاكل الأداء في الشبكة. يمكن أيضا أن تساعد رسومات الوقت الفعلي في تشخيص مشاكل إدارة الشبكة المتعلقة بمصادر الأجهزة والوصلات المصاحبة لها: وقد يشمل ذلك معلومات عن الأجهزة مثل: استخدام الذاكرة – معدل استخدام المعالج – معدل الوصول إلى قرص التخزين – عدد الجلسات – الخ. وقد تشمل معلومات الوصلة: معدل الاستخدام – معدلات الخطأ – النسب المئوية للخطأ – الخ.



شكل 6.3 a,b : معدل استخدام الوصلة، وإجمالي معدل الخطأ لتشخيص مشاكل الأداء.

إن الرسومات التي تمثل معلومات تاريخية عن الشبكة لا تظهر حالة الشبكة الحالية، لكنها مفيدة في توضيح الاتجاهات. إن بيانات تحديد الاتجاه Trend Data ، تساعدنا في التنبؤ عندما تزيد طلبات مستخدم الشبكة عن سعة الوصلة أو الجهاز. وهذا يساعدنا في التخطيط لزيادة سعة الشبكة أو إعادة تصميمها لتفي باحتياجات المستخدمين. وتستخدم رسومات المراحل التاريخية للشبكة غالبا لفحص حالة الشبكة إما أسبوعيا، شهريا، ربع سنويا، أو سنويا، بحسب الاحتياجات.

توضح الرسومات ليس فقط عمليات الزيادة أو النقصان في معدل الاستخدام لوصلة الشبكة، ولكن أيضا يمكن أن تستخدم لإجراء إحصائيات مفيدة، مثل معدلات الخطأ في الوصلة، ومعدل استخدام المعالج لجهاز معين، عند فترات زمنية محددة. عندما نلاحظ اتجاه كمية الأخطاء التي يعاني منها أحد الأجهزة، فإن هذا قد يمكنا من تشخيص المشكلة قبل أن تؤثر على الأداء. علي سبيل المثال، عندما نلاحظ أن أحد أجهزة الشبكة، يقوم ببطء بزيادة قدرة المعالج التي يستخدمها مع الوقت، ربما نقرر تقليل حركة التدفق على الجهاز قبل أن تصل قدرته على المعالجة إلى المستوي الحرج. أو كحل بديل آخر، ربما نقوم بتحديث المعالج ونستخدم جهاز ذو معالج له قدرة معالجة أعلي من الحالي.

2.3 ضبط القيم الحدية Setting Thresholds

الخطوة الأخرى في عملية إدارة الأداء هي ضبط القيم الحدية لمعدلات الاستخدام. نستطيع تهيئة القيم الحدية للبنود المتعددة التي تؤثر على أداء الشبكة. بخصوص معالج أو جهاز الشبكة، فإن هذه القيم قد تشمل: معدل استخدام المعالج وفترات الإنذار Alarm Durations. بخصوص الوصلة، يمكن أن نختار وضع قيم حدية علي بعض البنود مثل: معدل الخطأ – متوسط الاستخدام Utilization – سرعة الأداء Throughput الإجمالية.

وفور ضبط القيم الحدية، تستطيع أدوات إدارة الأداء تدوين (لمهندس الشبكة) ، متى يصل أداء الشبكة إلي معدل خطأ معين، أو معدل استخدام معين. إن تحديد القيمة الحدية ربما يكون صعبا، لكن بواسطة إجراء تجارب المحاولة (وربما الخطأ)، سوف نحصل على القيمة الحدية المناسبة. إن القيم الحدية، تمكن مهندس الشبكة من تحديد مكان المشكلة وتصليحها قبل أن تؤثر على أداء الشبكة. إن دمج عمليتي التعبير بالرسومات عن بيانات معدل الاستخدام، مع القيم الحدية لمعدل الاستخدام، يكون أداة قوية لتحقيق إدارة الأداء.

4.2 استخدام محاكاة الشبكة لفحص الأداء

تعتبر محاكاة الشبكة أداة أخرى لإدارة الأداء يمكن استخدامها. باستخدام هذه الأداة، يستطيع مهندس الشبكة، أن يضمن بطريقة أحسن أن الشبكة التي يتم بناؤها سوف تحقق طموحات المستخدمين. إن بناء نموذج لمحاكاة الشبكة تكون مهمة صعبة. قليل من شركات البرمجيات تستطيع إنشاء محاكاة تهيئة شبكية بسيطة عادلة. إن هذا الجزء من الوحدة لا يشرح كيفية إنشاء برامج لمحاكاة الشبكة، لكنه يشرح كيفية استخدام برامج محاكاة الشبكة في تحقيق إدارة الأداء.

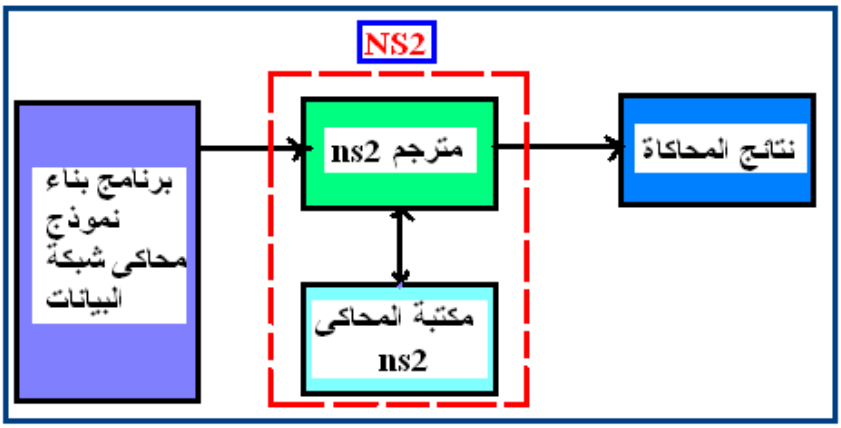
نستطيع استخدام المحاكاة في تحديد كيفية تغيير الشبكة كي تكون أكثر فاعلية وذات أداء أعلي. علي سبيل المثال، نفترض موقع شبكة بعيد، حيث يعاني المستخدمين من زمن استجابة ضعيف، عندما يستخدمون أحد التطبيقات الجديدة لإجراء الاتصالات من شبكة إقليمية متصلة بوحدة مركز بيانات مركزية. غالبا ينتج زمن الاستجابة الضعيف من حدوث اختناقات كثيفة في وصلة البيانات. بعد إجراء عملية فحص الوصلة المؤدية لموقع الشبكة عن بعد، وجدنا أن متوسط معدل الاستخدام كان فوق النسبة المئوية 80%. بالتالي يتم اتخاذ قرار بتحديث Upgrade سعة نطاق الوصلة. وعلى الرغم من إجراء التحديث للوصلة، فإن مستخدمين موقع الشبكة البعيدين لا يزالون يعانوا من زمن استجابة ضعيف عند إجراء التطبيق الجديد.

بالبحث أكثر، نجد أن بروتوكول طبقة النقل المستخدم بواسطة التطبيق الجديد، يستخدم بروتوكول توقف–ثم–انتظر (Stop-and-Wait)، وهو بروتوكول ذو سعة نافذة تساوي حزمة واحدة (Window Size = 1 Packet). ويستخدم بروتوكول طبقة النقل، طريقة تحكم في التدفق التي ترسل حزمة واحدة لكل جلسة Session ، ثم ينتظر حتى يتم وصول الرد Acknowledge ، قبل أن يتم إرسال حزمة البيانات التالية. إن وجود سعة نطاق أكبر لوصلة الموقع البعيد للشبكة سوف يسمح بإرسال أكثر من حزمة بيانات في نفس الوقت، لكن ذلك لن يؤثر على زمن التأخير الإجمالي الذي يراه مستخدمين الشبكة.

لذلك فإن تحديث الوصلة لن يحل مشكلة زمن الاستجابة الضعيف. باستخدام تطبيق محاكاة دقيق للشبكة، وبروتوكول طبقة النقل، قبل أن يتم تحديث الوصلة، قد يساعد مهندس الشبكة في الكشف عن الإخفاق المصاحب لبروتوكول طبقة النقل. إن الحل المناسب لهذه المشكلة هو أن يستخدم التطبيق مخزن مكدس بروتوكولي Protocol Stack مصاحب لبروتوكول طبقة النقل الذي يستخدم طريقة تحكم في التدفق ذات حجم نافذة أكبر من واحد في شبكة البيانات الإقليمية.

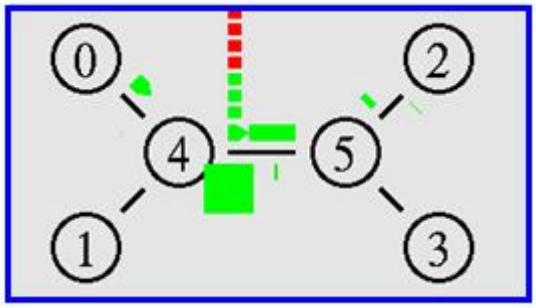
- **برنامج محاكي الشبكة:**

يمكن استخدام برنامج محاكي الشبكة Network Simulator المعروف باسم ns ، والذي تم تطويره بواسطة مؤسسة بركلي، وهو يستخدم لمحاكاة برتوكولات الشبكات IP ، TCP ، UDP ، وكذلك الشبكات التي تعمل معها. ويوجد منه متوفرا في الأسواق إصدارين ، أحدثهم هو الإصدار الثاني ns2. يتم كتابة برنامج بناء نموذج محاكاة الشبكة باستخدام لغة C++ ، أو لغة OTcl وهي لغات مبنية باستخدام تقنيات الكائنات Object Oriented. يوضح شكل6.4 المكونات الأساسية لهذا المحاكي.



شكل6.4 المكونات الأساسية لمحاكي الشبكة المعروف باسم NS2.

ويمكن استخدام برنامج الرسومات المتحركة Graphic Animator، المتوافق مع محاكي الشبكة ns2، لتمثيل حركة مرور الحزم البرمجية بين مكونات نموذج بناء محاكي أجهزة الشبكة ، وكذلك يمكن استخدام الألوان لإظهار مصادر متعددة متصلة بالشبكة، ويبين شكل 6.5 مثال على ذلك. وهذه الرسومات مفيدة جدا في دراسة وتتبع حركة مرور الحزم البيانية بين أجهزة الشبكة. وتستخدم في تحديد مراكز الاختناق (سواء كانت وصلات اتصال أو معالجات) كي يتم معالجتها بواسطة أدوات إدارة نظام الأداء في الشبكة.



شكل6.5 استخدام الرسومات المتحركة لتمثيل حركة مرور البيانات

3. إدارة الأداء في نظام إدارة الشبكة

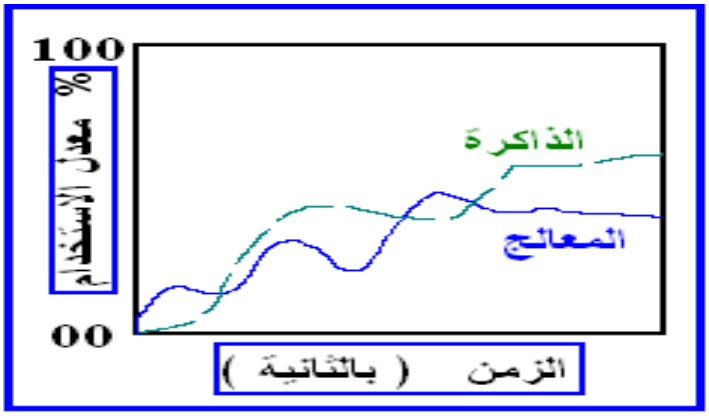
يختص إدارة الأداء في نظام إدارة الشبكة، باستخدام أدوات ذكية تستطيع فحص حالة الشبكة من منظور تاريخي، وكذلك من منظور الزمن الفعلي. وتعتمد فاعلية إدارة الأداء علي مستوى الأداة المتاحة لمهندس الشبكة.

3.1 الأداة البسيطة لفحص الأداء

ينبغي أن توفر أداة إدارة الأداء البسيطة معلومات الزمن الفعلي حول أجهزة الشبكة والوصلات، ويفضل أن تكون هذه المعلومات في شكل رسومات بيانية كالخطوط والقضبان. تستطيع هذه الأداة مساعدة مهندس الشبكة في إيجاد الاختناقات في الشبكة Network Bottlenecks، ومن ثم عزل مشاكل الأداء.

نستطيع رسم الإحصائيات المتاحة من الشبكة، باستخدام بروتوكول إدارة الشبكة، وهذا يعطينا مرونة كبيرة عندما نحاول تحليل أداء الشبكة. سوف توفر أيضا الأداة البسيطة وسيلة لإيجاد المعلومات الأساسية عن الجهاز أو الوصلة، دون أن نضطر لمعرفة تفاصيل معلومات إدارة الشبكة. في حالات كثيرة لا نحتاج معرفة كل تفاصيل عن معلومات أجهزة الشبكة (حيث أنها تكون معلومات ضخمة)، نريد فقط أن نعرف كيفية أداء الجهاز.

وتوفر الأداة البسيطة وسيلة سهلة لأجهزة الشبكة، مثل الضغط علي زر مفتاح أو بند في قائمة، لتجميع بيانات عن معدل استخدام المعالج والذاكرة. إن معدل الاستخدام المرتفع للمعالج يعني أن الجهاز لا يستطيع معالجة حركة مرور البيانات في الشبكة. بينما معدل استخدام الذاكرة (المكثف) قد يعني أن الجهاز يقوم بتخزين كمية ضخمة من المعلومات في الذاكرة. يوضح لنا الزمن الفعلي لهذه القيم مشاكل الأداء المحتملة للجهاز، كما هو مبين في شكل 6.6 .



شكل 6.6 مقارنة بين أداء معدل استخدام الذاكرة، والمعالج.

في وصلات الشبكة، يمكن أن توضح لنا الأداة البسيطة، معدل الاستخدام الحالي، ومعدلات الخطأ. على سبيل المثال، إن الرسم الذي يبين علاقة الحزم في الثانية والمعلومات في الثانية للوصلة يكون مفيدا في توضيح إجمالي أداء الوصلة. يعتبر معدل الاستخدام الحالي لوصلة الشبكة الذي يتم توضيح قيمته على الرسم مفيدا، ويتم حسابه بواسطة قسمة معدل المعلومات في الثانية للوصلة، على القيمة العظمي للمعلومات في الثانية. في حالة تشخيص الأعطال قد نحتاج فحص عدد الأخطاء في الوصلة، مقابل كمية البيانات الصحيحة المرسلة. تستطيع الأداة البسيطة تمثيل هاتين القيمتين على الرسم وإنشاء النتائج الضرورية.

ويوجد العديد من الأدوات المتوفرة في الأسواق تؤدي وظائف الأداة البسيطة. معظم برامج إدارة الشبكة تسمح بإنشاء رسومات في الزمن الفعلي للمعلومات المتاحة من جهاز الشبكة. بالإضافة إلى أن تطبيقات إدارة الشبكة، يتم تصميمها بواسطة الموردين لتعطينا رسومات تعبر عن الحالة الصحية للجهاز.

2.3 الأداة المركبة لفحص الأداء

تستطيع الأداة المركبة أن تسمح لمهندس الشبكة، بتهيئة القيم الحدية لمعدل الاستخدام ومعدلات الأخطاء. إذا زادت المعدلات الحدية عن المسموح في الشبكة، فإن الأداة المركبة تستطيع تحقيق اتخاذ فعل. تستطيع هذه الأداة أيضا، تجميع معلومات الزمن الفعلي وتخزينها في نظام إدارة قاعدة البيانات، كي نستطيع استخدامها في إجراء دراسات تاريخية، وإنشاء رسومات لرؤية أداء الشبكة عند فترات سابقة.

- **القيم الحدية:**

إن ضبط القيم الحدية التي تستطيع تشغيل أعمال لاحقة، تعطي مهندس الشبكة وظائف اعتبارية. سوف تمكنا الأداة من تحديد حدث بسيط، مثل حدوث إنذار ،أو وميض ضوئي، أو حدث متقدم مثل تشغيل الدوائر الاحتياطية، أو إرسال بريد الكتروني. علي سبيل المثال، يوفر مفتاح الخدمة المتكاملة ISDN دوائر ذات سعة نطاق مرتفع عند الطلب، باستخدام مودم خاص. وكلفة هذه الدوائر تعتمد على الوقت، وهذا يجعل هذه الدوائر اقتصادية. تستطيع الأداة استخدام هذه التقنية لطلب الدوائر، بناء على معدل الاستخدام، ومعدلات الخطأ، أو تهيئة القيم الحدية بواسطة مهندس الشبكة.

تمثل القيم الحدية وظيفة حيوية للأداة المركبة، ويمكن لمهندس الشبكة أن يقوم بتحديد القيم المثلى لهذه الوظيفة. تستطيع الأداة المركبة أن تحظرنا من وجود حالات تخطي لهذه القيم الحدية، وكذلك الأوضاع التي تقترب من القيم الحدية. على سبيل المثال، يمكن تشغيل الأداة كي ترصد معدل استخدام معالج جهاز الشبكة. بفرض أنه في مكان معين في الشبكة أن أحد الأجهزة يؤثر على أداء الشبكة، وكان معدل استخدام المعالج 90% من السعة الإجمالية. إن الأداة يمكن أن يتم تهيئتها، كي تنبهنا عندما يصل معدل استخدام المعالج إلي 80% من القيمة الحدية، وبذلك تسمح لنا بفحص حدوث مشكلة في أداء الشبكة.

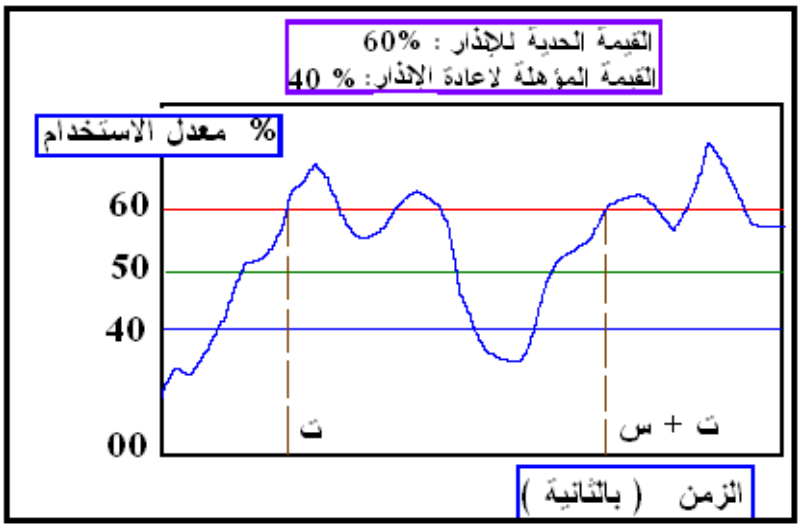
ينبغي للقيم الحدية أيضا، أن تحتوي على أولويات للملاحظات. يوجد على الأقل ثلاثة مستويات من الملاحظات هي(عالي – متوسط – منخفض). إن الأولوية العالية تبدي عن الأولوية المتوسطة، وأن الأولوية المتوسطة بدورها تبدي عن الأولوية المنخفضة. تعطي لكل أولوية لون مميز في خطة الشبكة، أو سجل الحدث في نظام إدارة الشبكة. في بعض الأحيان، يمكن أن تنتج نفس الأولوية للقيم الحدية، عند مواقع مختلفة داخل الشبكة. على سبيل المثال، بفرض انه تم تهيئة القيم الحدية لرصد معدل استخدام الوصلة. إذا زادمعدل استخدام الوصلة عن 40% ، فإن الأداة تجتاز الأولوية المنخفضة للقيمة الحدية. وأن معدل استخدام 65% يجتاز الأولوية المتوسطة للقيم الحدية، وأن معدل استخدام 75% يجتاز الأولوية العالية للقيمة الحدية.

نفترض بعد ذلك، في مرحلة لاحقة، أنه قد تم تهيئة قيمة حدية أخري، لمراقبة معدل استخدام الذاكرة لجهاز. إذا قلت الذاكرة المتبقية في الجهاز عن 100 كيلوبايت، تقوم الأداة المركبة بإعلان أن القيمة الحدية وصلة للأولوية العالية. خلال دقائق من اختيار معدل استخدام الوصلة للقيمة الحدية للأولوية المتوسطة، فإن القيمة الحدية للأولوية العالية للذاكرة يتم اجتيازها. تحتاج الأداة المركبة الآن أن تحتفظ بقائمة لكل القيم الحدية الزائدة للجهاز، وأن تعرضهم على مهندس الشبكة حسب الأولوية. إذا استخدمت الأداة المركبة، خريطة الشبكة لعرض القيم الحدية الزائدة الحالية للجهاز بلون واحد، فإن هذا لا يصلح. لذلك يفضل تخصيص لون مختلف لكل أولوية.

- **القيم التأهيلية Re-arm Values:**

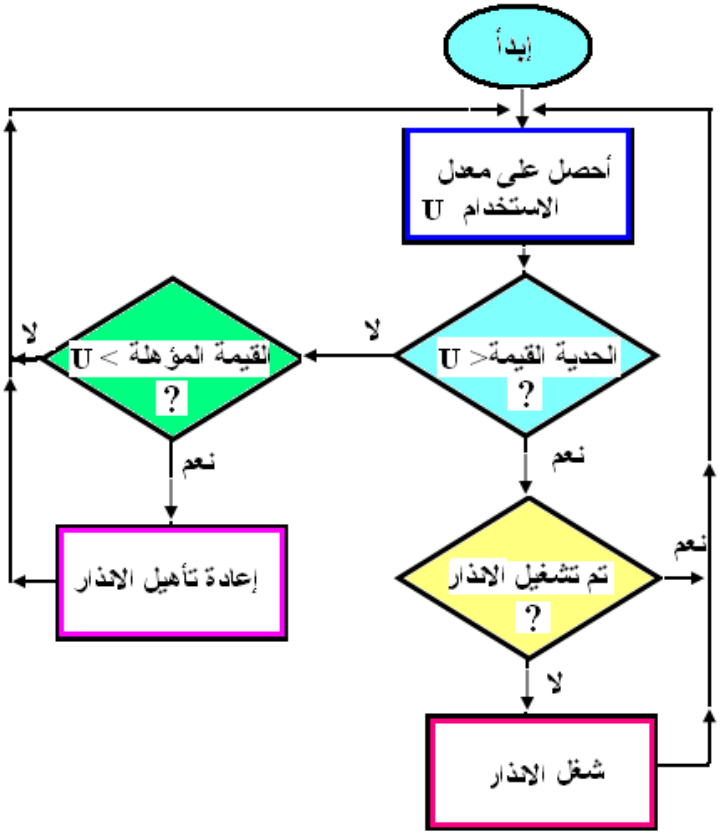
ينبغي علي الأداة أيضا، أن تكون قادرة على تأهيل Re-arm القيمة الحدية بالسلوك المعقول، ويتم عمل ذلك بواسطة إعادة تأهيل القيم الحدية بقيم تسمي "القيم التأهيلية". علي سبيل المثال، نفترض أنه تم حدوث إنذار عندما وصل معدل الاستخدام إلي القيمة الحدية 60% ، بعد لحظة متأخرة، توقف الإنذار عندما قل معدل الاستخدام إلي 58%، بعد مرور ثواني قليلة لاحقا، عندما وصل معدل الاستخدام 61%، حدث الإنذار مرة

أخرى. لمنع هذا الفائض المزعج المتتالي من الإنذارات المتعددة، ينبغي ضبط الأداة بحيث عندما تصل القيمة الحدية في المرة الأولي، فإن الأداة تحدث الإنذار. لاحقا، فإن الأداة ينبغي أن تؤهل القيمة الحدية فقط عندما يقل معدل الاستخدام عن القيمة المعرفة، مثلا 40%، كما هو موضح في شكل 6.7 . بهذه الترتيبات، تقوم الأداة بإعطاء صوت إنذار عندما يتم اجتياز القيمة الحدية، وسوف يتم إصدار إنذار آخر فقط، عندما يقل معدل الاستخدام عن 40% ، وزاد بعد ذلك مرة أخرى فوق 60%. توضح خريطة التدفق شكل 6.8 هذا المثال. يمكن أيضا، ضبط الأداة كي تستخدم نفس الأسلوب لفحص معدلات الخطأ في وصلة الشبكة.



شكل6.7 يتم تشغيل الإنذار مرتين، عند الزمن ت، ت+س لتجاوز القيمة الحدية لمعدل الاستخدام.

إن معظم برامج إدارة الشبكة تتعامل مع القيم الحدية. وتحديد الأعمال Actions اللازم اتخاذها عندما يتم اجتياز القيمة الحدية، وتحديد أولويات القيم الحدية، وتأهيل (ضبط) القيمة الحدية آليا. بعض تطبيقات الشبكة يمكنها تشغيل القيم الحدية آليا لمراقبة معايير حرجة خاصة بأجهزتهم.



شكل6.8 فحص معدل الاستخدام وتشغيل الإنذارات، بناء على تخطي القيمة الحدية والقيمة المؤهلة.

أسئلة تقويم ذاتي

قارن بين كلا مما يلي، موضحا تأثيرهما على أداء الشبكة:

1- زمن الاستجابة Response Time ، وزمن دورة الرحلة Round Trip Time.

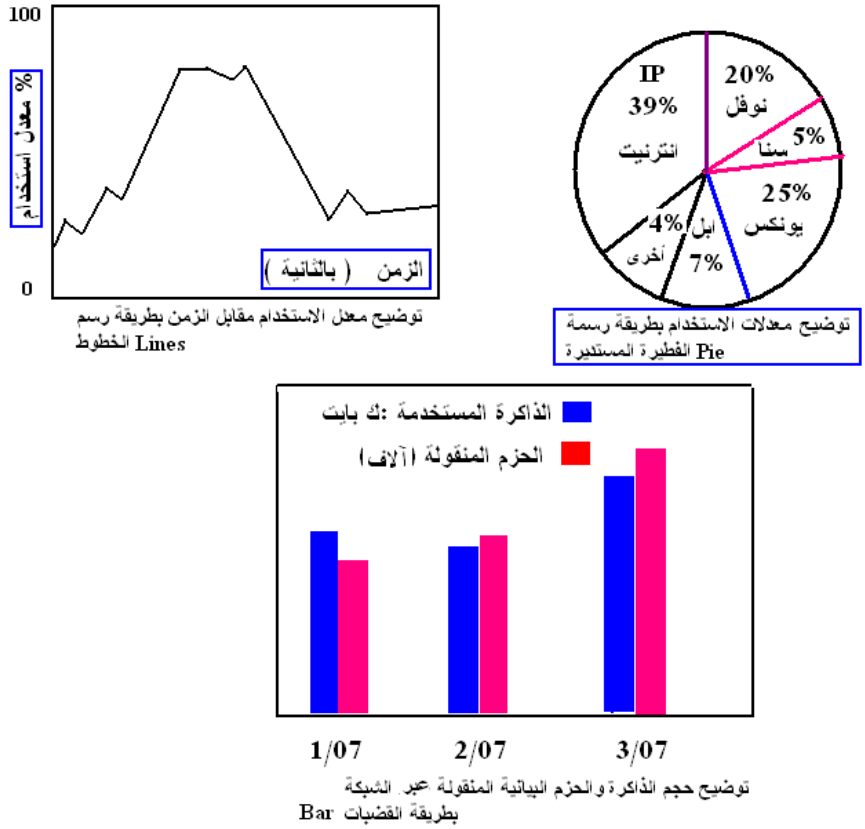
2- القيم الحدية Threshold Values، والقيم التأهيلية Re-arm Values.

- **رسم البيانات التاريخية لفحص أداء الشبكة:**

ينبغي أيضا، أن تستطيع الأداة المركبة رسم البيانات التاريخية الموجودة في نظام إدارة قاعدة البيانات والخاصة بإدارة الأداء. عندما تعاني شبكة البيانات من مشاكل في الأداء، فإنه غالبا لا يستطيع مهندس الشبكة في نفس اللحظة فحص كل العلاقات ذات الصلة. أيضا في كثير من الحالات، ربما يشتكي المستخدم عن حدوث المشاكل بعد مدة من حدوثها. في مثل هذه الأوضاع، فإن الرسومات التي توفرها الأداة البسيطة في الزمن الفعلي لا تساعدنا كثيرا. لكن بواسطة القدرة على استرجاع المعلومات الضرورية ، وبعد ذلك فحصها في شكل رسومات بيانية، تستطيع مساعدتنا في حل هذا النوع من المشاكل بشكل صحيح. ينبغي على الأداة إنشاء رسومات بيانية علي شكل خطوط Lines – قضبان Bars – شكل مستدير

- **فوائد الرسومات في تقييم أداء الشبكة:**

تفيد الرسومات الخطية عند فحص اتجاهات البيانات، مثل معدل الاستخدام. تكون الرسومات القضبانية أكثر فاعلية عند إجراء مقارنة القيم مثل حجم الذاكرة المستهلكة في جهاز الشبكة مقابل عدد حزم البيانات التي يتم معالجتها. تكون الرسومات البيانية علي شكل مستديرفائدة كبيرة خاصة عند توضيح النسب المئوية للقيم، مثل أنواع حركة مرور البيانات التي تمر عبر أجهزة الشبكة أثناء فترات بطء الأداء . ويوضح شكل 6.9 أمثلة لهذه الرسومات البيانية.



توضيح معدل الاستخدام مقابل الزمن بطريقة رسم الخطوط Lines

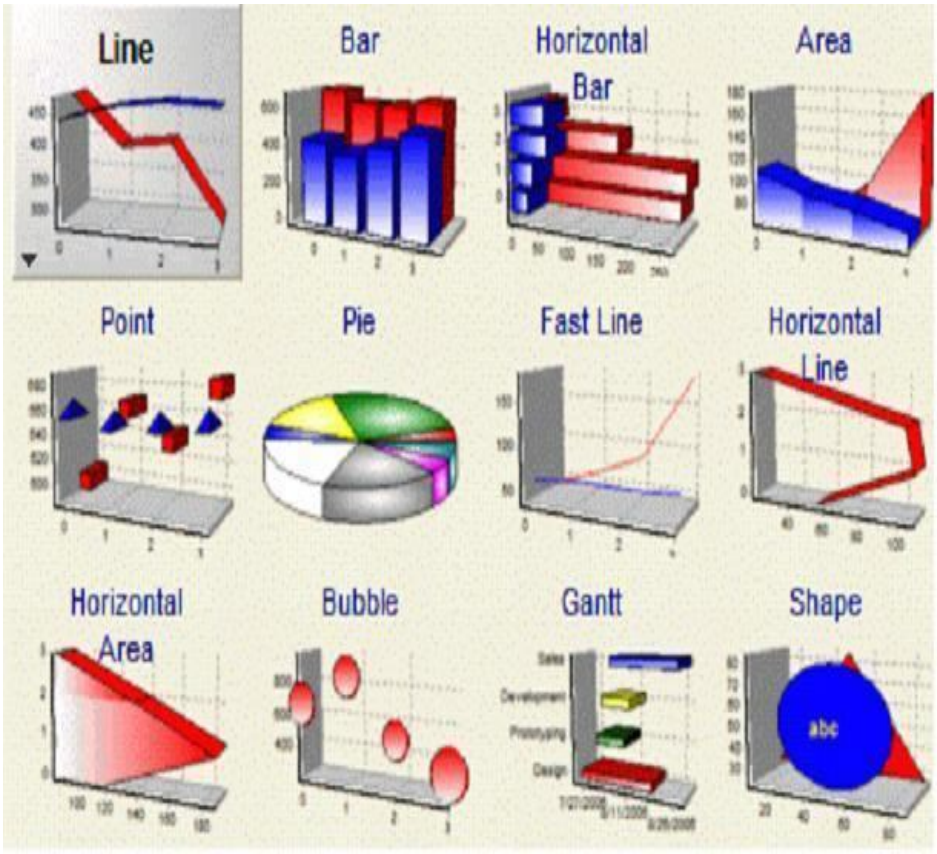
توضيح معدلات الاستخدام بطريقة رسمة الفطيرة المستديرة Pie

توضيح حجم الذاكرة والحزم البيانية المنقولة عبر الشبكة بطريقة القضبان Bar

شكل6.9 يوضح بعض أنواع الرسومات التي تستطيع الأداة المركبة إنشائها.

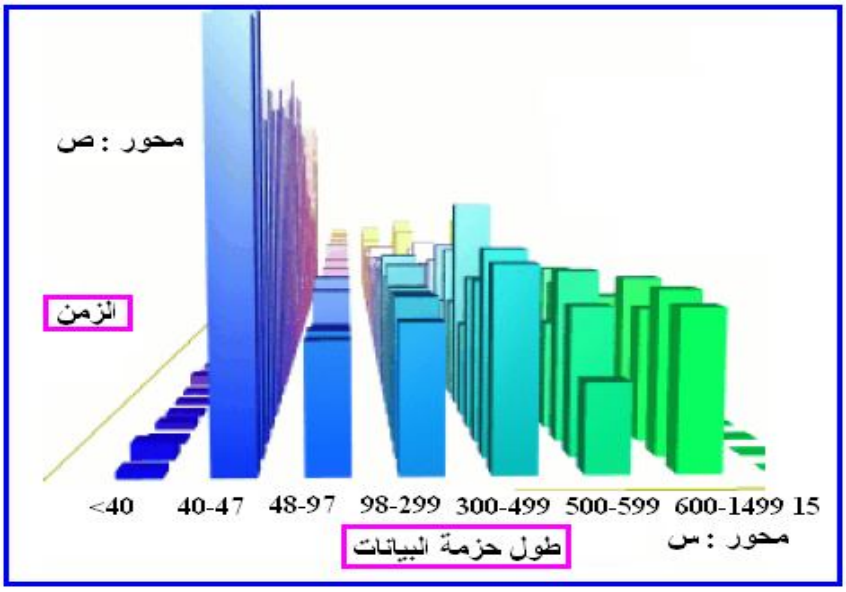
- **الرسومات المجسمة (ثلاثية الأبعاد):**

لقد تطورت طرق عرض الرسومات البيانية الخاصة بقياس الأداء، بواسطة أدوات إدارة الأداء المتطورة، وهذا يمكن أدوات إدارة الأداء من إنشاء رسومات مجسمة ترسم في الأبعاد الثلاثية 3Dimension Graphics ، ويوضح شكل 6.10 نماذج من هذه الأنواع المجسمة للرسومات.



شكل6.10 بعض أشكال الرسومات المجسمة التي يمكن استخدامها لقياس وتوضيح الأداء في شبكة البيانات.

علي سبيل المثال، يوضح شكل 6.11 ، رسم قيم البيانات الفعلية Real Data، لتوضيح العلاقة بين جيوب حزم البيانات، مقابل الزمن. كل جيب حزمي على محور س يمثل نطاق أطوال حزم بيانية Packet Sizes . ويمثل محور ص ، انتشار عينات البيانات Data Samples. يبين كل قضيب منها عدد حزم البيانات التي تقع في جيب حزمي محدد خلال مدة العينة Sample Interval.



شكل6.11 رسم ثلاثي الأبعاد يبين العلاقة بين أطوال حزم البيانات مقابل الزمن.

3.3 الأداة المتقدمة لفحص الأداء

توفر الأداة المتقدمة الكثير من الخدمات مثل: فحص البيانات التاريخية للشبكة، تحقيق محاكاة الشبكة، التنبؤ بزمن الاستجابة، معدل الرفض، والإتاحة.

- **فحص البيانات التاريخية للشبكة:**

ينبغي على الأداة المتقدمة أن تكون قادرة على استخدام المعلومات الموجودة في قاعدة البيانات العلائقية لفحص حالة الشبكة، عند أي فترة زمنية ماضية، للبحث عن مشاكل محتملة في الأداء وتساعد في تخطيط سعة الشبكة. لتحقيق ذلك فإن الأداة المتقدمة تحتاج أن تكون قادرة على الأتي:

1- تستقبل دخل المستخدم الذي يعبر عن حالة الشبكة ومشاكل الأداء.

2- تستقبل المعلومات من قاعدة البيانات.

3- تحلل حالة الشبكة.

تتطلب الخطوة الأولي لهذه العملية، أن يتم إخبار الأداة عن المدة الزمنية الماضية المطلوب أن يتم عندها فحص بيانات الشبكة. وكذلك أن يتم إخبار الأداة عن الحاسبات المضيفة والأجهزة والوصلات التي ينبغي أن تفحصها. علي سبيل المثال، يمكن أن نخبر الأداة لمراجعة الأداء بين حاسبين مضيفين متصلين بالشبكة في الشهر الماضي.

الخطوة الثانية، تحتاج الأداة استرجاع المعلومات من قاعدة البيانات العلائقية في نظام إدارة الشبكة. لكل عنصر مراد فحصه، تحتاج الأداة معرفة المعلومات المراد استرجاعها. على سبيل المثال، بخصوص جهاز في الشبكة، فإن الأداة تستطيع تجميع معلومات عن المعالج، والذاكرة ومعدل استخدامهما. بخصوص وصلة الشبكة، فإن الأداة تستطيع البحث عن بيانات متعلقة بمعدلات الخطأ، ونسبة استخدام سعة النطاق.

ملاحظة: ينبغي أيضا أن يستطيع مهندس الشبكة تحديد أية معلومات إضافية، قد تحتاجها الأداة من قاعدة البيانات.

بعد ذلك، تستطيع الأداة تحليل البيانات وتحديد مصدر مشكلة أداء معينة. كما تستطيع فحص أعمال Actions تم تعريفها سابقا، مثل معدلات الخطأ العالية، أعمال متعلقة بزيادة القيم الحدية، أو زيادة في حركة المرور في الشبكة. باستخدام لغة الاستفسار الهيكلية SQL ، يستطيع مهندس الشبكة إضافة قواعد لإجراء التحليلات. على سبيل المثال، يضيف الأمر التالي قاعدة للبحث عن حاسب مضيف host، الذي يوجد به أكثر من عشرة مستخدمين.

```
SELECT * FROM hosts WHERE users > 10
```

- **تخطيط سعة وصلات الشبكة:**

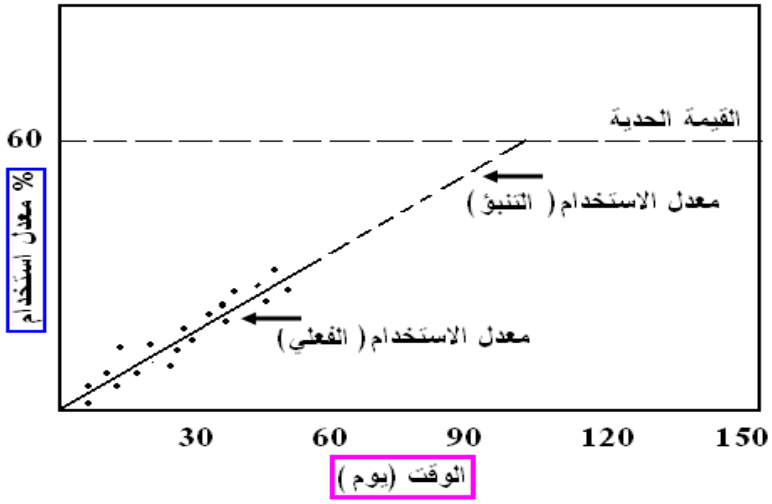
تستطيع الأداة المتقدمة مساعدة مهندس الشبكة، في تحقيق تخطيط السعة لوصلات الشبكة، بواسطة معلومات من قاعدة البيانات العلائقية. عندما تستخدم وصلات الشبكة فوق نسبة مئوية معينة، يمكنها أن تؤثر على أداء الشبكة يمكن أن تتغير هذه النسبة كثيرا، ويعتمد ذلك على مدى استخدام الوصلة وزمن الاستجابة الذي يتطلبه المستخدمين. أحد المشاكل الشائعة تنتج عندما يكتشف مهندس الشبكة، أن الوصلة بلغة النسبة المئوية الحرجة لمعدل الاستخدام، وهى غالبا تأخذ وقتا طويلا حتى يمكن تحديثها.

- **المعاونة في التنبؤات لتحديث الشبكة:**

تستطيع الأداة المتقدمة استخدام المعلومات من قاعدة البيانات العلائقية لمساعدة مهندس الشبكة في التنبؤ عندما تصل الوصلة مقدما إلى القيمة الحدية الحرجة لمعدل الاستخدام. لذلك يستطيع مهندس الشبكة بدء عملية تحديث الوصلة وتركيبها، قبل أن يلاحظ المستخدمين مشكلة الأداء. ينبغي أولا، أن نوفر الدخل عن المدة المطلوبة لتحديث الوصلة، وكذلك النسبة المئوية لمعدل الاستخدام، التي يبدأ عندها مستخدمين الشبكة ملاحظة مشكلة الأداء. على سبيل المثال، يمكن أن نحدد للأداة أن تأخذ خمسون يوما من أجل إنشاء وصلة جديدة، وأن المستخدمين تبدأ تلاحظ مشكلة الأداء عند نسبة مئوية لمعدل استخدام 60%. ينبغي لقاعدة البيانات العلائقية أن توفر المعلومات التي تسمح للأداة حساب متوسط معدل الاستخدام لوصلة خلال كل ساعة منذ بدء عملها. لتجميع هذه المعلومات، فإن الأداة تقوم بإجراء عملية الانتخاب للوحدة البينية لجهاز الشبكة التي توصل إلى الوصلة على الأقل مرة كل ساعة وتلاحظ معدل الاستخدام الحالي للوصلة.

فور تخزين هذه المعلومات في قاعدة البيانات العلائقية، تستطيع الأداة المتقدمة ،داخليا، حساب اتجاه معدل الاستخدام الفعلي، وتسلط الضوء عندما يزيد معدل الاستخدام عن القيمة الحدية، التي وضعها مهندس الشبكة، كما هو مبين في شكل 6.12. إذا كان الوقت

المخطط لهذه العملية أقل أو يساوى الوقت اللازم لإجراء عملية تحديث الوصلة، فإن الأداة تقوم بتنبيه مهندس الشبكة كي يجري عملية التحديث. على سبيل المثال، إذا قامت الأداة بقياس معدل استخدام الوصلة عند 23%، ولاحظت أنه إذا استمر معدل الاستخدام في التزايد عن معدله الحالي، فإنه سوف يفوق 60% عن القيمة الحدية في خمسون يوما، وينبغي أن يتم تنبيه مهندس الشبكة. يمكن للأداة عمل ذلك بواسطة إرسال رسالة بريد الكتروني، أو إظهار رسالة على نظام إدارة الشبكة.



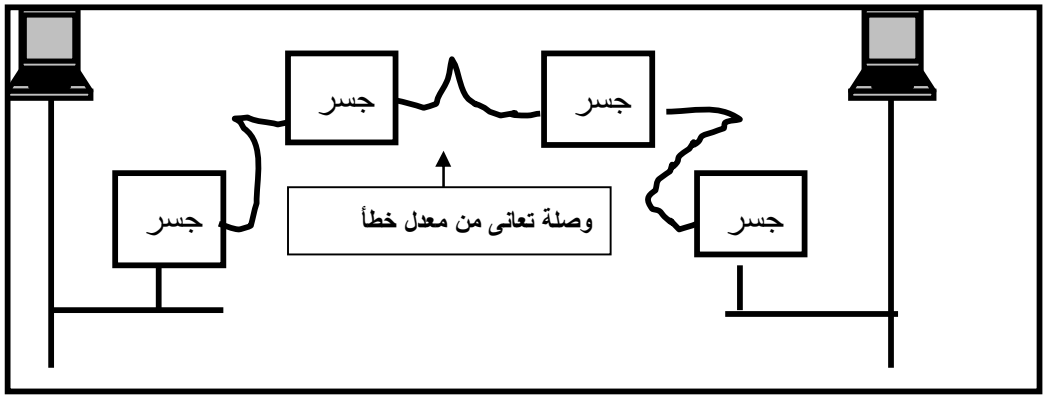
شكل6.12 يوضح اتجاه معدل استخدام الوصلة

- **تقليل الوقت اللازم لتحليل وصيانة مشاكل الشبكة:**

يمكن للأداة المتقدمة أن توفر وقت مهندس الشبكة، وإجراء المساعدة في رسم النتائج عن مناطق الشبكة التي تعاني أداء غير مقبول. (لاحظ أن هذه الأداة من المحتمل أن تستهلك كمية ضخمة من الذاكرة). لذلك ينبغي أن يتم تحدد كمية المعلومات التاريخية المطلوبة، لتوفير المساحة اللازمة لتخزينها.

مثال، نفترض إننا نستقبل دخل البيانات الذي يقوم المستخدمين بنقله من الحاسب"أ" إلى الحاسب"ب" ، وأن الأداء كان يعاني بطئا خلال أسبوع مضي. يوضح شكل6.13 تهيئة الشبكة لهذا التطبيق. يمكن أن تستخدم الأداة لتحليل جزء من الشبكة الذي يوصل

الحاسبين "أ" ، "ب" . دعنا نفترض أن التحليل يبين تزايد تدريجي لمعدل الخطأ في الوصلة التي تربط القنطرتين على المسارين بين الحاسبين "أ" ، "ب". وأن معدل الخطأ هذا قد ازداد بدرجة كافية، لكن ليس بالدرجة التي تؤدي إلى تشغيل إنذار تخطي القيمة الحدية. تستطيع الأداة المتقدمة إنشاء رسم بياني خطي يوضح تقدم معدل الخطأ، وهذا يمكن مهندس الشبكة من مخاطبة مورد الجهاز وتدوين المشكلة في التقرير. بذلك نلاحظ أن استخدام الأداة المتقدمة توفر الوقت المستغرق في عملية تحليل وصيانة مشاكل الشبكة.



شكل6.13 يوضح وصلة تعاني من معدل خطأ مرتفع،
تم تحليل هذه المشكلة بسرعة بواسطة الأداة المتقدمة.

- **محاكاة الشبكة لفحص أدائها:**

ينبغي أن تساعد الأداة المتقدمة مهندس الشبكة في تحليل الأداء المستقبلي وتحديد التهيئة التي تستطيع إنشاء أعلى أداء. يمكن تحقيق ذلك بواسطة محاكاة الشبكة، حيث تقوم الأداة بأخذ دخل البيانات عن تشغيل الشبكة، أو بواسطة المحاكاة، ثم تقوم بإجراء التنبؤات عن إدراك المستخدمين لأداء الشبكة.

إن أصعب جزء في إنشاء محاكاة الشبكة، هو بناء نموذج الشبكة. يقوم النموذج بتعريف كيفية حساب كل مكون في الشبكة وطريقة تفاعله مع معايير المحاكاة. أساسا، فإن النموذج هو عبارة عن مجموعة من القواعد يحتاجها نظام المحاكاة لأداء عمله. ويوجد

بعض الشركات توفر أدوات محاكاة الشبكة، وذلك لشبكات البيانات المركبة. الجزء الذي تحتاجه كل أداة هو القدرة على توليد النموذج المناسب. إن المعلومات التي تأخذها الأداة المتقدمة من نظام قاعدة البيانات تساعد في بناء نموذج المحاكاة، الذي بدوره يقوم بإنشاء محاكاة أكثر دقة للشبكة. يمكن أيضا لمهندس الشبكة أن يستخدم الأداة المركبة في تجميع المعلومات، وبعد ذلك يقوم بتغذية هذه النتائج يدويا، إلي جزء المحاكاة الخاص بالأداة المتقدمة.

- **التنبؤ بزمن الاستجابة، معدلات الخطأ، والإتاحة:**

بمعلومية دخل كافي، تستطيع الأداة المتقدمة أيضا، محاكاة حركة مرور الرسائل وتوضيح الإتاحة، معدلات الرفض، وأزمنة الاستجابة، وهذا يساعدنا في شراء أجهزة الشبكة المناسبة، وتخصيص سعة النطاق الصحيحة. تكون هذه الخاصية مفيدة بالتحديد عندما نبني شبكة البيانات، وتساعدنا في أن نضمن الأداء المثالي للشبكة، وكذلك تجنب مشاكل الشبكة المستقبلية المحتملة.

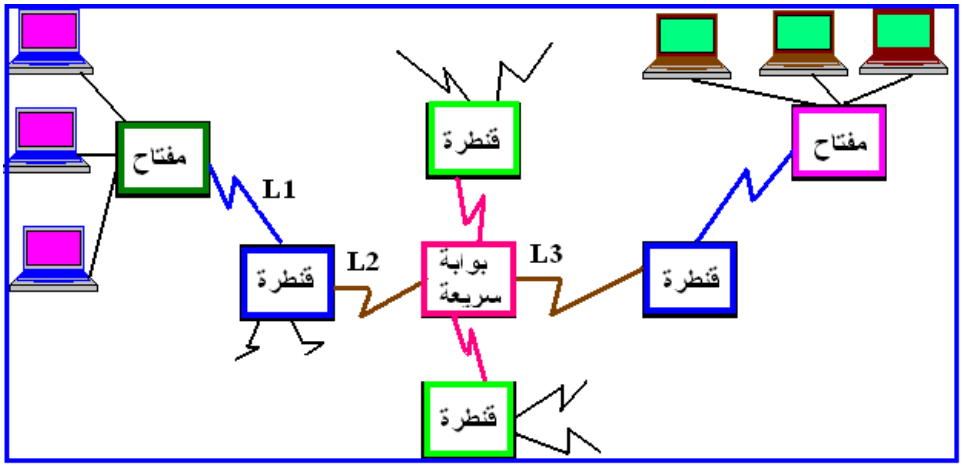
على سبيل المثال، نفترض أن موقع جديد، يرغب في توصيل شبكة. وأن المستخدمين تتوقع زمن استجابة أقل من نصف ثانية، ومعدل رفض قريبا من الصفر، و100% إتاحة للوصلة التي بين موقعهم وبين مكتب مبيعات بعيد باستخدام الأداة المتقدمة، تستطيع نمذجة الوصلات المختلفة من الموقع الجديد، واستخدام وصلات ذات سرعات مختلفة، بعد ذلك نجهز النموذج بعدد الحاسبات المضيفة وأجهزة الشبكة المناسبة.

إن هذا الجزء من الأداة المتقدمة تستخدم محاكاة الشبكة. بتوفير نموذج محاكاة جيد، يمكن تحقيق التنبؤ بكل من الإتاحة، معدلات الرفض، وزمن الاستجابة. بالطبع، إن هذه الوظيفة يخصص لها نفس عدد الإنذارات مثل مكونات محاكاة الشبكة. يمكن لمهندس الشبكة، استخدام الأدوات المتقدمة المتاحة في الأسواق لإجراء التطبيقات السابقة. كذلك يمكن أن يقوم هو بنفسه ببناء الأداة المتقدمة التي يمكنها تحقيق المحاكاة.

4. تدوين معلومات الأداء في نظام إدارة الشبكة

يوجد عدة طرق متاحة لتدوين بيانات الأداء. تعتبر طريقة التدوين النصي أشهر هذه الوسائل، حيث يمكن عرضها على جميع أجهزة الحاسبات ويمكن طبعها بسهولة. وهى تستخدم في إظهار معدل الاستخدام ومعدلات الأخطاء لأجهزة الشبكة. كمثال: يبين جدول 6.2 معدلات الاستخدام والخطأ للشبكة الموضحة في شكل 6.14. ويكون هذا النوع من التقارير مفيدا للحصول على معلومات إدارة الأداء لأجهزة الشبكة، كما يمكن توليد تقرير مماثل لوصلات الشبكة كما هو مبين في جدول 6.3 .

ويمكن أن يحتوي التقرير النصي على معلومات قيمة. لكن بسبب أنه أيضا من المفيد التعبير عن معلومات الأداء بواسطة الرسومات، فإنه من الناحية المثالية ينبغي أن تقوم البرامج بتحويل التقارير النصية إلى رسومات بيانية. إن معظم نظم إدارة الشبكة توفر طريقة للتعبير عن البيانات بواسطة الرسومات، وذلك باستخدام فورمات رسومية مثل طريقة عرض خريطة المعلومة Bit-Map Display . علي سبيل المثال، يمكن تشغيل العرض بحيث إذا ذاد معدل استخدام الوصلة فإن الصورة تظهر أكثر سمكا ، أو يتغير اللون على خريطة الشبكة عندما يتم تجاوز القيمة الحدية. إن الصورة التي تعبر عن وجود أخطاء ناتجة عن مشكلة في وصلة الشبكة، التي تعاني معدل خطأ ضخم، يمكن أن يتم التعبير عنها بواسطة خط متقطع، كما هو مبين في جدول6.3.



شكل6.14 تدوين بيانات الأداء.

توفر اشكال رسم خريطة المعلومة نفس المميزات لأجهزة الشبكة. على سبيل المثال، عندما يزداد معدل استخدام الأجهزة، كما هو مبين في جدول6.4، فإن صورة الجهاز على خريطة الشبكة يمكن أن يكبر حجمها، وأن معدل الاستخدام المفرط يمكن أن يظهر صورة الجهاز يفرز عرقا، وأن الصورة التي تعبر عن جهاز شبكة زاد معدل الخطأ فيه، يمكن أن ترسم صورة الجهاز مشروخا. بالاستعانة بمميزات عرض الرسومات بطريقة فورمات خريطة المعلومة، نستطيع بمجرد النظر إلي هذه الرسومات أن نتعرف على الأداء العام لأجهزة ووصلات الشبكة.

جدول6.2 ، 6.3 تدوين بيانات الأداء.

جدول1 معدل استخدام و أخطاء أجهزة الشبكة

الأداء /	% الاستخدام	% الاستخدام	% الأخطاء	% الأخطاء
جهاز الشبكة	المتوسط	القمة	المتوسط	القمة
مفتاح	30	35	5	6
قنطرة	60	70	7	8
بوابة سريعة	75	78	9	12

جدول2 معدل استخدام و أخطاء وصلات الشبكة

الأداء /	% الاستخدام	% الاستخدام	% الأخطاء	% الأخطاء
وصلة الشبكة	المتوسط	القمة	المتوسط	القمة
L1	40	50	0	1
L2	50	60	6	8
L3	77	79	7	9

جدول6.4 تمثيل صورة الوصلة على خريطة أداء الشبكة حسب معدل الاستخدام.

أداء الوصلة	صورة الوصلة
زيادة معدل استخدام الوصلة	تظهر الصورة أكثر سمكا
تجاوز القيمة الحدية	يتغير لون الوصلة على خريطة الشبكة
الوصلة تعاني معدل خطأ كبير	يتم التعبير عنها بواسطة خط متقطع

جدول 6.5 تمثيل صورة الجهاز على خريطة أداء الشبكة حسب معدل الاستخدام.

أداء الجهاز	صورة الجهاز
يزداد معدل استخدام الجهاز	تكبر حجم صورة الجهاز على الخريطة
معدل الاستخدام المفرط	تظهر صورة الجهاز يفرز عرقا
زيادة معدل الخطأ في الجهاز	تظهر صورة الجهاز مشروخا

5. برامج عملية للتدريب على قياس الأداء

يوجد العديد من البرامج المتاحة للتدريب على قياس أداء الشبكات، ويبين جدول6.6 بعض هذه البرامج المشهورة، التي يمكن تحميلها من شبكة الانترنيت والتدريب عليها. وفيه يتضح مسمى البرنامج واستخدامه والموقع الذي يمكن منه تحميل البرنامج. معظم هذه البرامج متاح منها نسخة مجانية على شبكة الانترنيت.

جدول6.6 بعض البرامج العملية لقياس أداء شبكات البيانات.

مسمى البرنامج (الأداة)	استخدامه	الموقع على شبكة الانترنيت *URL*
bing	قياس سعة النطاق bandwidth	http://fgouget.free.fr/bing/index-en.shtml
bprobe	قياس سعة النطاق العظمي	http://cs-people.bu.edu/carter/tools/Tools.html
Cprobe	تحديد اختناق المسارcongestion	http://cs-people.bu.edu/carter/tools/Tools.html
iperf	قياس سعة النطاق العظمي	http://dast.nlanr.net/Projects/Iperf/
netperf	قياس سرعة الأداء throughput	http://www.netperf.org/netperf/NetperfPage.html
treno	قياس سرعة الأداء throughput	http://www.psc.edu/networking/treno_info.html
nettimer	قياس أداء الشبكة وعمل محاكاة	http://gunpowder.Stanford.EDU/~laik/funding/nettimer/index.html
pathload	قياس سعة نطاق	http://www.pathrate.org/

	الشبكة	
pathrate	قياس سعة capacity مسار الشبكة	http://www.pathrate.org/
Pchar	قياس سعة capacity مسار الشبكة	http://www.employees.org/~bmah/Software/pchar/
sprobe	قياس اختناق bottleneck سعة النطاق	http://sprobe.cs.washington.edu/
pingplotter	رسم مسارات الأداء في الشبكة	http://www.pingplotter.com/
Traceroute	رسم مسارات الأداء في الشبكة	ftp://ftp.ee.lbl.gov/traceroute.tar.gz

أسئلة تقويم ذاتي

الجدول التالي يوضح مسمى الأداة العملية التي يمكن استخدامها لفحص أداء الشبكة.أكمل المعلومات التي توضح استخدامات كل منهم؟

رقم الأداة	مسمى الأداة العملية (البرنامج)	استخدامه
1	iperf	.....
2	netperf	.....
3	nettimer	.....
4	pathload	.....
5	traceroute	.....
6	pathrate	.....
7	treno	.....

الخلاصة

عزيزي الدارس ، تعرفنا في هذه الوحدة على إختصاصات إدارة الأداء بضمان أن الخط السريع للشبكة يظل غير مزدحم، وكذلك تم تم تناول أمكانية الوصول إليه. و كيفية تحقيق ذلك من خلال:

- رصد أجهزة الشبكة والوصلات المصاحبة لها لتحديد معدل الاستخدام Utilization ، ومعدلات الخطأ Error Rates.
- مساعدة الشبكة في توفير مستوى خدمة متناسقة إلى المستخدمين، بضمان أن سعة الأجهزة والوصلات ليست مرهقة إلى حد غير ملائم يؤثر على الأداء.

لتحقيق إدارة الأداء يتم تتبع الخطوات التالية:

- تجميع بيانات عن معدل الاستخدام الحالي لأجهزة الشبكة والوصلات.
- تجميع البيانات ذات الصلة لتبيان اتجاه معدل الاستخدام المرتفع.
- ضبط حدود معدل الاستخدام.
- استخدام المحاكاة Simulation لتحديد كيفية تعديل الشبكة للحصول على أقصي أداء.

في هذه الوحدة أيضاً تناولنا فوائد إدارة الأداء، ومناقشة الخطوات الأربعة الخاصة بتحقيق هذه الفوائد. بعد ذلك، يتم وصف ثلاثة أدوات لإدارة الأداء، ويشمل ذلك الأداة البسيطة، والمركبة والمتقدمة. وأخير

لمحة مسبقة عن الوحدة القادمة

عزيزي الدارس في الوحدة القادمة سنشرح إدارة الحسابات بتجميع إحصائيات عن الشبكة، لتساعد مهندس الشبكة في اتخاذ القرارات المتعلقة بتخصيص مصادر الشبكة. تكون هذه الإحصائيات مفيدة في إدارة نظام المصادر، مثل: مساحات أقراص تخزين البيانات، قدرة المعالجة، عمليات التخزين الاحتياطية. في الوحدة القادمة ستناول فوائد إدارة الحسابات، وبعد ذلك الخطوات المتعلقة بتحقيقها. تشمل الوحدة أيضا، شرح تفصيلي لتحديد فواتير دفع ،كن معنا في الوحدة القادمة وستجد الكثير المفيد إنشاء الله .

مسرد المصطلحات

- **تخطيط السعة Capacity Planning:**

يفيد تخطيط السعة كل من المستخدمين ومهندس الشبكة. باستخدام معلومات إدارة الأداء، يستطيع مهندس الشبكة تحديد السعة الحالية للشبكة بواسطة استخدام بروتوكول إدارة الشبكة لتجميع معلومات عن كل الحروف المرسلة والمستقبلة في الوحدة البينية للشبكة.

ثانيا:- معدل الرفض Rejection Rate.

ثالث:- الإتاحة Availability.

إجمالي زمن الاستجابة Response Time .

يعرف إجمالي زمن الاستجابة بأنه الفترة الزمنية التي تأخذها معلومة استدلالية تدخل الشبكة ويتم معالجتها إلي أن يتم الاستجابة وتترك الشبكة.

ضبط القيم الحدية Setting Thresholds:

الخطوة الأخرى في عملية إدارة الأداء هي ضبط القيم الحدية لمعدلات الاستخدام. نستطيع تهيئة القيم الحدية للبنود المتعددة التي تؤثر على أداء الشبكة. بخصوص معالج أو جهاز الشبكة

- **برنامج محاكي الشبكة:** Network Simulator

المعروف باسم ns ، والذي تم تطويره بواسطة مؤسسة بركلي، وهو يستخدم لمحاكاة برتوكولات الشبكات IP ، TCP ، UDP ، وكذلك الشبكات التي تعمل معها. ويوجد منه متوفرا في الأسواق إصدارين ، أحدثهم هو الإصدار الثاني ns2. يتم كتابة برنامج بناء نموذج محاكاة الشبكة باستخدام لغة C++ ، أو لغة OTcl وهي لغات مبنية باستخدام تقنيات الكائنات Object Oriented. يوضح شكل6.4 المكونات الأساسية لهذا المحاكي.

المصطلح بالإنجليزية	معناه بالعربية
Acknowledge	وصول الرد
Alarm Durations	فترات الإنذار
Animator Graphics	الرسومات المتحركة
Availability	الإتاحة
Bar Graphics	رسومات قضبانية
Bit-Map Display	عرض خريطة المعلومة
Bucket Packets	جيوب حزم البيانات
Capacity Planning	تخطيط السعة
Datum	معلومة استدلالية
Data Samples	عينات البيانات
Destinations	الأهداف
3Dimension Graphics	رسومات في الأبعاد الثلاثية
Error Rates	معدلات الخطأ
Full Duplex	الإرسال في الاتجاهين
Frames	الأطر
Idle Time	زمن توقف
Lines Graphic	خطوط رسومية
MTBF(Mean Time Between Failure)	المتوسط الزمني بين الإخفاق
Mainframe	الحاسب الكبير
Network Simulator	محاكي الشبكة
Network Bottlenecks	الاختناقات في الشبكة
Network Volume	حجم الشبكة
Object Oriented	تقنيات الكائنات
Overtaxed	مرهقا

المصطلح بالإنجليزية	معناه بالعربية
Overloaded	حمولة زائدة
Packet Sizes	حزم بيانية
Performance Management	إدارة الأداء
Pie Graphics	رسومات على شكل فطيرة مستديرة
Protocol Stack	مكدس بروتوكولي
Processor Load	حمل المعالج
Response Time	زمن الاستجابة
Rejection Rate	معدل الرفض
Real Data	البيانات الفعلية
Re-arm Values	القيم التأهيلية
RMON	بروتوكول رصد الشبكة عن بعد
Round-Trip Time	زمن دورة الرحلة
Utilization	معدل الاستخدام
Upgrade	تحديث
Sample Interval	مدة العينة
Setting Thresholds	ضبط القيم الحدية
Session	جلسة
Simulation	محاكاة
Stop-and-Wait	توقف–ثم–انتظر
Throughput	سرعة الأداء
Trend Analysis	تحليلات تحديد الاتجاهات
Trend Data	بيانات تحديد الاتجاه
Troubleshooting	تشخيص الأعطال
Window Size	حجم النافذة

المراجع

[1] Performance and Fault Management, by Paul L Della Maggiora (Author), Christopher E. Elliott (Editor), James M. Thompson (Author), Robert L. Pavone Jr. (Author), Kent J. Phelps (Author), Cisco press, 2006.

[2] Intranet Performance Management, by Kornel Terplan – 2000.

[3] System Performance Tuning, by Gian-Paolo D. Musumeci, Mike Loukides – 2002.

[4] Telecommunications Network Design and Management, by Subramanian Raghavan, G. (ed.) Anandalingam – 2003.

[5] Network Management Systems Essentials, by Divakara K. Udupa – 1996.

[6] Networks and Systems Management: Platforms Analysis and Evaluation - Page 329 by Iosif G. Ghetie - Computers – 1997.

[7] Mpls Network Management: MIBs, Tools, and Techniques , by Thomas D. Nadeau – 2003.

[8] Optimizing Network Performance with Content Switching: Server, Firewall and Cache Load Balancing , by Matthew Syme, Philip Goldie - Computers – 2003.

[9] Network Performance Management And Capacity Planning, 2006., www.firewall.cx/ftopict-2820.html - 42k.

[10] Performance and Fault Management, safari.adobepress.com/1578701805.

[11] Network Performance Toolkit: Using Open Source Testing, www.amazon.com/Network-Performance-Toolkit-Source-Testing/dp/0471433012.

[12] Network Management: A Practical Perspective. by Allan Leinwand, Karen Fang-Conroy. Info at Addison-Wesley , 1996.

[13] Internet Sites:-

www.bitpipe.com/rlist/term/Network-Performance-Management-Software.html
\www.lockergnome.com/nexus/it/2006/12/06/application-and-network-performance-management-buyers-guide/
www.amazon.ca/Unix-System-V-Performance-Management/dp/0130164291

[14] Internet Sites on Simulations:

www.amazon.co.uk/Storage-Network-Performance-Analysis-Huseyin/dp/076451685X
www.securitypark.bitpipe.com/rlist/1078177630_947/Network-Performance.html
www.isi.edu/nsnam/ns/ns-documentation.html

www.winlab.rutgers.edu/~zhibinwu/html/network_simulator_2.html

www.ripe.net/ripe/meetings/ripe-51/presentations/pdf/ripe51-network-performance.pdf

www.amazon.com/Network-Performance-Toolkit-Source-Testing/dp/0471433012 -

www.bitpipe.com/rlist/term/Network-Performance-Management-Software.html 2007

www.objs.com/OSA/Network-Performance-Monitor-Service.html

www.podcast.burtongroup.com/ip/files/managing_network_performance_trends_2007.pdf.


الوحدة السابعة
إدارة الحسابات

محتويات الوحدة

مقدمة

تمهيد

عزيزي الدارس،في هذه الوحدة سنتناول إدارة الحسابات واختصاصاتها بقياس استعمالات مصادر الشبكة بواسطة المستخدمين من أجل تحقيق معايير Metrics، وفحص حصص Quotas، وتحديد الأسعار، وفواتير Bills المستخدمين. وتختص إدارة الحسابات بعمليات تجميع البيانات عن معدل استخدام مصادر الشبكة.وضبط استخدامات الحصص Quotas، بواسطة معايير Metrics. ثم تحديد قيمة فاتورة المستخدم Billing ، نظير استخداماته مصادر الشبكة. كذلك سنتناول إدارة الحسابات بتجميع إحصائيات عن الشبكة، ومدي فائدتها في إدارة نظام المصادر، مثل: مساحات أقراص تخزين البيانات، قدرة المعالجة، عمليات التخزين الاحتياطية. في هذه الوحدة نفحص أولا، فوائد إدارة الحسابات، وبعد ذلك الخطوات المتعلقة بتحقيقها. تشمل الوحدة أيضا، شرحاً تفصيلياً لتحديد فواتير دفع المستخدمين، ووصف الأدوات الثلاثة التي يمكن أن تستخدم في إدارة الحسابات، وهي الأداة البسيطة، والمركبة، والمتقدمة. وأخيرا، نناقش طرق فحص وتدوين معلومات الحسابات.

أهداف الوحدة

عزيزي الدارس، بنهاية دراسة هذه الوحدة ينبغي أن تكون قادرا على أن :

- تعرف كيفية تحقيق إدارة الحسابات في نظام إدارة الشبكة.
- تستخدم المعايير القياسية لضبط حصص استخدام الشبكة.
- تعدد الطرق المتعددة لتحديد رسوم الفواتير الخاصة باستخدام مصادر الشبكة.
- توضح أمثلة لبيان طرق إدارة الحسابات في الشبكات.
- تعدد استخدامات الأدوات البسيطة والمركبة والمتقدمة لإدارة الحسابات في نظام إدارة الشبكة.
- تصف الطرق المختلفة لتدوين معلومات الحسابات.

يصف عناصر فاتورة دفع رسوم استخدام الشبكة

1. فوائد إدارة الحسابات

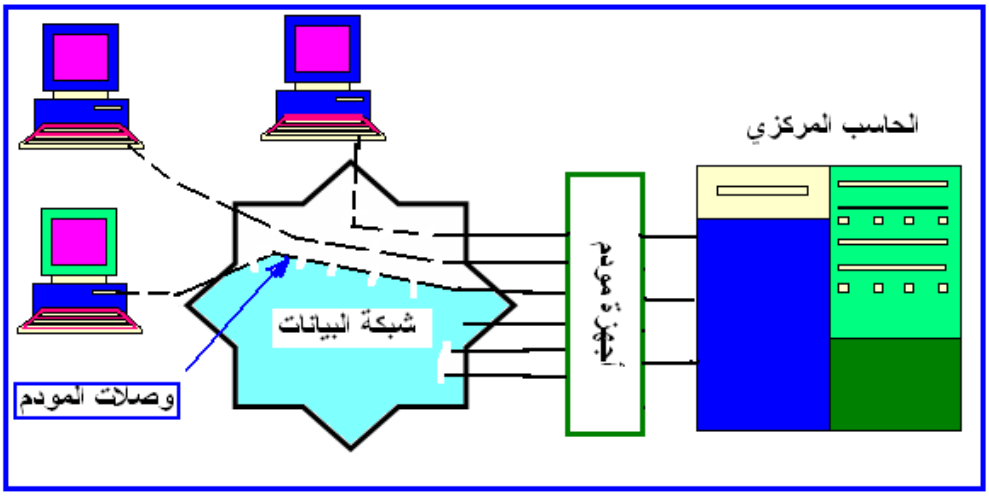
عزيزي الدارس، تساعد إدارة الحسابات مهندس الشبكة في **قياس وتدوين معلومات الحسابات بناء على إرسال بيانات المستخدمين عبر الشبكة**. واستخدام هذه البيانات في تحديد قيمة دفع المستخدمين لفواتيرهم، وتوزيع المصادر، وحساب التكاليف. كما تعزز إدارة الحسابات من فهم مهندس الشبكة لمعدل استخدام مصادر الشبكة، وإنشاء شبكة أكثر إنتاجية.

إن فواتير الدفع للمستخدمين عملية ضرورية لتغطية المصاريف المتعلقة ببناء وصيانة الشبكة. تحتاج معظم المؤسسات عمل نموذج حسابي لاسترجاع النفقات Chargeback، للمساعدة في تغطية تكاليف الإنشاء، والتشغيل، وصيانة شبكة البيانات. تستطيع إدارة الحسابات حساب هذه التكلفة الراجعة، وربطها مع نظام دفع الفواتير، وتوفير المساعدة في توزيع هذه التكاليف بعدالة. يمكن لإدارة الحسابات أيضا، أن تعاون في تحديد الميزانية Budget ، والتخطيط الشخصي Personal Planning. وتنظر المؤسسة غالبا لهذه الاهتمامات الحيوية لإدارة الحسابات، على أنها عظيمة الأهمية، لأنها تسمح بتغطية البنية التحتية Infrastructure للشبكة.

ويمكن بواسطة فحص المعايير والحصص، أن نضمن أن كل مستخدم يمتلك مصادر كافية لتحقيق المهام المطلوبة. يمكن أيضا، الاستعانة بهذه الإحصائيات لمتابعة استخدام المصادر المختلفة للشبكة. على سبيل المثال، يمكن لفريق التوثيق استخدام الشبكة للوصول إلى حاسب النشر في النظام المتصل بخادم التطبيق عند موقع بعيد. باستخدام إدارة الحسابات، نجد أن غالبية حركة المرور داخل الشبكة، تأتي من فريق التوثيق المتصل بخادم التطبيق. يمكن لإدارة الحسابات أن توفر المعلومات التي تسمح لنا باتخاذ قرار بالعلم أن فريق التوثيق يبرر أحقيته في استخدام خادم التطبيقات.

1.1 استخدام إدارة الحسابات في تخصيص مصادر الشبكة

في الوسط المحيط بالشبكة التقليدية، الذي يعتمد على ربط الحاسب المركزي بواسطة جهاز مودم، تستطيع إدارة الحسابات مساعدة مهندس الشبكة في إجراء تخصيص مشاركة الوقت Time-sharing، لمجموعة من الطرفيات، كما هو موضح في شكل 7.1. حيث يتم التحكم في توصيل مجموعة مستخدمين الوحدات الطرفية بوصلات المودم إلى الحاسب المركزي. ويمكن تخصيص أولويات لمجموعة من المستخدمي على الوحدات الطرفية. كما تستطيع إدارة الحسابات تقديم المساعدة في تحديد أو تعديل هذه الأولويات.



شكل7.1 استخدام إدارة الحسابات في تخصيص مصادر الشبكة.

2.1 فهم سلوك المستخدمين في شبكة البيانات

تساعد إدارة الحسابات في فهم سلوك المستخدمين في شبكة البيانات، وربما تسمح لمهندس الشبكة بالتدخل في هذا السلوك، كي يجعل مصادر الشبكة أكثر مثالية. على

سبيل المثال، نفترض موقع شبكة يتكون من خادمات ملفات للحاسبات الشخصية الموزعة، التي تساهم في مهام متعددة في الشبكة، تشمل جدولة الطباعة Print Spoolers على خادمات قاعدة البيانات. بفرض أن خادم الملفات المسمى "ألفا" في شبكة المؤسسة يحتوي معلومات مهمة عن سوق الأسهم في قاعدة البيانات. بفرض أن أحد المستخدمين لخادم الملفات "ألفا"، قرر إجراء عملية نسخ احتياطي لقرص الحاسب الشخصي الخاص به على خادم الملفات "ألفا"، وكانت سعة القرص 40 ميجابايت. يبدأ المستخدم إجراء عملية النسخ الاحتياطي، ثم يترك المكتب لمدة الليلة. بعد الانتهاء من عملية النسخ الاحتياطي، أصبحت الذاكرة المتبقية على خادم الملفات "ألفا" هي واحد ميجابايت. في صباح اليوم التالي، يقوم الخادم "ألفا" بتنفيذ برنامج لتجميع معلومات مهمة عن سوق الأسهم من جهاز خادم آخر في الشبكة، لكن بينما يقوم بتحميل هذه البيانات، تمتلئ مساحة قرص التخزين في الخادم "ألفا" ، وتتوقف عملية النقل.

بعد مضي عدة ساعات، عندما يحاول بعض الموظفين في المؤسسة استرجاع معلومات الأسهم، تصلهم رسالة خطأ. لفحص المشكلة، يقوم مهندس الشبكة بفحص إحصائيات إدارة الحسابات على الخادم "ألفا"، ويلاحظ أن أحد المستخدمين قد قام بتحميل عدد من الملفات استغرقت وقتا طويلا أثناء الليل. يوجد أمامنا الآن بعض الاختيارات، تعتمد على الوسائل المتوفرة في عمل الشبكة. ربما نقوم بالاتصال بالمستخدم، أو إبلاغ المعلومات إلى مدير النظام المسئول عن الخادم "ألفا"، لاتخاذ الإجراءات المناسبة.

3.1 تحديد المكان الذي يتم فيه تخصيص مصادر الشبكة

وبسبب أن تقنيات الشبكات تتطور بسرعة، فإن أساليب إدارة الحسابات تستخدم أيضا في تحديد المكان الذي يتم فيه تخصيص مصادر الشبكة، بحيث تكون ذات جدوى اقتصادية، على حسب التقنيات المختلفة. نفترض مؤسسة تحدد تكلفة تشغيل شبكة بيانات إقليمية تمتلكها، وتستخدم دوائر مؤجرة مخصصة للبيانات، على أساس شهري، من أحد الموردين. بسبب أن هذه التكاليف المرجعية Recurring Cost تمثل جزءاً كبيراً من

ميزانية المؤسسة، يتم دفعها شهريا لتشغيل شبكة البيانات الإقليمية. فإن استخدام التقنيات ذات الجدوى الاقتصادية Cost-effective يكون دائما أحد العوامل الهامة.

4.1 استخدام التقنيات ذات الجدوى الاقتصادية

بالاستعانة بالتكلفة المرجعية فقط كأساس، وكمية البيانات التي تنقلها الشبكة في الشهر، فإن المؤسسة تستطيع حساب كمية النقود التي تدفعها لنقل حرف واحد من البيانات عبر الشبكة الإقليمية. بسبب أن المؤسسة، تريد نقل أقصى كمية ممكنة من البيانات لكل قرش تدفعه في التكلفة المرجعية، فإن مهندس الشبكة ربما يقرر استخدام شبكة إقليمية ذات تقنية جديدة. باستخدام على سبيل المثال، نظام ترحيل الأطر Frame Relay، أو نظام نمط الاتصال غير المتزامن ATM. بعد إنشاء الشبكة الإقليمية الجديدة، تستطيع المؤسسة إعادة حساب دراسة الجدوى الاقتصادية للشبكة. من هذا المثال، نجد أن إدارة الحسابات، قد ساعدت المؤسسة في اتخاذ قرار مبني على أساس اختيار تقني.

2. تحقيق إدارة الحسابات

2 .1 تتكون إدارة الحسابات من الخطوات التالية

- تجميع البيانات عن معدل استخدام مصادر الشبكة.
- استخدام المعايير للمساعدة في توزيع حصص الاستخدام.
- حساب وإصدار فواتير الدفع للمستخدمين نظير استعمالهم للشبكة.

1.1.2 تجميع بيانات معدل استخدام الشبكة

للحصول على معلومات عن الحصص والمعايير، نحتاج تجميع بيانات إدارة الحسابات بشكل دائم، مرة أو مرتين يوميا. كما نحتاج استرجاع بيانات الفواتير. إذا كانت أجهزة الشبكة تستطيع تخزين كميات كافية من البيانات، فإن الاسترجاع الدوري لهذه البيانات ربما يواجه صعوبة. عندما تقوم الشبكة بتدعيم العمل بواسطة بروتوكول إدارة الشبكة

المعروف SNMP ، فإن عدادات استرجاع البيانات تستطيع أن تعد إلى قيم كبيرة كافية. قد نحتاج أيضا، تجميع بيانات عن أجهزة الشبكة، ويشمل ذلك عدد الحروف أو حزم البيانات المرسلة والمستقبلة. يمكن تجميع هذه البيانات بواسطة الاستفسار من أنشطة ملفات التسجيل Logs الموجودة على الحاسبات المضيفة، أو تجميع حركة مرور البيانات من أجهزة الشبكة مثل الجسور، والمجمعات والموجهات.

2.1.2 استخدام المعايير وضبط الحصص

تساعد المعايير في تحديد المدى المتاح للمستخدم لمصادر الشبكة. على سبيل المثال، تستطيع هذه المعايير تبيان عدد الوصلات المخصصة لخادم الطرفيات، عدد العمليات التي تمر من شبكة البيانات لتصل إلى قاعدة بيانات محددة ، أو زمن الدخول الكلي بواسطة مستخدم للحاسب العملاق Supercomputer. كجزء من استخدام إدارة الحسابات، يمكن تحديد مصادر الشبكة التي نريد قياسها، وبعد ذلك نبدأ تجميع المعايير عن استخدامها.

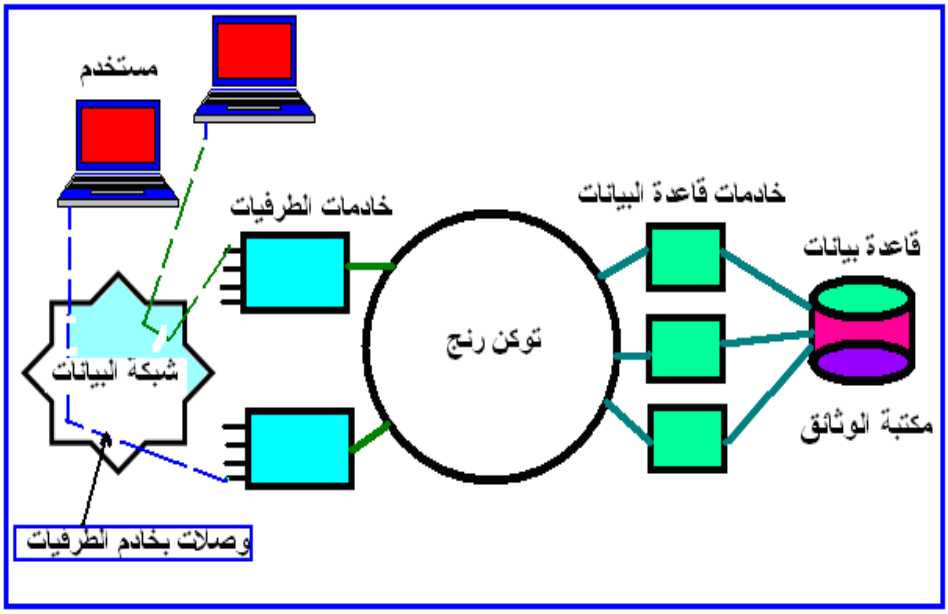
ويوجد بعض الوثائق المنشورة الخاصة بالمعايير وضبط الحصص،منها، الوثيقة رقم RFC-1272 وتعني بطلبات التعليق Request For Comments، وعنوانها حسابات الانترنت. وهي تركز على إعطاء خلفية معلوماتية مطلوبة لتعريف الخدمات المراد قياسها، وتدوين استخداماتها. وهذه الوثيقة تعرض أيضا العوامل المهيمنة Dominant Factors المقابلة لعمليات الحسابات. إن نموذج الحسابات العام المقدم في الوثيقة RFC-1272، يعرف أنواع المعلومات الضرورية في المستويات المختلفة لمكدس بروتوكولي Protocol Stack.

ويساعد استخدام **المعايير والحصص**، ضمان أن كل مستخدم يحصل على مشاركة عادلة Fair Sharing لمصادر الشبكة. يمكننا تخصيص الحصص، وبعد ذلك يتم مجازاة المستخدمين الذين يجتازون هذه الحصص. على سبيل المثال، بواسطة حرمانهم من

استخدام مصدر الشبكة المخصص لهم. أحد العقوبات الأخرى المعروفة، هي أن يتم زيادة فاتورة الدفع الخاصة بالمستخدمين الذين تخطوا حصصهم.

مثال: توصيل مستخدمين بقاعدة بيانات المعلومات:

من الشائع، توصيل المستخدمين بأحد الحاسبات الضخمة، المتصلة بقاعدة بيانات المعلومات، من خلال شبكة البيانات. ربما تقوم المؤسسة التي تمتلك قاعدة البيانات، بعد ذلك بطلب التكلفة من المستخدمين نظير هذه الخدمة. يوجد في أحد أجزاء الشبكة، مجموعة من المستخدمين تحتفظ بالاتصال بقاعدة بيانات مكتبة الوثائق، كما هو مبين في شكل 7.2. يقوم المستخدمون بدفع أجرة الاتصال Access Fee نظير الاتصالات التليفونية للمكتبة. كل مساهم في الشبكة، يسمح له باستخدام المكتبة لمدة عشرة ساعات أسبوعيا. على الرغم من أن هذا قد يبدو وقتا قصيرا، لكن المستخدمين يقومون بالدخول إلى المكتبة للبحث عن البيانات، وتحميل المعلومات، وبعد ذلك تتم عملية خروجهم. يستخدم وقت الاتصال المباشر، في البحث عن البيانات ونقل وتحميل المعلومات، أما عمليات التصفح والمطالعة بإمعان لهذه المعلومات، فتتم بعد فصل الاتصال عن الشبكة .



شكل7.2 يتم توصيل المستخدمين بقاعدة بيانات مكتبة الوثائق
من خلال وصلات مودم وخادمات الطرفيات.

تحدد المؤسسة التي توفر هذه الخدمات، أن معيار عشر ساعات، هو وقت مناسب لمعظم العملاء. وأن العميل الذي تتخطى استخداماته هذه الحصة، سوف يدفع رسوماً شهرية أكبر ، حسب كمية الوقت الإضافي الذي يستخدمه.

3.1.2 رصد المستخدمين

من مهام مهندس الشبكة، أن يتابع أداء هذه الخدمات في الشبكة، وأن يقوم برصد المستخدمين المتصلين بأجهزة المودم. تقوم أجهزة خادمات الطرفيات، بعد ذلك بتوصيل أجهزة المودم إلى الشبكة الرئيسية، حيث توجد حاسبات قاعدة البيانات. يستطيع مهندس الشبكة، على أساس زمني، الاستفسار من خادمات الطرفيات، لمعرفة العملاء المتصلين بالشبكة، والمدد الزمنية المخصصة لهم. يقوم المهندس بعد ذلك، بتحديد العدد الأكبر من المستخدمين لقاعدة البيانات، ويحسب متوسط زمن الاتصال لكل مستخدم، والفترة الزمنية التي تم فيها استقبال مكالمات بأعلى معدل. إذا كانت خادمات الطرفيات المتصل

بها المستخدمون متصلة بملف نظام إدارة الشبكة، فإن مهندس الشبكة سوف يحتاج فقط كتابة برنامج لإحضار هذا السجل، ويستخرج منه هؤلاء المستخدمين. ربما تكون الوسيلة المثالية لتنفيذ ذلك، هو كتابة برنامج لاستخراج المعلومات من سجل النشاط Activity Log ، ووضعه في قاعدة بيانات نظام إدارة الشبكة. يستطيع مهندس الشبكة بعد ذلك، استخدام لغة الاستفسار الهيكلية SQL لفحص الحصص، وتوليد تقارير النشاط Activity Reports.

2.2 تحديد قيمة فواتير الاستخدام

يحتاج مهندس الشبكة عادة، تجميع بيانات فواتير الدفع بطريقة منتظمة. معظم أجهزة الشبكة بها عدادات إحصائية تمكن مهندس الشبكة من إجراء عملية التصويت Polling، على الجهاز للحصول على المعلومات بصورة دائمة، وملاحظة التغيرات منذ لحظة حدوث التصويت الأخير. لمساعدة مهندس الشبكة في تنفيذ هذه المهمة، يمكن لجهاز الشبكة أن يحتفظ بجدول حسابات يسجل عنوان المصدر والهدف، وكذلك عدد العمليات، حزم البيانات، الحروف المرسلة، والحروف المستقبلة. يتم غالبا تحديد قيمة الفواتير بناء على طريقتين هما:

- رسوم فترة زمنية واحدة نظير التركيب كل شهر.
- تحديد الرسوم بناء على كمية مصادر الشبكة المستهلكة.

3.2 رسوم فترة زمنية واحدة نظير التركيب شهريا

في هذه الطريقة، يتم تحديد فاتورة المستخدم بناء على تركيب وصلة الشبكة، بالإضافة إلى رسوم قياسية نظير الاستخدام عن كل شهر. إن إدارة الحسابات ليس من الضروري أن تكون من أجل الفواتير، لأنها لا تتطلب معلومات من الشبكة. على الرغم من ذلك، فإن هذا النظام من السهل جدا تنفيذه، لكنه قد يصبح صعبا للحكم عل مستخدم يقوم باستخدام الشبكة باستمرار، ومستخدم آخر يستخدمها بشكل عادي، وتم تخصيص نفس قيمة الفاتورة لكليهما.

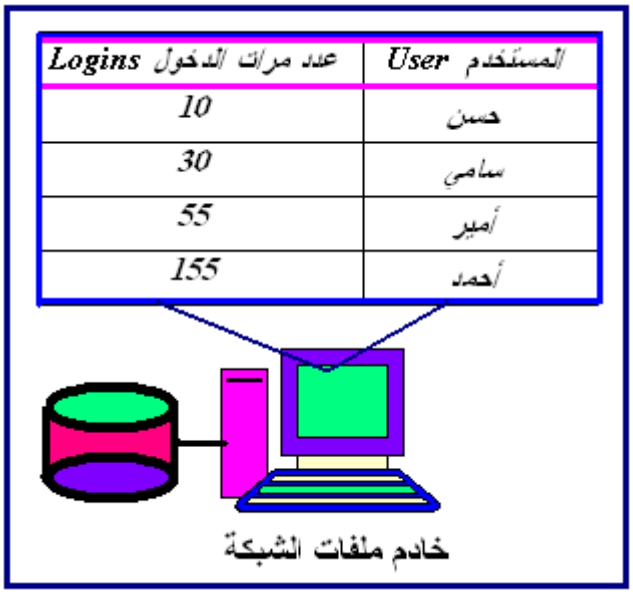
4.2 تحديد الرسوم بناء على كمية مصادر الشبكة المستهلكة

تستخدم بعض المؤسسات هذه الطريقة مع ربطها بتكلفة صغيرة للتركيب، ورسوم شهرية. يتطلب تنفيذ هذه الطريقة بيانات إحصائية عن معدل استخدام العميل للشبكة. تستخدم المعايير التالية، إما فرادى أو معا، لقياس وتحديد استخدامات مصادر الشبكة وهي: إجمالي عدد العمليات، إجمالي الحزم، وإجمالي الحروف. يتم قياس إجمالي الحزم أو إجمالي الحروف، إما بناء على مداخل Inputs المستخدم للشبكة أو مخارج Outputs لمستخدم من الشبكة.

بواسطة **عد إجمالي عدد العمليات لكل مستخدم**، تستطيع المؤسسة، قياس عدة معايير، تشتمل على: عدد مرات الدخول إلى خادم الحساب، الاتصالات التي تمت من المحكمات الطرفية، رسائل البريد الإلكتروني المرسلة، وعدد جلسات الدخول عن بعد التي تم إجراؤها... الخ.

مثال: طريقة إجمالي عدد العمليات لكل مستخدم:

يوضح شكل 7.3 مثالاً على طريقة تصميم وتحديد الرسوم بهذه الطريقة. على الرغم من أن هذه الطريقة سهلة التنفيذ نسبيا، فإن كل عملية ينتج عنها نفس كمية التكلفة، بغض النظر عن الوقت، أو مصادر الشبكة المستخدمة. بذلك إذا قام أحد العملاء بإجراء عملية منفردة لإرسال 500 ميجابايت من المعلومات، فإن هذا العميل سوف يدفع نفس رسوم مثل عميل آخر قام بإرسال 100 بايت لرسالة بريدية. يمكن لكثير من العملاء الاعتراض على هذه الطريقة في تحديد الرسوم.



شكل7.3 يوضح نموذج تحديد فاتورة التكاليف للمستخدمين، بناء على عدد مرات دخولهم خادم الحسابات، حيث تعبر عدد مرات الدخول عن استعمال مصادر الشبكة.

5.2 طريقة العد الإجمالي لعدد الحزم

في هذه الطريقة يتم عد إجمالي لعدد الحزم، وهذا يبين استخدام الشبكة. ثم تزداد الفاتورة، عند كل مرة يرسل المستخدم، أو يستقبل حزمه. من عيوب هذه الطريقة، أن الفاتورة لعدد معلوم من الحزم تكون واحدة، بغض النظر عن كمية المعلومات المرسلة أو المستقبلة. على سبيل المثال، ربما يقوم أحد المستخدمين بإرسال حزم قصيرة لحركة مرور تفاعلية التي لا تمثل عبأ على وصلات أو أجهزة الشبكة. لكن مستخدم آخر، ربما يقوم بإرسال ملف يعتمد على حزم ضخمة. إذا كان كل من حركة المرور التفاعلية، وملف النقل تحتاج 1000 حزمة لإتمامهما، فإن الفاتورتين سوف تتوافقان. لكن ، لا يتم الإجراء كذلك ، إن ملف النقل ذو الحزم الضخمة، سوف يستخدم مصادر أكثر من الشبكة، على الرغم من أنه يدفع نفس الفاتورة، مثل حركة المرور التفاعلية، التي تستخدم مصادر أقل.

دفع الفاتورة الإجمالية حسب الحروف المستخدمة:

يمكن **تجنب عيوب الطريقتين السابقتين** بواسطة دفع الفاتورة الإجمالية للحروف المستخدمة، يقوم المستهلك بالدفع حسب كمية مصادر المستخدم للشبكة. تشمل هذه المصادر: سعة النطاق، والحروف المستهلكة (حرف–حرف أو بيت–بيت)، وليس من الضروري على أساس الحزم. القرار التالي الذي يجب اتخاذه هو هل يتم تحديد الفاتورة بناء على إجمالي عدد الحروف المرسلة أم الحروف المستقبلة؟

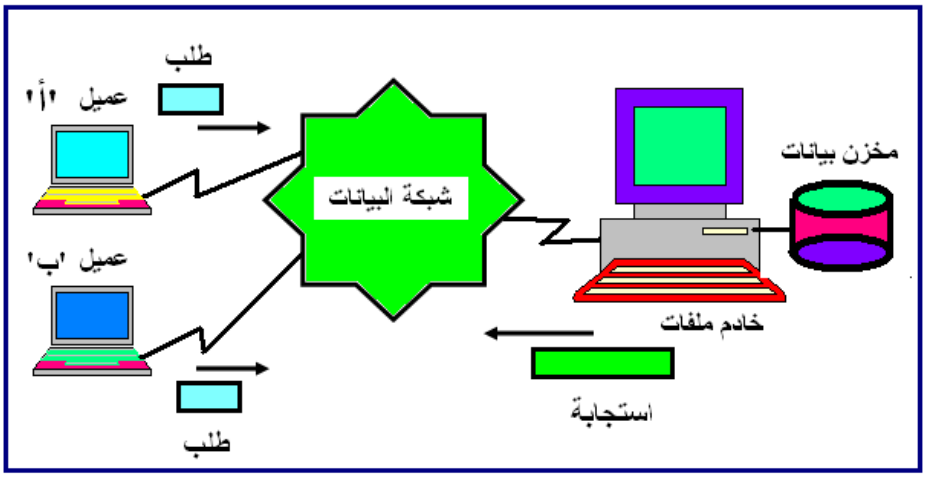
إن تطبيقات الشبكة التي تستخدم **بروتوكول طبقة النقل الاعتمادي**، مثل TCP أو بروتوكول شبكة نوفيل SPX ، يتم تأكيد حزم البيانات المستقبلة من الهدف بواسطة **حزم إعلام** Acknowledgement Packets. في هذه التطبيقات، يتم فقط عد الحروف في حزم البيانات، وهذا منطقي ومعقول، لأنها الحزم الأكبر التي تستهلك مصادر شبكية أكثر. أما التطبيقات التي لا تستخدم طبقة النقل الاعتمادي، تحتاج منا أن نقوم فقط بعد الحروف في اتجاه واحد عبر الشبكة.

كثير من الوسائط المحيطة، تقوم بدمج التطبيقات التي تستخدم طبقة النقل الاعتمادي والتطبيقات التي لا تستخدمها. معظم المؤسسات تختار طريقة تحديد فاتورة الدفع على أساس الحروف المستقبلة من الشبكة، والحروف المرسلة إلى الشبكة، أو الدمج بينهما. يوجد مميزات واضحة لكل من هذين الأسلوبين، بالتماشي مع الخروق المصاحبة.

طريقة تحديد فاتورة الدفع بناء على الحروف المرسلة:

إن طريقة تحديد فاتورة الدفع بناء على الحروف المرسلة إلى شبكة البيانات بديهي ومعقول. عندما يقوم المستخدم بإرسال أشياء عبر الشبكة، فإن الفاتورة ينبغي أن تزداد. لسوء الحظ، في نموذج شبكة الخادم/ العميل، الشائعة، فإن هيكلية تحديد فاتورة الدفع يوجد بها بعض الخروق الخطيرة. إن تحديد فاتورة الدفع على أساس الخرج يؤدي إلى عدم تشجيع المستخدم من عرض الخدمات من أجهزة الخادم التي يملكونها. لتوضيح ذلك، نفترض أن أحد المستخدمين على الشبكة يمتلك خادم ملفات يحتوي بيانات مهمة

لمشروع بحثي. وأن العديد من المستخدمين تم توصيلهم بخادم الملفات، ويقومون بتحميل كمية ضخمة من المعلومات يوميا. وهؤلاء الذين يجمعون المعلومات، يرسلون حزماً صغيرة إلى أجهزة الخادمات، لطلب معلومات. يقوم خادم الملفات بعد ذلك بنقل كمية ضخمة من البيانات وترجيعها إلى المستخدم، كما هو موضح في شكل7.4. إذا تم تحديد فاتورة الدفع بناء على الحروف الخارجة، فإن المستخدم الذي يوفر المعلومات سوف يستلم فاتورة ضخمة، التي بدورها تسبب أن المستخدم الذي يقوم بتشغيل خادم الملفات، سوف يطلب من مستخدميه بدفع فاتورة تغطي هذه التكاليف.



شكل7.4 يستقبل خادم الملفات طلبات رجاء تحقيق اتصال صغيرة الطول، بينما يرجع استجابات طويلة. وهذا يسبب زيادة فاتورة المستخدم.

تحديد قيمة فاتورة الدفع بناء على الحروف المستقبلة:

عزيزي الدارس، إن تحديد قيمة فاتورة الدفع بناء على الحروف المستقبلة من الشبكة يمنع هذه المشكلة السابقة. حيث لا يوجد فاتورة تدفع لإرسال كمية ضخمة من البيانات إلى الشبكة، بل فقط عند استقبالها.

في تشغيل الشبكات الكلاسيك (العريقة)، التي يتم فيها **تحديد الفاتورة بناء على الحروف المستقبلة** – بشكل مناسب، نفترض وجود مركز بيانات رئيسي في الشبكة. يوجد عند هذا الجانب حاسب كبير من نوع IBM، يسمى "الأمل". يتم توصيل العملاء إلى حاسب

"الأمل" من خلال حاسبات المقدمة–المؤخرة، التي توصل إلى مجموعة من المحكمات إلى الطرفيات الموزعة خلال شبكة حلقية من نوع توكين رينج Token Ring. في هذه الشبكة يقوم جزء من الوحدات الطرفية بالإرسال إلى حاسب "الأمل"، وأن معلومات نفايات مهملة Dumps ضخمة يرجع يستقبلها حاسب "الأمل" ليوصلها إلى الوحدة الطرفية.

يستطيع كثير من المستخدمين في العديد من الأوساط المحيطة بالشبكة، تهيئة الحاسب المضيف **لتسمح بالتوصيل إلى ملفات معينة دون الاحتياج إلى تصريح**. من الشبكات التي تستخدم بروتوكول الانترنيت IP، يتم تحقيق هذه الطريقة من خلال بروتوكول نقل الملفات FTP باستخدام طريقة "Anonymous". في شبكات أبل توك AppleTalk، يتم تحقيق نفس التأثير من خلال مشاركة المجلدات Folders. في شبكات خادم ملفات شبكة نوفيل، يمكن ترك الدليل متاح للعملاء من أجل وضع أو استقبال بيانات. معظم هذه الخدمات، يتم تصميمها لتحقيق مكان مخصص للعملاء لأخذ الوثائق والتطبيقات. بواسطة دفع فواتير المؤسسة على أساس استقبال الحروف من الشبكة. تستطيع الشبكة المساعدة في تأمين المستخدم الذي يوفر الخدمة، بحيث لا يستقبل فاتورة ضخمة آليا.

عيوب طريقة الدفع على أساس الحروف المستقبلة:

إن طريقة الدفع المبنية على أساس الحروف المستقبلة يوجد بها بعض الخروق.

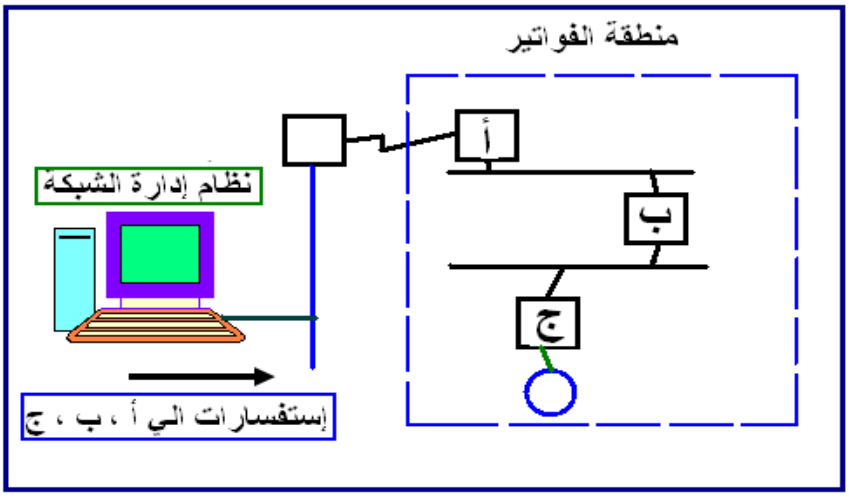
أولا: يوجد العديد من بروتوكولات الشبكة ترسل **رسائل إعلام** من الهدف إلى المصدر. ينتج عن ذلك أن المستخدمين الذين يوفرون هذه الخدمات للشبكة تستقبل حروف بيانات غير مطلوبة من الشبكة. لحسن الحظ، أن حزم الشكر تكون عادة ذات أطوال صغيرة للغاية. يمكن إهمال هذه الحروف، لكن باستخدام الإحصائيات عن أجهزة الشبكة، نستطيع حساب إجمالي عدد الرسائل المرئية. أيضا، أن المؤسسة

التي تحسب فواتير الدفع، تستطيع تذكير المستخدمين الذين يوفرون هذه الخدمات للشبكة، ومن الممكن أن توفر لهم تخصيص خصومات على فواتير الدفع.

ثانيا: مشكلة أخرى خاصة بطريقة تحديد فاتورة الدفع بناء على طول الحروف المستقبلة من الشبكة، هي **حدوث البيانات التي لم تطلب** Unsolicited Data، مثل البريد الإلكتروني. حيث تضاف إلى فاتورة دفع المستخدم. ربما يمكن للمؤسسة أن تتغاضى عن هذه الخروقات، بسبب أن العديد من المستخدمين ويرسلون ويستقبلون البريد بنفس المعدل. لكن ليست هذه هي الحالة، عندما يكون المستخدم على قائمة البريد ويستقبل العديد من الرسائل البريدية. بسبب أن المستخدم يكون على القائمة البريدية لأحد الأسباب، فإن فاتورة الدفع ينبغي أن تعكس استقبال هذه البيانات نتيجة خدمة هذه الشبكة. لسوء الحظ، إن نمو شبكة الانترنيت قد أدى إلى نمو طردي في حدوث نفايات بريدية Junk e-Mail غير مطلوبة، يمكنها أن تغرم المستخدمين بسبب نظام دفع الفواتير حسب طريقة الحروف المستقبلة.

ثالثا: أحد العيوب الأخرى الممكنة لهذه الطريقة في تحديد قيمة فواتير الدفع طبقا للحروف المستقبلة، تنتج عن أن **كل مستخدم يستلم بيانات من الشبكة، عندما تقوم المؤسسة برصد الشبكة لأسباب إدارية**، كما هو مبين في شكل 7.5. على الرغم من أن معظم هذه البيانات سوف يتم إرسالها إلى المستخدم بطريقة منتظمة، ولفترة زمنية محددة. يمكن إجراء الاستفسارات Queries مرة في اليوم، أو في الساعة، أو كل بضع دقائق. من الممكن حساب عدد الاستفسارات النوعية التي يتم إرسالها خلال فترة دفع الفواتير، وكم عدد الحروف التي تحتويها. إذا كانت المؤسسة تحدد دفع الفواتير شهريا، يمكن بسهولة حساب متوسط عدد الاستفسارات خلال الشهر(على سبيل المثال، فإن الاستفسار الواحد الذي طوله 500 حرف يتم إرساله كل خمسة دقائق). عندما يقوم مهندس الشبكة بفحص مشاكل الشبكة، يتم طرح هذه الحروف من قيمة كل فاتورة، وكذلك كل الحروف

الأخرى التي ينبغي حدوثها ويتم إرسالها لأسباب إدارية، والتي تؤدي خدمة للمستخدم.



شكل7.5 يمكن لاستفسارات نظام إدارة الشبكة أن تزيد عدد الحروف التي تستقبلها منطقة الفواتير، وهذه الحروف تضاف لإجمالي فاتورة العميل.

أسئلة تقويم ذاتي

أذكر مزايا وعيوب طرق حساب فاتورة مستخدم الشبكة نظيراستعمال مصادر الشبكة بواسطة :

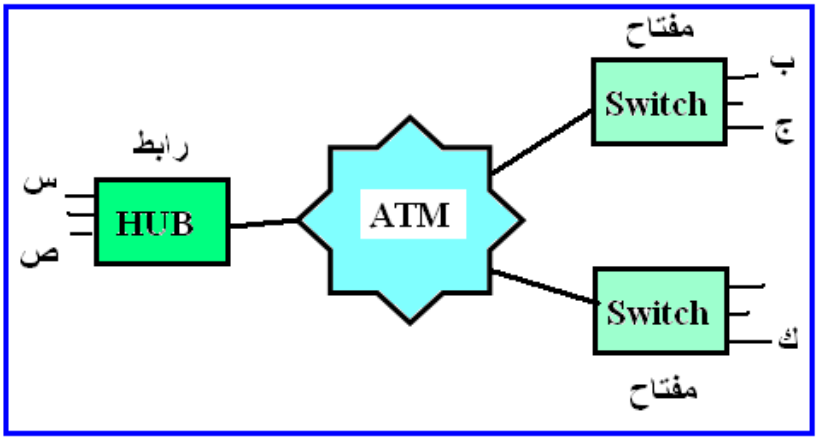
أ- طريقة عدد الحروف المرسلة إلى الشبكة.

ب- طريقة عدد الحروف المستقبلة من الشبكة.

3. إدارة الحسابات في الشبكة المحلية التخيلية

عزيزي الدارس، كما شرحنا، إن تنفيذ نظام دفع الفواتير المبني على أساس المصادر، يتطلب استخدام إدارة الحسابات لتجميع الإحصائيات المطلوبة. بعد ذلك ينبغي على المؤسسة أن تحصل على مصادر المعلومات، ومعالجتها، وتنشئ فواتير الدفع بناء على المصادر المستهلكة. على الرغم من أن هذه العملية ربما تبدو صعبة، فإنها ربما تكون أكثر صعوبة في الشبكات المحلية التخيلية Virtual LANs.

إن تقنيات الشبكة المحلية التخيلية تقوم بالتوصيل المنطقي لأجهزة الشبكة المحلية عند المواقع الفعلية المختلفة، لتكوين شبكة محلية منطقية واحدة، كما هو مبين في شكل 7.6. في الواقع، فإن الأجهزة الفعلية ربما يتم ربطها عبر شبكة ذات سرعة عالية باستخدام نظام نمط الاتصال غير المتزامن ATM أو نظام وحدة مواجهة بصرية لتوزيع البيانات FDDI ، أو ربطها إلى نفس أجهزة الشبكة. يوجد بالأسواق العديد من الموردين تمتلك برامج تشغيل الشبكة المحلية التخيلية وتكوين شبكات محلية تصورية متعددة.



شكل7.6 تسمح تقنيات الشبكة المحلية التخيلية للمحطات س،ص،ب،ج،ك

أن تنتمي لنفس الشبكة المحلية، على الرغم من وجودهما فعليا في أماكن متفرقة.

نفترض شبكة محلية تخيلية، تقوم بتوصيل العديد من المستخدمين من خلال مفتاح من نوع ATM Backbone . وأن هذه الشبكة تمكن العديد من المستخدمين الموجودين في مواقع بعيدة أن تربط منطقيا على نفس قطاع الشبكة المحلية. للمساعدة في إجراء إدارة الحسابات، فإن أجهزة مفتاح ATM ، ينبغي أن تكون قادرة على عد حركة المرور المرسلة والمستقبلة بواسطة كل قطاع في الشبكة المحلية التخيلية. يمكن تخصيص خادم إدارة مركزي لتحقيق إدارة الشبكة المحلية التخيلية. يمكن تجميع التبولوجي اللازمة

للشبكة المحلية التخيلية من الخادم المركزي، وبعد ذلك تجميع إحصائيات حركة المرور من مفتاح ATM المصاحبة لها.

يمكن توظيف بروتوكول الجيل الثاني للانترنيت IPng ويعرف أيضا باسم IPv6 ، المقترح من قبل جمعية الشبكات، ليعمل كبروتوكول طبقة شبكية ليحل محل البروتوكول IP . وتوضح الوثيقة رقم RFC-1672 عمل إدارة الحسابات الخاصة بالبروتوكول IPng . حيث يتم إضافة علامة حسابات An Accounting Tag ، لتحديد عنوان المصدر الذي يرسل الحزم، ومن الممكن إضافة معلومات عن بيانات التطبيقات في المستوى الأعلى خلال الحزمة. يمكن أن يكون متاحا في الأسواق مكدسات بروتوكولية Protocol Stacks خاصة تقوم بتنفيذ البروتوكول IPng.

4. إدارة الحسابات في نظام إدارة الشبكة

يعتمد تحقيق إدارة الحسابات على الوظائف الثلاثة التي يتيحها مستوى الأداة لمهندس الشبكة. في الجزء التالي من هذه الوحدة الدراسية، نشرح ثلاث أدوات يستطيع مهندس الشبكة استخدامها لتحقيق إدارة الحسابات في الشبكة.

1.4 الأداة البسيطة لإدارة الحسابات

ينبغي أن تمكن الأداة البسيطة مهندس الشبكة من رصد الشبكة للحصول على أي معيار يزيد عن الحصة المخصصة. يمكن تخزين بيانات المعيار في قاعدة بيانات علائقية، والتي هي جزء من بناء نظام إدارة الشبكة، ويمكن أن يتم تهيئة هذا المعيار من قبل مهندس الشبكة. لتحديد عدم تخطي الحصص، يمكن لمهندس الشبكة استخدام لغة SQL للاستفسار، ويمكن للأداة أن تظهر نتائج الاستفسارات. كحل آخر بديل، يمكن لمهندس الشبكة، أن يستخدم تقنيات قاعدة البيانات وتوليد تقارير بطريقة آلية عندما يتم تخطي الحصص.

على سبيل المثال، عندما يحتاج مهندس الشبكة، رصد عدد المستخدمين على خادم التطبيقات، يمكن إعلام الأداة البسيطة بالاستفسار عن خادم التطبيقات مرة كل ساعة، وتحديد عدد المستخدمين، بعد ذلك يتم وضع البيانات في قاعدة البيانات العلائقية. بعد ذلك، يقوم المهندس بإعلام الأداة البسيطة بالبحث في قاعدة البيانات العلائقية بواسطة الأمر التالي بلغة SQL:

```
SELECT time, number-users FROM system-
```

يمكن للأداة بعد ذلك، إظهار كل ساعة، عدد المستخدمين الذين يستخدمون خادم التطبيقات. يوضح جدول 7.1 عينة من نتائج الاستفسارات SQL. بسبب أن بيانات المعيار تخزن في قاعدة البيانات العلائقية، يمكن عرض هذه الإحصائيات واستخدامها في تحقيق المعايير والحصص لأقصى عدد من المستخدمين المتصلين بخادم التطبيقات.

جدول1 نتائج الاستفسار باستخدام SQL

الوقت	عدد المستخدمين
8:00AM	10
9:00 AM	20
10:00 AM	25
11:00 AM	30
12:00 PM	15

بالمثل، عندما يريد مهندس الشبكة، معرفة متى تم توصيل أحد المستخدمين إلى خادم ملف معلومات سوق الأسهم المسمى"الأمل"، لمدة أكثر من ثلاثة ساعات. يمكنه استخدام الأداة البسيطة، لرصد هذا الإحصاء بواسطة إخبار الأداة بإجراء هذا الاستفسار من "الأمل" كل خمسة عشر دقيقة لكل المستخدمين الحاليين لخادم الملفات. تقوم الأداة البسيطة، بعد ذلك بتخزين هذه المعلومات في قاعدة البيانات العلاقية. الاستفسار SQL التالي ينشئ معلومات الحسابات اللازمة من جدول دخول المستخدمين في قاعدة البيانات:

SELECT user, hours-connected FROM user-logins WHERE hours-connected > 3

وطبقا لهذا، فإن الأداة البسيطة ستبين اسم المستخدم، وعدد ساعات الاتصال، إذا كانت أكثر من ثلاثة، كما هو مبين في جدول 7.2.

أحد عيوب الأداة البسيطة هي أنه يجب أن يقوم مهندس الشبكة، بإجراء استفسارات SQL. يوجد أدوات لتشغيل الاستفسارات عند فترات منتظمة بواسطة قاعدة البيانات، لكن من المفيد أن توجد طريقة يتم بواسطتها توليد التقارير من قاعدة البيانات، فقط عندما يتم تجاوز الحصص. وهذه الطريقة يمكن أن تكون مفيدة لإدارة الأمن (مثل إيجاد محاولات الدخول غير الناجحة)، ومفيدة لإدارة الحسابات (لإيجاد متى تم تجاوز الحصص). لهذا تستطيع العديد من قواعد البيانات تشغيل مقادح Triggers التي تحدث فعل Action بناء على استفسار SQL. إن الأداة البسيطة يمكنها أن تشغل مقادح قاعدة البيانات، عندما يحدد لها مهندس الشبكة بأنه يرغب معرفة متى تم تخطي الحصص.

جدول2 معلومات الحسابات المنتجة من
قاعدة بيانات جدول دخول المستخدمين

المستخدم عن بعد	عدد ساعات الاتصال
أحمد	9.30
أمير	5.55
علي	6.80
سامي	7.40
حسن	4.20

إن الأداة البسيطة تعتمد على تقنيات قاعدة البيانات. وينبغي على قاعدة البيانات أن تسمح باستفسارات SQL هلامية ad-hoc ، وعمل فورمات للنتائج، وكذلك عمليات القدح. إن هذه الوظائف توجد في العديد من منتجات قواعد البيانات المعروفة مثل

أوراكل Oracle، وسايبس Sybase، ونظام انجريس Ingres ، على سبيل الأمثلة لا الحصر. عندما يستخدم نظام إدارة الشبكة قواعد البيانات هذه، فإن إنتاجية الأداة البسيطة ينبغي أن يسهل نسبيا.

2.4 الأداة المركبة لإدارة الحسابات

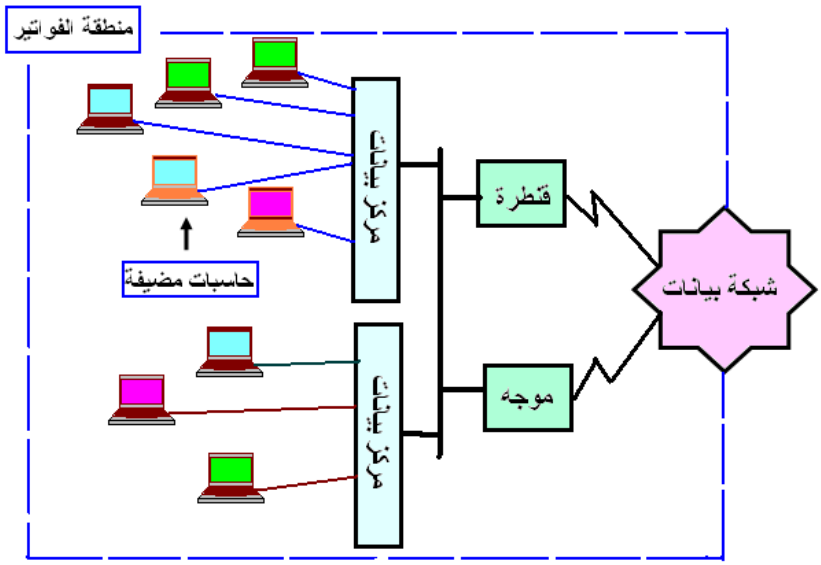
ينبغي على الأداة المركبة أن تمكن مهندس الشبكة من **إجراء عملية تحديد فاتورة الدفع**. إن عملية تحقيق فاتورة الدفع في شبكة البيانات يمكن أن تكون صعبة للغاية وتتطلب وقتا. تستلم الأداة المركبة الدخل من تبولوجي شبكة بيانات مجالات الفواتير Billing Domains، ثم تحسب بعد ذلك قيمة فواتير الدفع لكل مستخدم. تحتاج الأداة المركبة البيانات من إدارة النظام ومن مهندس الشبكة لأداء عملها. ينبغي أن تكون الأداة قادرة على الحصول على التبولوجي من قاعدة البيانات؛ العلائقية من نظام إدارة الشبكة. بسبب أن الخريطة الهرمية لنظام إدارة الشبكة يكون داخل قاعدة البيانات؛ فإن هذه المعلومات أيضا ينبغي أن تكون متاحة للأداة. بعد ذلك ، ينبغي أن تفهم الأداة كيفية تقسيم التبولوجي المنطقي للشبكة حسب مناطق فواتير الدفع ، وهذه الخطوة يمكن أن تحتاج التدخل من مهندس الشبكة.

أحد الوسائل لتحقيق هذه المهمة هو **استخدام الفارة** في نظام إدارة الشبكة، ليتم الإشارة إلى منطقة دفع الفاتورة على الخريطة. لإجراء ذلك نضع الفارة على الخريطة، ونحدد حجم مستطيل يحيط أجهزة الشبكة، مثل الحاسبات المضيفة والوصلات. على سبيل المثال، تكون المجموعة المطلوب حساب قيمة فواتيرها تكون لها حاسبات مضيفة تقيم خلف جهاز شبكة منفرد. تقوم الأداة بإجراء عملية التصويت على جهاز منفرد بالشبكة وتجمع الإحصائيات اللازمة.

تحديد مكان عملية الانتخاب :

تكون الأداة قادرة على تحديد مكان عملية التصويت من أجل حساب معلومات الفواتير. نفترض شبكة مكونة من مجموعة من الحاسبات المضيفة في شبكة محلية، كما هو مبين

في شكل 7.7. كل حاسب مضيف يتم توصيله إلى الشبكة المحلية بواسطة سلك مزدوج إلى جهاز مركز بيانات. باستخدام خريطة الشبكة، يمكن أن نشير بالفارة إلى طابق واحد في مبنى المكاتب، حيث يتم توصيل كل الحاسبات المضيفة بواحد من جهازين مركزين للبيانات. بسبب أن كل الحاسبات المضيفة متصلة بأجهزة مركزات البيانات، تستطيع الأداة بسهولة أن تستنتج أن عملية تصويت مركزات البيانات هو التصرف الصحيح.



شكل7.7 توصيل جميع الحاسبات المضيفة

ولكن بفرض أن مهندس الشبكة طلب من الأداة إنشاء معلومات حساب فواتير الدفع لمنطقة يوجد بها ثلاثة حاسبات مضيفة، اثنان منهما متصلان بمركز بيانات واحد، والحاسب المضيف الثاني موجود بمركز البيانات الآخر. الآن تستطيع الأداة أن تستنتج أن الطريقة الصحيحة تكون بالاستفسار من كل حاسب مضيف منفرد عن المعلومات اللازمة.

لاحظ أن العديد من الشبكات تحتوي على **وصلات إضافية** Redundant، **وحلقات** Loops، وأجهزة **تعمل فقط عندما يتعطل أحد الأجهزة**. يمكن أن تؤدي هذه الإضافات إلى صعوبة للأداة بأن تقوم بعزل الأجهزة التي تستفسر منها. عندما تعاني الأداة من مثل هذه الصعوبات فإنه ينبغي على الأداة الاستعانة بمهندس الشبكة.

لتحديد مكان عملية الانتخاب للحصول على بيانات إدارة الحسابات، فإن الأداة تحتاج إنشاء شجرة بتوصيلة الشبكة. بإجراء البحث في شجرة توصيلة الشبكة بطريقة العرض أولا Breadth-First (من الأوراق والاتجاه لأعلى)، يمكن أن تجد الأداة المكان المثالي لإرسال الاستفسارات. إذا لم يوجد تقاطعات بين الأجهزة المختلفة المطلوبة للاستفسار، تستطيع الأداة استنتاج إجراء عملية الانتخاب لكل جهاز على حدة. تستطيع الأداة حساب توصيلة الشبكة، بواسطة استقبال الدخل من العديد من الأماكن مثل: معلومات تبولوجي نظام إدارة الشبكة، جداول الموجهات لأجهزة الشبكة، أو من شجرة الاجتياز Spanning Tree الموجودة في القناطر. ويتم إتاحة هذه المعلومات لمهندس الشبكة.

عندما يقوم مهندس الشبكة بالإشارة إلى منطقة في الشبكة، فإن **الأداة تسأل عن أنواع المعلومات التالية:**

1- طريقة حساب فواتير الدفع.
2- أسعار كل منطقة.
3- معدل إجراء عملية التصويت.

عند هذه النقطة تبدأ عملية حساب فواتير الدفع للمنطقة، بواسطة تجميع بيانات فواتير الدفع ووضعها في قاعدة البيانات العلاقية، كما هو مبين في شكل 7.8.

3.4 الأداة المتقدمة لإدارة الحسابات

تستطيع الأداة المتقدمة تحسين قدرات إدارة الحسابات بواسطة التنبؤ باحتياجات مصادر الشبكة. تساعد هذه التنبؤات مهندس الشبكة في إجراء المعايير والحصص المعقولة. كما يمكن للأداة المتقدمة مساعدة المستخدمين لمعرفة تكاليف فواتير الدفع الخاصة بهم.

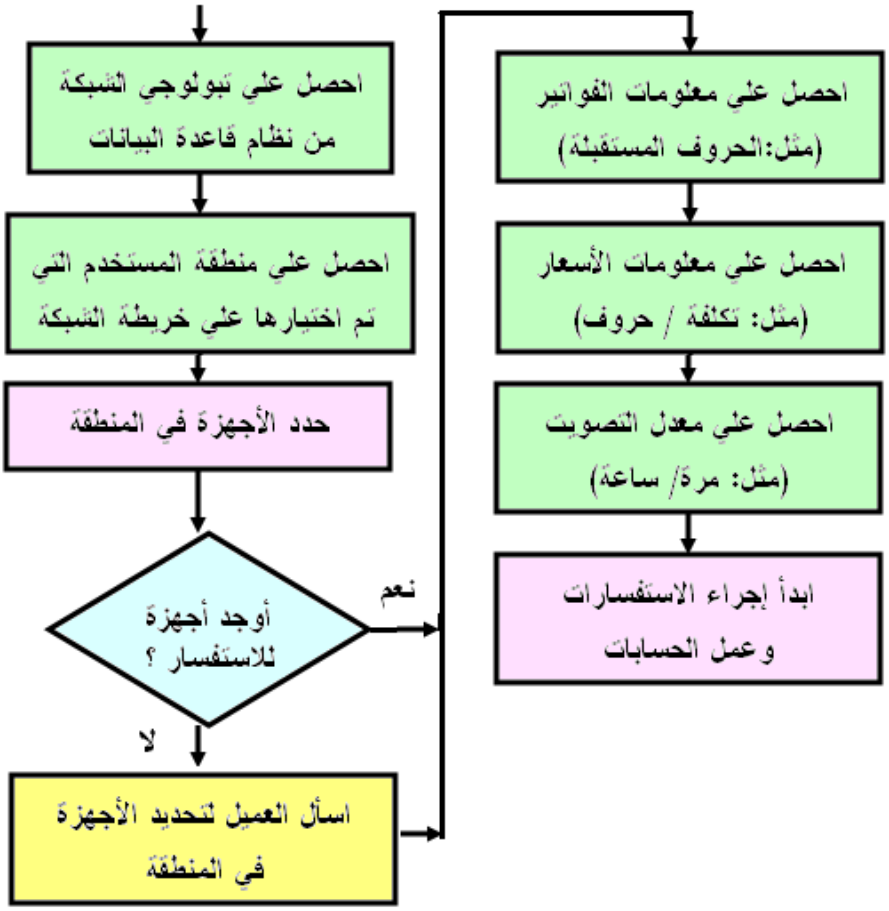
تساعد البيانات المعيارية والحصص مهندس الشبكة في تحديد مدى كفاية مصادر الشبكة. إن استخدام قاعدة البيانات العلاقية يسمح للأداة المتقدمة بإنشاء إحصائيات عدد المرات التي يقوم فيها المستخدمون غالبا بتخطي حصصهم في مدة زمنية محددة. بالإضافة ، ينبغي أن تكون الأداة المتقدمة قادرة على تحديد ما إذا كانت الشبكة تتجه نحو التسبب في الوصول إلى الحصة، وبذلك تنبه مهندس الشبكة بتحديث المصدر، أو إضافة أجهزة أكثر إلى المصدر ، وتعديل الحصة، أو تحديد أعمال أخرى تكون مطلوبة.

على سبيل المثال، يقوم المستخدمون في قطاع الشبكة المحلية بتخصيص مجموعة من أجهزة المودم للاتصال بالشبكة العامة لاسترجاع المعلومات. ربما يكون من المناسب لهؤلاء المستخدمين تحديد طول الفترة الزمنية التي يستخدمون فيها جهاز المودم. نفترض انه تم تحديد هذه الفترة اختيارية لتصل إلى خمسة ساعات في المكالمة الواحدة، بعدها يقوم المودم بفصل الاتصال.

ينبغي أن تكون الأداة المتقدمة قادرة على التنبؤ بقيمة فاتورة الدفع لمستخدم الشبكة. لإجراء ذلك، يمكن للأداة أن تقوم بعمل خطوتين هما:

1- فحص قاعدة البيانات العلائقية لتحديد أي اتجاه في فواتير الدفع، لمستخدم محدد عن فترات فواتير سابقة.

2- بعد ذلك تأخذ كل البيانات المتاحة عن دورة الفاتورة الحالية وترحلها إلى نهاية فترة الفاتورة.



شكل7.8 طريقة عمل الأداة المركبة لتحديد الفواتير.

على سبيل المثال، إذا طلب مدير مجموعة المستخدمين من مهندس الشبكة أن يقوم بحساب فاتورة الدفع القادمة، يمكن لمهندس الشبكة أن يقوم بإدخال بيانات المجموعة إلى الأداة التي تبحث عن معلومات الفواتير في قاعدة بيانات إدارة الشبكة للحصول على جميع السجلات السابقة لهذه المجموعة. بفرض أن هذه السجلات أظهرت زيادة 5% عن كل عشرة فترات فواتير دفع. تقوم الأداة بعد ذلك بفحص المعلومات في قاعدة البيانات عن فترة الدفع للفواتير الحالية. وترحيلها إلى نهاية المدة، وتجد الأداة أن 6%

زيادة محتملة منذ فترة دفع الفاتورة السابقة. عند الخرج، تقوم الأداة بإنشاء الفاتورة عن المدة المطلوبة التي تمثل 6% زيادة عن فاتورة المدة السابقة.

نفترض أن المعلومات التي تم استخراجها لا ترتبط عن قرب برسوم الفاتورة السابقة. يمكن أن يحدث هذا، عندما تكون مدة الفاتورة الحالية بدأت في التو، وأن عينة البيانات لا تمثل مدة الفاتورة بالكامل، أو أن المجموعة قد زادت أو نقصت من أنشطتها في استعمال الشبكة. في مثل هذه الحالات، تحتاج الأداة المتقدمة إخراج التنبؤات (الحسابات) على أساس البيانات التاريخية، وبعد ذلك تشتق منها مدة الفاتورة الحالية.

إن التقنيات التي تستخدمها الأداة المتقدمة متاحة في الأسواق، وتستطيع الأداة استخدام قاعدة البيانات، واستخراج المعلومات التي تساعد على حساب حصص وفواتير الدفع لمستخدمي الشبكة.

أسئلة تقويم ذاتي

اشرح كيف يتم إدارة الحسابات في الشبكة المحلية التخيلية

قارن بين استخدام الأداة البسيطة والأداة المركبة في إدارة الحساب لشبكة البيانات.

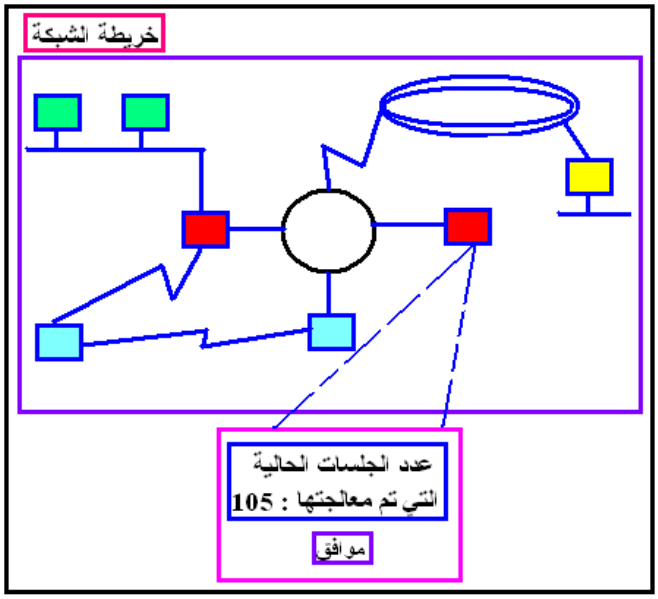
قارن بين استخدام الأداة المركبة والأداة المتقدمة في إدارة الحسابات لشبكة البيانات .

5. تدوين معلومات الحسابات

عزيزي الدارس، يمكن تدوين معلومات إدارة الحسابات على شكل رسائل وتقارير في الزمن الفعلي. يمكن لرسائل الزمن الفعلي أن تخبر مهندس الشبكة بقيمة معيارية معينة، كما توفر التقارير النصية الحساب التاريخي ومعلومات فواتير الدفع.

على سبيل المثال، نستطيع أن نطلب من نظام إدارة الشبكة إنشاء نافذة رسائل في الزمن الفعلي على شاشة عرض النظام لتوضيح معيار محدد لأحد أجهزة الشبكة، كما هو مبين

في شكل 7.9. تبين هذه الرسالة عدد الجلسات التي تعامل معها جهاز الشبكة. يكون هذا المعيار هاما بسبب أن الجهاز يقوم بترجمة البروتوكول ويستطيع إجراء الدعم المثالي لعدد معين من الجلسات فقط.



شكل7.9 تظهر شاشة نظام إدارة الشبكة رسالة إدارة الحسابات في الوقت الفعلي.

يستطيع النظام أيضا، توليد تقارير نصية عن إحصائيات إدارة الحسابات، وأن هذه التقارير مشابهة لخرج الأداة البسيطة، ويمكن أن تلخص المعايير أو الاتجاهات التنبؤية عن الاستخدامات المستقبلية لمصادر الشبكة. يستطيع مهندس الشبكة استخدام هذه المعلومات لتخطيط حصص حقيقية لمصادر الشبكة. تكون التقارير ذات أهمية في إعطاء المستخدمين فواتير الدفع الخاصة بهم نظير استعمال الشبكة. حيث تظهر هذه التقارير المعلومات التي استخدمت لحساب الفاتورة الحالية، والتنبؤ أيضا بتكلفة الفاتورة التالية مستقبلا. يوضح جدول 7.3 عينة لأحد هذه التقارير.

جدول7.3 مثال: عينة من فاتورة دفع رسوم استخدام الشبكة.

مدة الفاتورة	1 يناير : 1 فبراير 2007
إجمالي الحروف المستقبلة من الشبكة	150 ميجابيت
الأجهزة التي جري عليها عملية التصويت في الشبكة	رابط الشبكة والقنطرة
السعر / ميجا بايت	30 جنيها
إجمالي الفاتورة الحالية	4500 جنيه
إجمالي الفاتورة السابقة	4300 جنيه
نسبة التغير	10.5 % زيادة
حساب الفاتورة التالية المتوقع (Predicted)	4550 جنيها
نسبة التغير المتوقع (Predicted)	10.1 % زيادة

الخلاصة

في هذه الوحدة تعرفنا على إدارة الحسابات والتي تختص بقياس استعمالات مصادر الشبكة بواسطة المستخدمين من أجل تحقيق معايير Metrics، وفحص حصص Quotas، وتحديد الأسعار، وفواتير Bills المستخدمين. وتختص إدارة الحسابات بالعمليات الآتية:

تجميع البيانات عن معدل استخدام مصادر الشبكة.

- ضبط استخدامات الحصص Quotas، بواسطة معايير Metrics.
- تحديد قيمة فاتورة المستخدم Billing ، نظير استخداماته مصادر الشبكة.

تختص إدارة الحسابات بتجميع إحصائيات عن الشبكة، لتساعد مهندس الشبكة في اتخاذ القرارات المتعلقة بتخصيص مصادر الشبكة. تكون هذه الإحصائيات مفيدة في إدارة نظام المصادر، مثل: مساحات أقراص تخزين البيانات، قدرة المعالجة، عمليات التخزين الاحتياطية. في هذه الوحدة نفحص أولا، فوائد إدارة الحسابات، وبعد ذلك الخطوات المتعلقة بتحقيقها. عرضت الوحدة أيضا، شرح تفصيلي لتحديد فواتير دفع المستخدمين، ووصف الأدوات الثلاثة التي يمكن أن تستخدم في إدارة الحسابات، وهي الأداة البسيطة، والمركبة، والمتقدمة. وأخيرا، ناقشت طرق فحص وتدوين معلومات الحسابات.

مسرد المصطلحات

التكاليف المرجعية Recurring Cost

تمثل جزء كبير من ميزانية المؤسسة، يتم دفعها شهريا لتشغيل شبكة البيانات الإقليمية. فإن استخدام التقنيات ذات الجدوى الاقتصادية Cost-effective يكون دائما أحد العوامل الهامة

المحلية التخيلية Virtual LANs.

إن تقنيات الشبكة المحلية التخيلية تقوم بالتوصيل المنطقي لأجهزة الشبكة المحلية عند المواقع الفعلية المختلفة، لتكوين شبكة محلية منطقية واحدة

مجالات الفواتير Billing Domains،

ثم تحسب بعد ذلك قيمة فواتير الدفع لكل مستخدم. تحتاج الأداة المركبة البيانات من إدارة النظام ومن مهندس الشبكة لأداء عملها. ينبغي أن تكون الأداة قادرة على الحصول على التبولوجي من قاعدة البيانات العلائقية من نظام إدارة الشبكة

علامة حسابات An Accounting Tag

لتحديد عنوان المصدر الذي يرسل الحزم، ومن الممكن إضافة معلومات عن بيانات التطبيقات في المستوى الأعلى خلال الحزمة. يمكن أن يكون متاحا في الأسواق مكدسات بروتوكولية Protocol Stacks خاصة تقوم بتنفيذ البروتوكول

المصطلح بالإنجليزية	معناه بالعربية
Account Management	إدارة الحسابات
ATM	نظام نمط الاتصال غير المتزامن
Access Fee	أجرة الاتصال
Activity Log	سجل النشاط
Activity Reports	تقارير النشاط
Action	فعل (حدث)
Acknowledgement Packets	حزم شكر
Accounting Tag	علامة حسابات
Ad-hoc	هلامية
Anonymous	دخول موقع على الشبكة كزائر
Billing	عملية تحديد النفقات
Bills	فواتير المستخدم
Billing Domains	مناطق الفواتير
Breadth-First	طريقة البحث "العرض أولا"
Budget	الميزانية
Chargeback	استرجاع النفقات
Cost-Effective	الجدوى الاقتصادية
Dominant Factors	العوامل المهيمنة
Dumps	نفايات مهملة
Fair Sharing	مشاركة عادلة
FTP	بروتوكول نقل الملفات
FDDI	وحدة مواجهة بصرية لتوزيع البيانات

المصطلح بالإنجليزية	معناه بالعربية
Frame Relay	ترحيل الأطر
Folders	المجلدات
Infrastructure	البنية التحتية
Inputs	مداخل
IPng (or IPv6)	بروتوكول الجيل الثاني للانترنيت
Junk e-Mail	نفايات بريدية
Loops	حلقات
Logs	ملفات التسجيل
Metrics	معايير
Off line	عدم اتصال
Online	وقت الاتصال
Outputs	مخارج
Personal Planning	التخطيط الشخصي
Print Spooler	جدولة الطباعة
Protocol Stack	مكدس بروتوكولي
Polling	عملية التصويت
Queries	استفسارات
Quotas	حصص
Time-Sharing	مشاركة الوقت
Triggers	مقادح
Recurring Cost	التكاليف المرجعية
RFC(Request For	برجاء التعليق

المصطلح بالإنجليزية	معناه بالعربية
Comments)	
Redundant	إضافية
Spanning Tree	شجرة الاجتياز
SQL	لغة الاستفسار الهيكلية
Supercomputer	الحاسب العملاق
Unsolicited Data	البيانات التي لم تطلب
Virtual LANs	الشبكات المحلية التصورية

المراجع

[1] Stephen B. Morris, Network Management, MIBs and MPLS : Principles, Design and Implementation, Prentice Hall, 2006.

[2] Aidarous Salah, Plevyak Thomas, Telecommunication Network Management: Technologies and Implementations, Wile, 2004.

[3] Raman Lakshmi G, Fundamental of Telecommunication Network Management, Prentice Hall, 2007.

4] Subramanian, Network Management, Wiley, 1999.

[5] Allan Leinwand , Karen Fang , Network Management, Addison Wesley 1992.

[6] Gary Cokins, Activity-based Cost Management: An Executive's Guide Wiley, 2001.

[7] Rigney, C., "RADIUS Accounting", RFC 2139(and 2866), April 1997.

[8] McCloghrie, K., Heinanen, J., Greene, W. and A. Prasad, "Accounting Information for ATM Networks", RFC 2512prop, February 1999.

[9] McCloghrie, K., Heinanen, J., Greene, W., and A. Prasad, "Managed Objects for Controlling the Collection and Storage of Accounting Information for Connection-Oriented Networks", RFC 2513prop, February 1999.

[10] Cooper, R., Kaplan, R. S., The Design of Cost Management Systems. Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[11] Brownlee, N. and A. Blount, "Accounting Attributes and Record Formats", RFC 2924, September 2000.