
الوحدة الاولى
مقدمة في علم الشبكات

محتويات الوحدة

الموضوع	رقم الصفحة
مقدمة	**3**
تمهيد	**3**
أهداف الوحدة	**4**
1. تعريف شبكة البيانات	**5**
2. دور مهندس الشبكات	**6**
3. مهام مدير الشبكة	**8**
4. أهداف إدارة الشبكات	**8**
1.4 إدارة الأعطال Fault Management	9
2.4 إدارة التهيئة Management Configuration	**11**
3.4 إدارة الأمن Management Security	**12**
4.4 إدارة الأداء Management Performance	**14**
5.4 إدارة الحسابات ManagementAccount	**15**
5. بروتوكولات إدارة الشبكة	**17**
الخلاصة	**20**
لمحة مسبقة عن الوحدة التالية	**20**
إجابات التدريبات	21
مسرد المصطلحات	**22**
المراجع	**25**

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

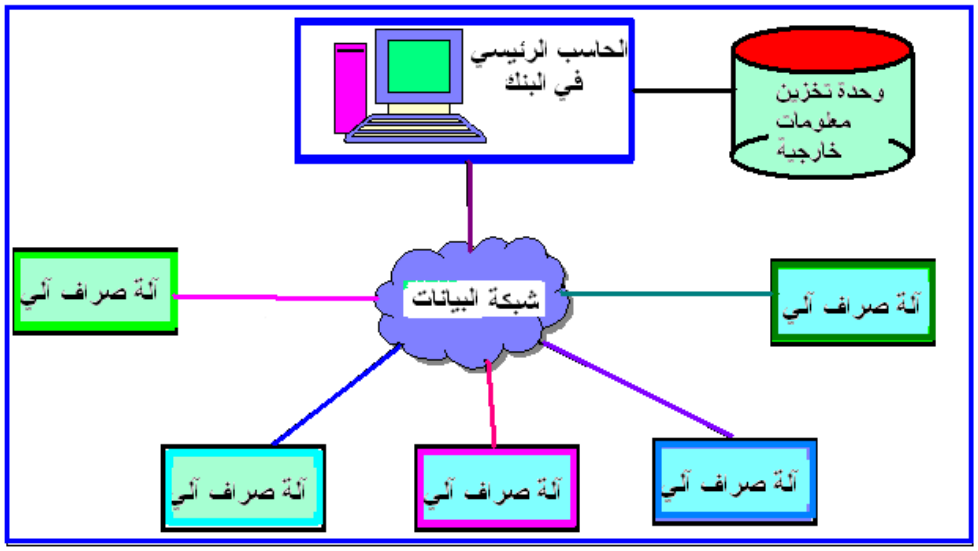


عزيزي الدارس، بعد فراغك من دراسة هذه الوحدة ينبغي أن تكون قادرا على أن :

- 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 تقـوم الشـبكة بـأداء وظائفها بشـكل صـحيح فإنه يتم عــادة تكليف مجموعة من مهندسي الشــبكات بمسـئولية تشــغيل وصــيانة الشــبكة. وكلما زادت عمليــات التوسع في الشــبكة، زادت مشـاكلها وبالتـالي زادت الأعبـاء الوظيفية على مهندسي الشـبكة. إذ **يجب عليهم الإلمــام بكميــات ضــخمة من المعلومــات حــول الشبكة**. ولهـذا السـبب يـأتي دور علم إدارة الشـبكات فهو **علم نشأ لمساعدة مهندسي الشبكات** على أداء وظائفهم المهنية.

إن الهدف من بناء شـبكة البيانـات هو **تحقيق احتياجات المؤسسة من توفير عمليات الاتصال**. ولتحقيق ذلك فإنه يجب على مهنـدس الشبكة إجراء العمليات الضـرورية لتخطيط الشـبكة. إذ يقـوم مهنـدس الشبكة بإجراء عملية مسح Survey شاملة لأماكن تجمع المسـتخدمين. 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.

يقو[redacted]يلات المطلوبة[redacted]. ويوجد **نوعان من تقنيات طرق توصيل الشبكات هما:**

أن يتم إنشاء شـبكة محلية(Local Area Network)ـ LAN، أو أن يتم إنشاء شبكة واسعة WAN (Wide Area Network). إن الشبكة المحلية تقوم بتوصيل الحاسبات معا بسـرعة مـداها يـتراوح من 4 ميجا بـايت / الثانية إلى 155 ميجا بـــــايت / الثانية (4MB_____155MB). وهي توصل المستخدمين لمسافات قصيرة نسبيا. أما الشبكة الواسـعة فهي تعمل عند سرعات نقل بيانات تتراوح من 9.6 كيلـوبت / ثانية إلى أكـثر من 45 ميجا بت / الثانية. وهي توصل المستخدمين لمسافات أطـول. إن الشبكة الواسعة عـادة توصل مجموعـات من الشـبكات المحلية مع بعضها من عدة أماكن متفرقة.

بعد بنـاء الشـبكة فـإن مهنـدس الشـبكة سـوف يحتـاج متابعة عملية صـيانتها. فمثلا قد تتغـير بـرامج تشـغيل الشـبكة أو أجهـزة الحاسـبات المتصلة بهـا، أو قد يتم توسـعة الشـبكة أو قد يحـدث أعطـال أو إجـراء عملية إحلال لأجزاء تالفة من الشـبكة. إن تغـير احتياجـات مسـتخدمي الشبكة عادة سوف يؤثر في خطة إنشاء الشـبكة، وهـذا بـدوره 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 الاعتبـار وأن يسـتخدم الحلول السليمة لمعالجة إجراءات توسعة الشـبكة. كما يجب أن تتـوفر لمهندس الشبكة القدرة المعرفية والاطلاع على المنتجـات الجديـدة، و إمكانية إحلال منتج جديد محل الأجـــزاء المتهالكة من الشـــبكة. وذلك بهدف تحقيق العمليـات الاقتصـادية في المـوارد المتاحة وتحقيق خدمة أفضل لمسـتخدمي الشـبكة بكلفة مناسـبة. كما يجب على مهنـدس الشـبكة اسـتخدام الأدوات المناسـبة اللازمـة لفحص أعطـال الشـبكة وصيانتها.

3. مهام مدير إدارة الشبكة

تسـتخدم التعبـيرات: مـدير إدارة الشـبكة Network Administrator، اختصاصي الشبكات Network Specialist، ومحلل الشـبكات 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 أعمـالا تكـافئ المهـام الـتي يؤديها مديرو النظم System Administrators .

وتشمل صيانة العتاد والبرمجيات الخاصة بالشـبكة. ويشـمل أيضا رصد وتهيئة مكونـــات وعناصر الشـــبكة. كما أنهم مسـؤلون عن تخصـيص العنـاوين لأجهـزة الشـبكة وتحديد جـــداول تهيئة الموجهـــات وعمليـــات تفـــويض الشـــبكة Authorization. أما إخصائيوا ومحللو الشبكات، يتركز عملهم في تقـييم أمن الشبكة وفحص الأعطال وتشخيص مشاكل الشبكة، وكذلك صـيانة العمليـات المتعلقة بـالتفويض، وعمل النسخ الاحتيـاطي Backup لنظم الشبكة.

4. أهداف إدارة الشبكات

عزيزي الـدارس، تقـوم المؤسسـات والهيئـات عـادة باسـتثمار أمـوال كثـيرة وبـذل الـوقت والجهد في بنـاء شـبكات البيانـات. بالإضـافة إلى تعيين مهندس أو أكثر لصيانة هذه الشبكات. وقد يكون من الأفضل من ناحية التكلفة أن يقوم النظـام الشـبكي نفسه بـالنظر آليا بفحص بعض العمليـات الـتي تـؤدى داخلـه. وهـذه الترتيبـات يمكن أن تخفف العبء الواقع على مهندسي صيانة الشبكات. من هـذه الفكـرة نشأ علم إدارة الشبكات. إن علم إدارة الشبكات هو العلم الخاص بعمليات التحكم في شبكات البيانات المعقدة بهدف زيادة كفاءتها وإنتاجيتها.
وقد قـــــامت المؤسسة الدولية للقياســـــات Organization for Standardization) ISO (International .

بتقسيم وظائف إدارة الشبكات إلى خمسة وظائف أساسـية هي:

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

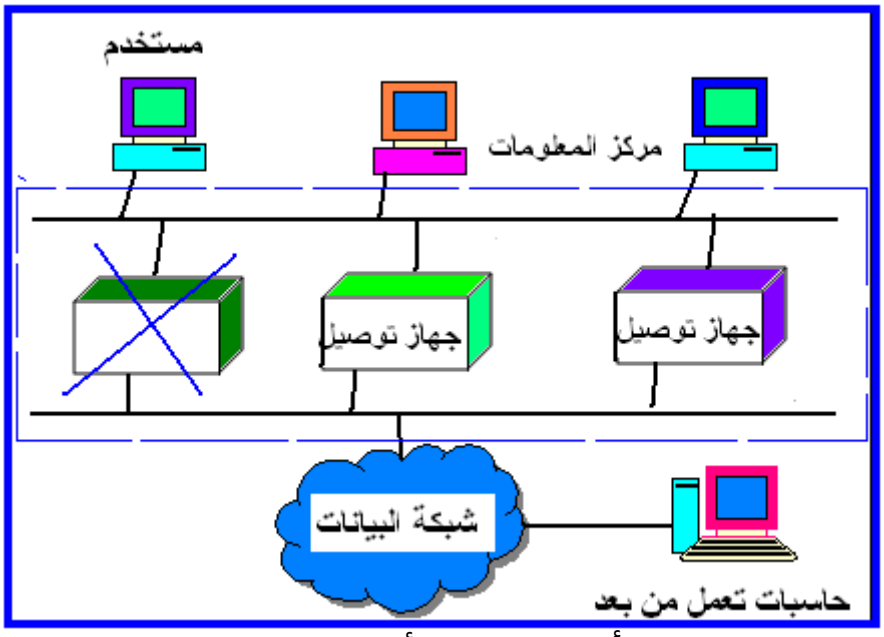
1.4 إدارة الأعطال

عزيــزي الــدارس، تكــون وظيفة إدارة الأعطــال **هي تحديد مكــان المشــكلة المســببة للعطل في شــبكة البيانــات** وذلك باتبــاع الخطوات التالية:

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

ويستطيع مهندس الشبكة أن يستخدم أدوات إدارة الأعطـال في تحديد مكـان وحل مشـكلة الأعطـال بسـرعة أكـبر مما كـان متوقعا بـدون استعمال هذه الأدوات.
مثال على ذلك، نفترض أنه عندما يبدأ المستخدم عملية التشـغيل، فإنه يطلب الدخول إلى الشبكة من عدة أجهزة متصلة بالشبكة، وقد يحـدث أن تتوقف الشبكة فجأة. عندما تحـدث هـذه الحالـة، يقـوم المسـتخدم بإبلاغ هذه المشكلة لمهندس الشبكة، كي يقوم مهندس الشـبكة بعـزل هذه المشكلة وحلها.

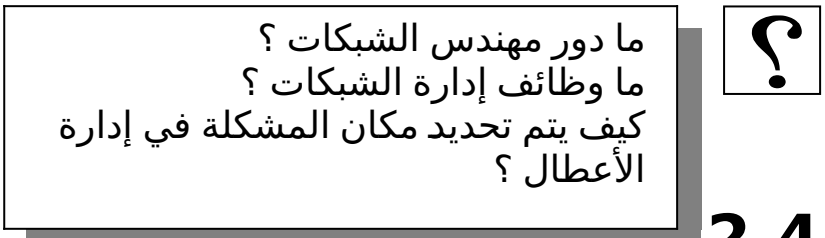
بدون استعمال أدوات إدارة الأعطـال، فـإن **مهنـدس الشـبكة يقوم بتحديد سـبب المشـكلة. هل هو بسـبب أن المسـتخدم قام بكتابة أوامر التشغيل خطأ، أم أنه قام بمحاولة الـدخول إلى مكـان غـير مسـموح به في الشـبكة**. إذا لم يجد مهنـدس الشـبكة أن الخطأ نـاتج بسـبب سـوء اسـتعمال من المسـتخدم. فـإن مهندس الشبكة يقوم بفحص الأجهزة الموجودة بين وصـلة المسـتخدم والشـبكة. بغـرض أنه وجد أن السـبب هو وصـلة اتصـال المسـتخدم بالشبكة كما هو موضح في شكل1.2.



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

وبـالرجوع إلى مسـار وصـلة المسـتخدم بالشـبكة، وجد أن وصـلة المسـتخدم مفصـولة. وعنـدما يقـوم مهنـدس الشـبكة بتوصـيلها فـإن المستخدم يستطيع الدخول إلى الشبكة والعمل بشكل صـحيح. وبـذلك يتم تصليح العطل.
ولكن باستعمال أدوات إدارة الأعطال فإنه كان من الممكن تصليح هـذا العطل بسرعة أكثر، حتى دون أن يتم الإبلاغ عن مثل هذا العطل.

أسئلة تقويم ذاتي



2.4 إدارة التهيئة

عزيزي الدارس، إن تهيئة أجهـزة شـبكة بيانـات معينة **يعـني التحكم في سـلوكيات أجهـزة هـذه الشـبكة**. حيث إن إدارة التهيئة هي عملية إيجاد وضبط (تهيئة) Setting up لهـذه الأجهـزة الحرجة Devices Critical. على سـبيل المثـال، بفـرض أن أحد الإصـدارات البرمجية من نوع الإصدار A، موجود في جسر شبكة إثرنيت يسبب مشاكل في أداء الشبكة. ولتصليح هذه المشـكلة الشـاذة Anomaly، فـإن منتجي هـذا الصنف من الجسر قد أصدروا برمجيات تحـديث، هو الإصـدار B، وهـذا يتطلب تنصـيب Installing برمجيـات دائمة Firmware جديـدة في كل خمسون جسر متصل متصلة بالشبكة.

وطبقا لهـذا، فإنه تم التخطيط لعمل ذلك في الشـبكة. ولكن أولا، فـإن مهندس الشبكة يحتـاج تحديد نـوع الإصـدار الـبرمجي الموجـود في كل جسر. ولكن لا يوجد أدوات إدارة تهيئة فاعلة. ولهـذا فإنه يجب عليه أن يعمل ذلك فعليا بنفسه لكل قنطرة.

إن أدوات إدارة التهيئة تقـوم بتزويد مهنـدس الشـبكة بقائمة بأسـماء الجسور المتصلة بالشـبكة موضـحا بها نـوع الإصـدار الـبرمجي الحـالي المستخدم في كل جسـر، وهـذا يسـهل معرفة مكـان القنطـرة المـراد تغيير الإصدار البرمجي الجديد لها. و يوضح جـدول1.1 بعض معلومـات إدارة التهيئة التي تساعد لهذه الحالة.

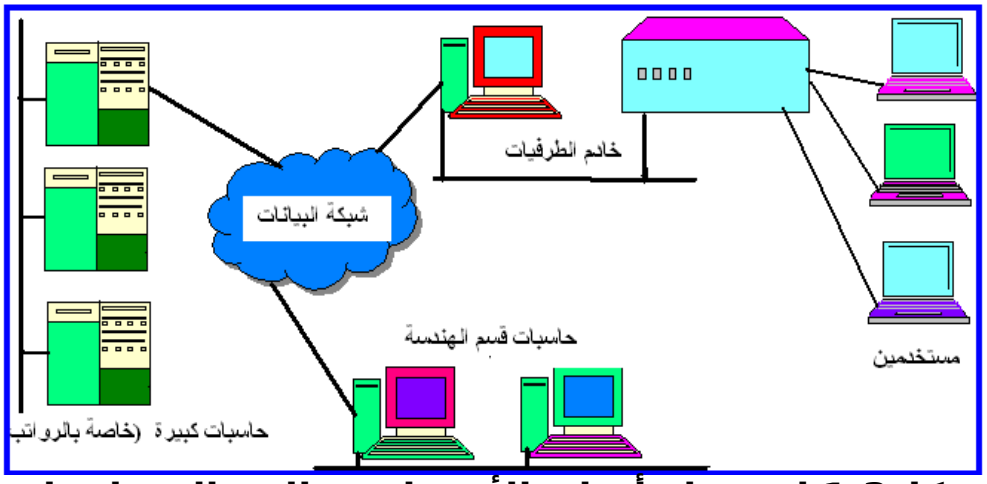
جدول1.1 يبين بعض معلومات إدارة التهيئة (اسم القنطرة ونوع إصدار البرنامج).

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

عزيـزي الـدارس، إن إدارة الأمن هي عملية **التحكم في الوصـول إلى المعلومـات المخزنة في شـبكة البيانـات**. إن بعض المعلومات المخزنة في أجهزة الحاسبات المتصلة بالشبكة ربما يكـون من غير المناسب أن يطلع عليها كل المسـتخدمين. فربما تشـمل هـذه المعلومات الحساسة على سبيل المثـال تفاصـيل عن منتجـات جديـدة للشركات، أو قد تحتوى على قواعد بيانات تخص العملاء بالشركة.

على فرض أن مؤسسة ما قد قررت اسـتخدام وسـائل إدارة الأمن كي تسمح للأجهـزة الطرفية البعيـدة بالاتصـال بالشـبكة من خلال خطـوط 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 الـدخول إلى جهـاز الحاسب لأداء عملهم من خلال الاتصـال بخـادم الطرفيـات. بعد أسـابيع قليلـة، قـام مـدير المؤسسة بالإبلاغ عن أنه قد تم محاولات عديدة خاطئة بالاتصال بخادم الطرفيات المسـتخدمة من قبل المهندسـين. وأن خـادم الطرفيـات لم يسـمح بتوصيل أي حاسب بالشبكة، تاركا حاسب الهدف المضيف يمنع توصـيل المعلومـات الحساسـة. وبـذلك لا أحد من المهندسـين يتمكن من التوصيل إلى حاسب الرواتب Payroll.
كمحاولة أولى، يمكن اسـتخدام أدوات إدارة التهيئة لتحديد وسـيلة التوصـيل بخـادم الطرفيـات. ولكن للكشف عن من هو الـذي يقـوم بمحاولة الوصول إلى حاسب بيان الرواتب Payroll، سـوف ينبغي على مهنـدس صـيانة الشـبكة أن يـدخل إلى خـادم الطرفيـات بشـكل دوري وتسجيل أي من المهندسين يقوم باستخدامه. يقوم مهنـدس الشـبكة بعمل ترابط Correlation الأوقـات الـتي يتم فيها محـاولات دخـول غـير 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 الطرفيـات بصـفة دوريـة. كما أن إدارة الأمن تـزود مهنـدس الشـبكة بتحذيرات صـوتية Sound Alarms للتنبيه باحتمـالات قوية قد حـدثت أو سوف تحدث في الشبكة لخرق أمن الشبكة.

4.4 إدارة الأداء

تتضـمن إدارة الأداء إجـراءات لقيـاس أداء عتـاد الشـبكة والبرمجيـات والوسـط. من أمثلة هـذه القياسـات : قيـاس سـرعة أداء الشـبكة Throughput – قيـاس معـدل الأخطـاء Error Rates – قيـاس نسـبة الاسـتخدام Percentage Utilization - قيـاس زمن الاسـتجابة Response Time. وباستخدام معلومـات إدارة الأداء، يسـتطيع مهنـدس الشبكة التأكد من أن الشبكة تتوفر لها السعة اللازمة لاحتواء احتياجات المستخدمين.

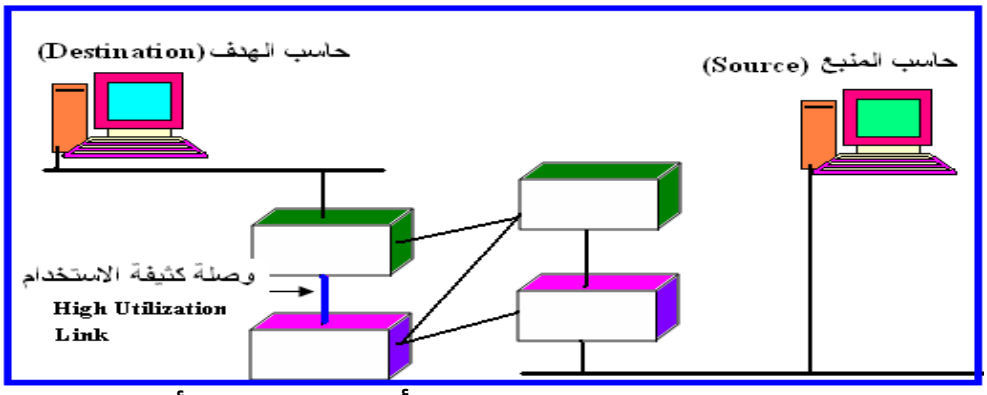
مثال:

بفرض أن أحد المستخدمين **يشتكي من أن أداء نقل الملفات** عبر الشبكة **يتم ببطء**.

بدون وسـيلة إدارة الأداء، فـإن مهنـدس الشـبكة يجب عليه أولا النظر في أعطـال الشـبكة. إذا لم يجد أعطـال بالشـبكة، فإنه سـوف يقوم بتقييم أداء كل الأجهزة والوصلات الموجودة بين أجهزة الطرفيات الـتي يسـتخدمها العميل والشـبكة. **وأثنـاء 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

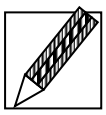
عزيزي الدارس، تختص إدارة الحسابات بمتابعة كل مستخدم أو مجموعة من المستخدمين باستعمال مصادر الشبكة للتأكيد من أن المستخدمين يتوفر لهم مصادر شبكية كافية. كما تكون أيضا مسئولة عن منع أو منح الصلاحية بالتوصيل بالشبكة.

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

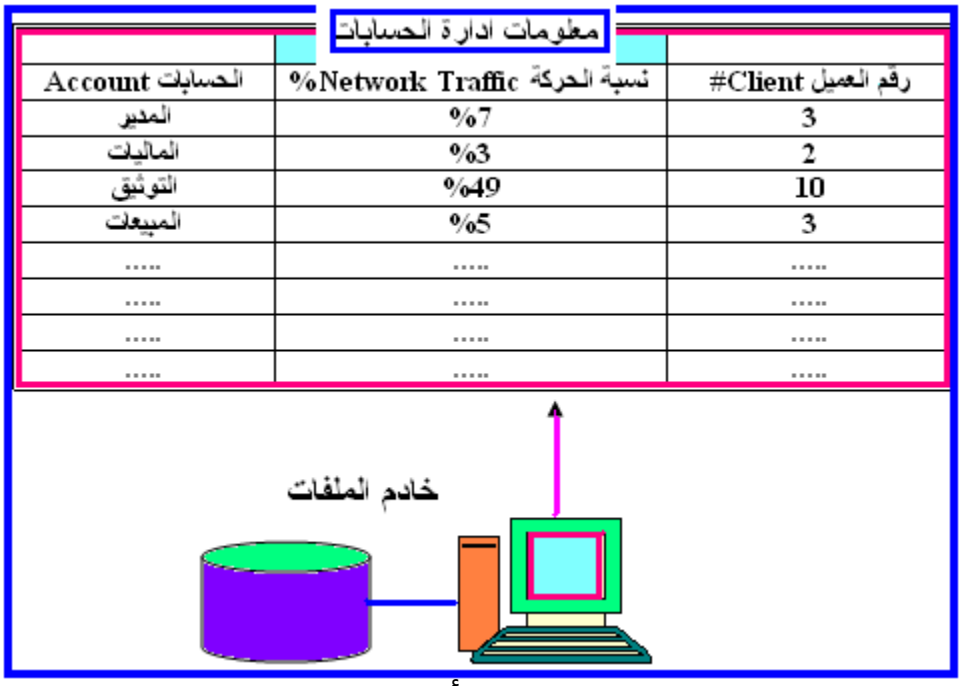
قسم التوثيـق، يكـون له عملاء عديـدون هم الـذين يسـتعملون أجهـزة حاسبات متصلة بخادم الملفات. وبـذلك يجد مهنـدس الشـبكة أن هـذه الحركة Traffic هي الـتي تمثل تقريبا نصف الحمل الواقع على الوحـدة البينية لشبكة خادم الملفات.
يمكن لمهنـدس الشـبكة أن يقـرر إعطـاء فريق التوثيق خـادم ملفـات خـاص بهم، يسـتطيع مواجهة حركة الشـبكة Network Traffic ويـترك باقي الشبكة بدون تغيـير. بالإضـافة إلى أن مهنـدس الشـبكة يمكن أن يقرر تحديد مكـان خـادم ملفـات جديد في نفس قطـاع الشـبكة لخدمة فريق التوثيق، والذي يمكن أن يقلل حركة الشبكة في قسم التوثيق.
باستخدام أدوات إدارة الحسـابات، يسـتطيع مهنـدس الشـبكة بسـرعة معرفة أن قسم فريق التوثيق يقوم بالاتصال بخادم الملفـات بمجموعة كبـيرة من العملاء بشـكل منتظم. وبـذلك يسـتطيع معالجة هـذا الوضع بأسـرع وقت ممكن. يوضح شـكل1.5 بعض المعلومـات الـتي 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 الإلكترونيات 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 أيضاً تعـــني الوصـــول الي المعلومـــات 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.

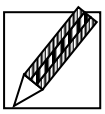
5. بروتوكولات إدارة الشبكة

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:

- بروتوكــول إدارة الشــبكة البســيط SNMP (Simple Network Management Protocol) **ويوجد منه ثلاثة إصدارات :**
أحدثهم هو الإصدار الثالث SNMPv3.
- وبروتوكـــول إدارة المعلومـــات الشـــائع CMIP (Common Management information Protocol) أو بروتوكــول خــدمات إدارة المعلومــات الشــائع CMIS (Common Management Information Services). ويفضل اســتخدام بروتوكــول SNMP عن الــبروتوكول 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 الـدارس، تعرفنا في هـذه الوحـدة على وظـائف شـبكة البيانـات، وعـددنا المهـام الوظيفية لمهنـدس الشـبكة، ثم تعرفنا على وظائف علم شبكات البيانات واوضحنا بالامثلة وظائف الشبكة، وبعـدها تناولنا بالشـــرح المؤسسة الدولية للقياســـات ISO (International Organization for Standardization) وتقسيم **وظائف إدارة الشبكات إلى خمسة وظائف أساسية هي:**

- إدارة الأعطال Fault Management
- إدارة التهيئة Management Configuration
- إدارة الأمن Management Security
- إدارة الأداء Management Performance
- إدارة الحسابات ManagementAccount

ثم تعرفنا على أدوات إدارة الشبكة ومنها بينا وظائف إدارة الأعطـال وإدارة التهيئة والحسابات ودرجنا بعـدها 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.	10.	11.
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 مكـان المشـكلة المسـببة للعطل في شـبكة البيانـات وذلك باتبـاع الخطـوات التاليـة:اكتشـاف المشـكلة، عـزل المشـكلة وعلاج المشكلة.

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

المصطلح بالإنجليزية	معناه بالعربية
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
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

المصطلح بالإنجليزية	معناه بالعربية
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 onroy. Addison Wesley 1996,

ok, By Marshall T. Rose, Daniel Vesley Professional 1992,ISBN-10:



محتويات الوحدة

الموضوع	رقم الصفحة
مقدمة	**29**
تمهيد	**29**
أهداف الوحدة	30
1.مكونات نظام إدارة الشبكة	**31**
2.منصة إدارة الشبكات	**34**
1.2 تبيين محتويات الحزم البرامجية	35
2.2 الخصائص التي يجب توفرها في برامج إدارة الشبكة	37
3. معماريات إدارة الشبكة	**41**
1.3 العمارة المركزية	41
2.3 العمارة الهرمية	44
3.3 العمارة الموزعة	46
4 . تطبيقات إدارة الشبكات	**48**
5. طريقة اختيار نظام إدارة الشبكة	**51**
6. إدارة الوسط الموزع DME	**53**
7. إدارة شبكات الاتصال TMN	**59**
الخلاصة	**64**
لمحة مسبقة عن الوحدة التالية	**64**
إجابات التدريبات	65
مسرد المصطلحات	**66**
المراجع	**69**

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

الشـمولي من دراسة هـذه الوحـدة هو أن يتمكن الـدارس من اختيـار نظـــام إدارة الشـــبكة وتطبيقاتها المناســـبة والـــتي 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 تكون قادرا على أن :

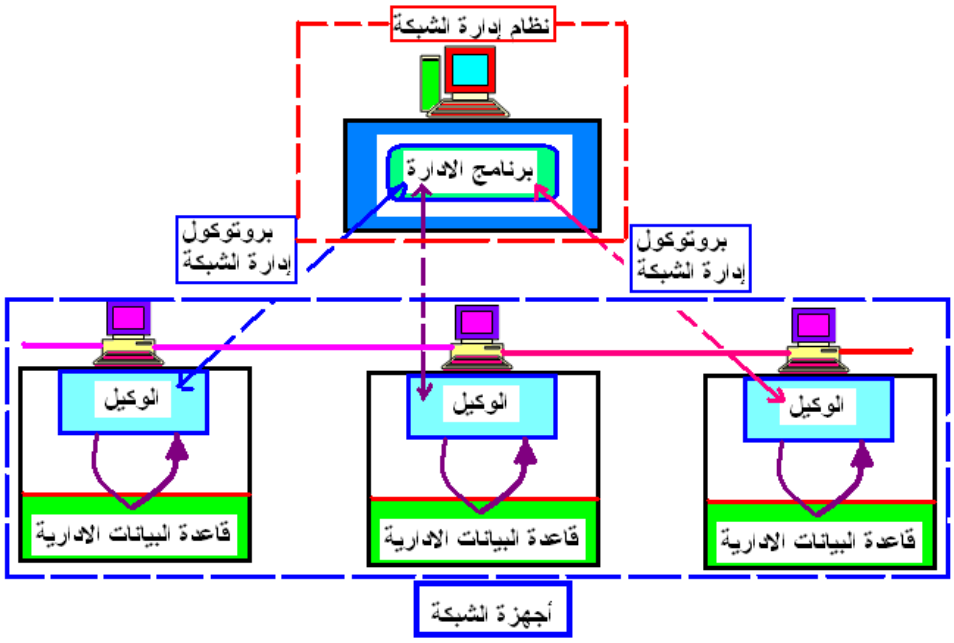
- تعرف وظائف نظام إدارة الشبكات.
- تصف مكونات نظام إدارة الشبكة.
- تعدد طرق التفاعل بين إدارة الشبكة وأجهزة الشبكة.
- تبين المهام الوظيفية لبرنامج إدارة الشبكات.
- تحدد المكونات الأساسية لبرنامج إدارة الشبكات.
- تشرح بعض الأمثلة لتوضيح وظائف برنامج إدارة الشبكة.
- تفرق بين انواع معمارية الشبكات الثلاثة .
- 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 بنـاء هيكلي كما هو موضح في شـكل 2.1. وتشمل ما يلي:

- محطة إدارة الشـبكة: وهي عبـارة عن حاسب مركـزي يوجد به برامج الإدارة والتحكم.
- الأجهزة الـتي يتم إدارتهـا، وهي تشـمل العناصر المكونة لشـبكة البيانـــات، مثل الموجهـــات Routers، والبوابة الســـريعة 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.

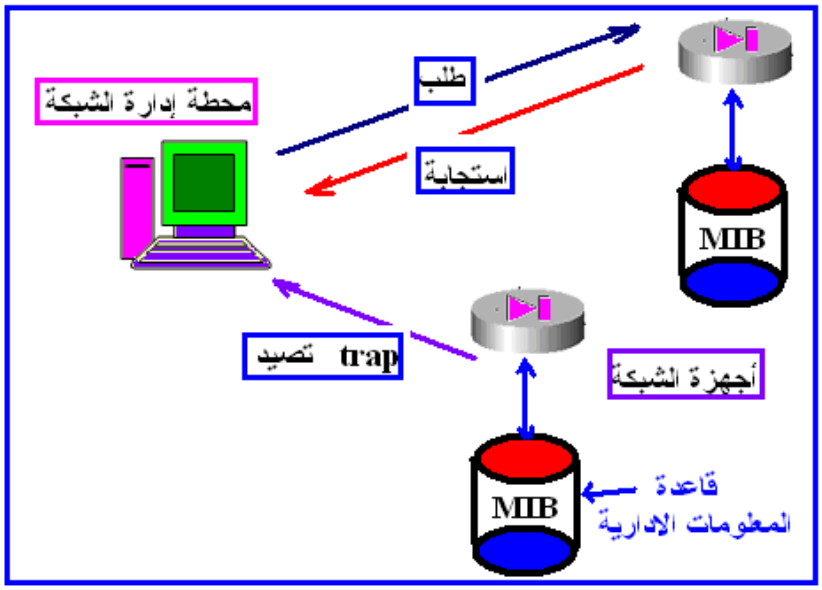
ويوجد في كل جهاز شبكة يتم إدارته برنامج يسمى الوكيل Agent، وقاعدة بيانات. حيث يقوم برنامج الوكيل بمعالجة وتخزين معلومات عن جهاز الشبكة المطلوب إدارته. ويقوم بتزويد هذه المعلومات إلى نظام إدارة الشبكة عن طريق بروتوكول إدارة الشبكة. كما يقوم برنامج الوكيل أيضا، بتحديد المعاملات التي يستخدمها نظام إدارة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

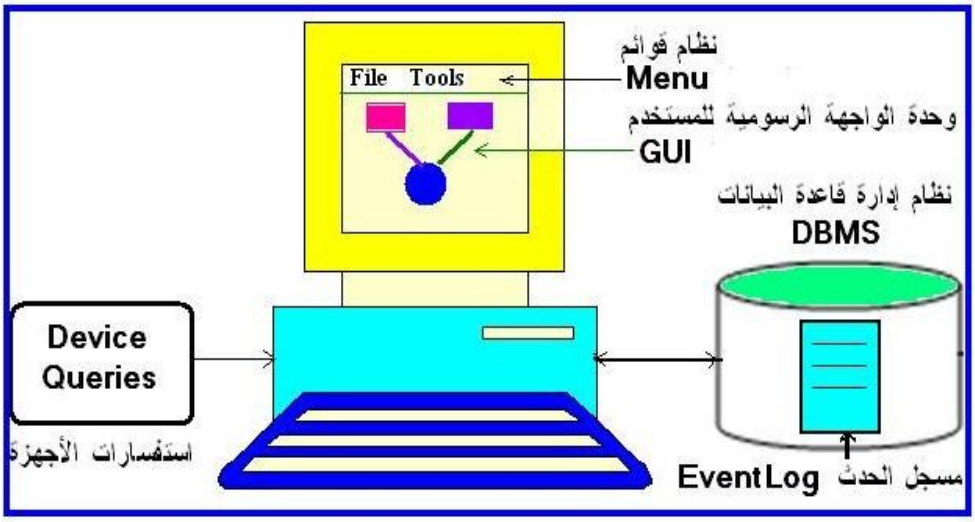
ثانيا :طريقة الولوج Logging: تقوم أجهزة الشبكة بتوليد إشارات تحذير عندما تصل معاملات الأجهزة إلى الحد الحرج، وهذه الإشارات تسمى مصايد Traps. بعد ذلك، تقوم محطة نظام إدارة الشبكة بتسجيل رسالة تنبيه إلى مهندس الشبكة. وهذه الطريقة تستهلك سعة نطاق قليلة. وفور استقبال هذه التحذيرات فإن محطة وحدة التحكم في 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 تبـــيين محتويـــات الحـــزم البرامجية

1.1.2 وحــدة الواجهة الرســومية للمستخدم

إن وحدة الواجهة الرسومية للمستخدم تكون مفيدة لعدة أغراض. فهي تجعل المستخدم يتصل بسهولة بخصائص برنامج إدارة الشـبكة. ويجب أن تكــون وحــدة الواجهة الرســومية للمســتخدم قياســية Standard، متوافقة مع نظم التشغيل المتعددة مثل ميكروسوفت وينـدوز أو نظـام أى بى إم أو نظام يونيكس. وأن تكون موثقة ومعتمــدة من قبل منتجي برمجيـــات الشـــبكات. إن نظم إدارة الشـــبكات يمكن أن تســـتخدم لتطبيقات متعددة باختلاف نوع المنتج والشـركة المصـنعة لـه. وعنـدما 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

أحــداث للشــبكة. وبغض النظر عن كيفية تعلم البرنــامج عن أحــداث الشبكة، فإنه يجب على البرنامج توفير سـجل للحـدث وذلك لمسـاعدة مهندس الشبكة في معرفة التطورات الجديدة التي تحدث في شــروط الشبكةNetwork Conditions .

2.2 الخصائص الـتي يجب توفرها في برامج إدارة الشبكة

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

1.2.2 أدوات جرافيك Graphic Tools

إن برنـامج إدارة الشـبكة يجب أن يـوفر لمهنـدس الشـبكة الوسـائل المعينة له كي يستطيع إنشاء رسومات بيانية للبيانات بأشكال متعـددة منها الرسم الخطي Line Drawing – رسم قضـيبي Bar Drawing – رسم الكعكي Pie Chart Drawing. وكـذلك إمكانية لـدمج الرسـومات البيانية مع التقارير. وهذا يكون ذا فائدة كبيرة حيث إن المـديرين عـادة تفضـلون رؤية المعلومـات على شـكل رسـومات بيانية بـدلا من تقـديم هذه المعلومات على شـكل تقـارير نصـية Text. إن الرسـومات البيانية التي توضح حركة الشبكة Network Traffic الحالية ومعدلات الأخطـاء، تساعد كثـيرا في إدارة الأعطـال وإدارة الأداء. وأن الرسـومات 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 وحــدة API هي عبــارة عن مكتبة برمجية تســمح بالوصــول إلى المعلومات التي يتم الاحتفاظ بها داخل برنامج إدارة الشـبكة. تسـتطيع البرامج الخارجية من خلال API استخدام خريطة الشـبكة، والاتحـاد مع قائمة Menu النظام، وتخزين واسترجاع المعلومات من قاعدة البيانـات 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 والـتي تناسب الوسط المحيط.
ويفضل أن تكون وحدة API ذات معايير قياسية وتصـلح للاسـتخدام مع العديد من بـرامج إدارة الشـبكات. ويعتـبر برنـامج OSF DME مثـالاً مناسباً يحقق المواصفات القياسـية لوحـدة API من أجل برنـامج إدارة الشبكة.

3.2.2 أمن النظام System Security

أحد الخـواص الهامة لبرنـامج إدارة الشـبكة هو أن يحتـوي على نظـام لتحقيق الأمن لنفسه داخل الشـــبكة. إن برنـــامج إدارة الشـــبكة والتطبيقات المصاحبة لها تحتوي على معلومات هامة جـدا عن الشـبكة تشمل: بيانات تهيئة أجهزة مكونات الشـبكة - أمن الشـبكة وتطبيقاتها – بيانـات الأداء – طـرق الحسـابات وغيرهـا. وهـذه المعلومـات تكـون مفيـدة لقراصـنة Crackers الشـبكة الـذين قد يحـاولون اقتحـام أمن الشبكة. إن الجزء المتعلق بأمن برنامج إدارة الشـبكة يفضل أن يكـون إضـافي إلى ما يسـتطيع أن يقدمه نظـام التشـغيل من توفـير وسـائل للحماية والأمن.
إن الوظائف الأساسـية لبرنـامج إدارة الشـبكة يجب أن تمكن مهنـدس الشـــبكة من تحقيق كل الأعمـــال المتعلقة بمنـــاطق إدارة الشـــبكة. ويستطيع مهندس الشـبكة أن يستفسر عن كل معلومـات الأجهـزة من خلال برنـامج إدارة الشـبكة. وأن يسـتخدم هـذه المعلومـات بعد ذلك بحسب احتياجاته.
مثال : بفرض أن مهندس الشبكة يريد **إنشاء مخطط بياني يوضح علاقة اسـتخدام وصـلة تـوالي** Serial Link Utilization، لكل الوصلات في الشبكة. في هذه الحالة فإنه يتبع الخطوات التالية:
1- يحدد نوع المعلومات الـتي يحتاجها من كل مكونـات الشـبكة(عـادة يكون عـدد الحـروف bytes المرسـلة أو المسـتقبلة من كل وحـدة بينية Interface).
2- يسـجل الأرقـام الـتي تم تحديـدها في جـدول برنـامج إكسل Excel ويحصل على الرسم البياني المطلوب.

وتعتبر الخطوة الأولى هي الأكـثر صـعوبة. فعلى الـرغم من أن برنـامج إدارة الشـبكة يسـتطيع اسـتخدام طـرق قياسـية للاستفسـار عن كل مكونات الشبكة، فـإن كل مكـون ربما يحتفظ بالبيانـات بشـكل منفـرد Unique خاص به فقـط. إن الوسط المحيط في مجـال الشـبكات حاليا ينظم حفظ أجـزاء المعلومـات على أشـكال قياسـية تسـمى قاعـدة

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.

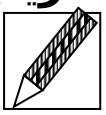
ويوجد العديد من حزم برامج إدارة الشبكات المتوفرة حاليا في الأسواق،

وفيما يلي أمثلة لبعض هذه البرامج:

- برنامج من إنتاج شركة "صن" هو Sun Net Manager Sun Connect
- برنامج من إنتاج شركة هيوليت بيكارد (Hewlett Packard) HP 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

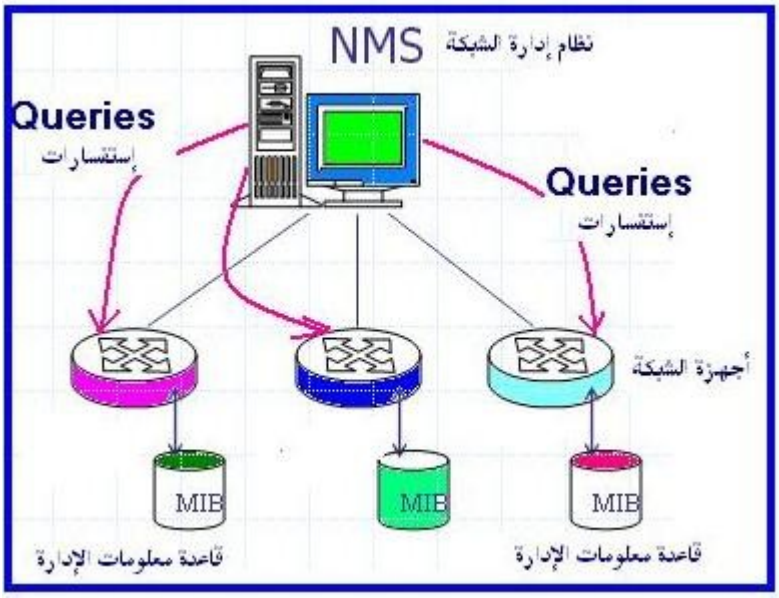
عزيزي الـدارس، يسـتطيع برنـامج إدارة الشـبكة اسـتخدام معماريـات متعـددة لأداء وظائفـه. ويوجد ثلاثة أنـواع شـائعة من معماريـات إدارة الشبكة هي:

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

ولا يوجد في هذه التقسيمات معمارية أحسن من غيرهـا. فـإن كلاً منها له خصائصه التي تجعله يعمل بشكل جيد في الوسط المحيط المناسب له. والقاعدة البديهية هي أن يستخدم النظام المعمـاري لإدارة الشـبكة الذي يكـون أقـرب إلى الهيكل المؤسسـي. حيث إنه في حـالات كثـيرة فإن هيكل الشبكة يكون في شكل مشابه.

1.3 العمارة المركزية

في البنـاء المعمـاري المركـزي يتم تنصـيب برنـامج إدارة الشـبكة على نظـام كمـبيوتري واحد عند الموضع المسـئول عن واجبـات 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 النظـام يتم نسـخه احتياطيا Backed up على نظـام آخر خلال فترات منتظمة. وعلى الرغم من أن النظام المركزي هو نقطة التركـيز لإدارة الشـبكة، فهو يسـتطيع السـماح بالاتصـال وتوجيه الأحـداث إلى وحدات إظهارConsoles (وحدة الإظهـار هـذه عبـارة عن شاشة عرض مزودة بوحدة مفاتيح) أخرى تعمل من خلال الشبكة.

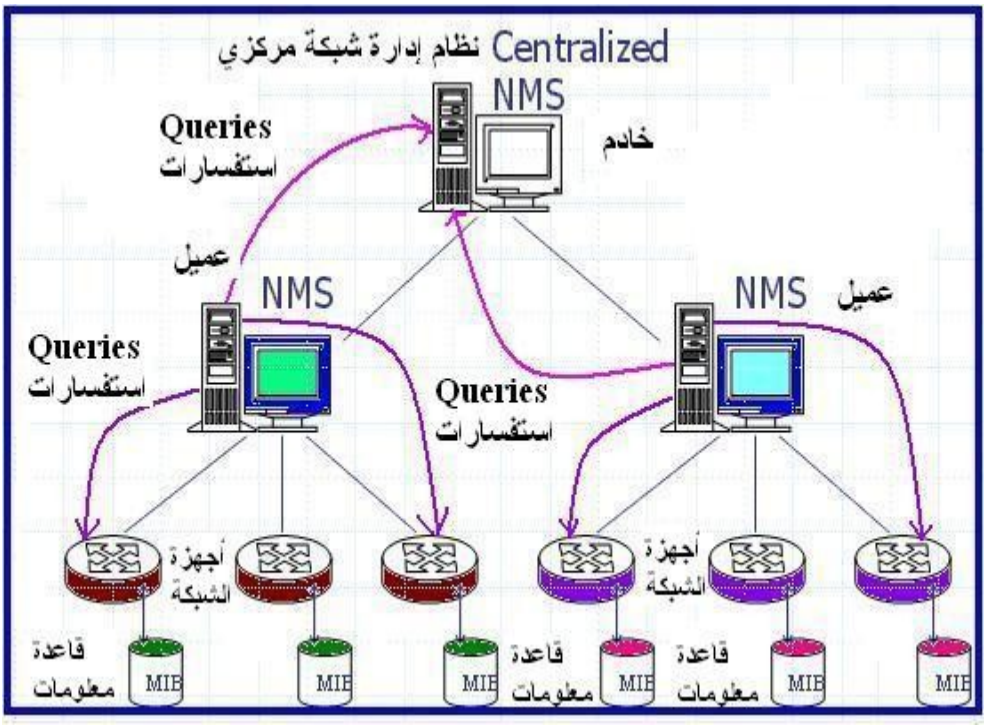
مميزات برنامج إدارة الشبكة المركزية :
يدير الأحداث والإنذارات.
يدير المعلومات.
يدير الاتصال بكل التطبيقات الإدارية.

ويسـتـ ـاهدة جميع التحذيرا ـحيص وحصر المشـــاكل. إن وجـــود مكـــان وحيد يوصل لكل التطبيقـــات الإدارية والمعلومات في الشـبكة يفي بـالغرض ويحقق الوصـول Accessibility، وتكـــون عملية الأمن أكـــثر ســـهولة في صـــيانتها. ومن الناحية الفعلية Physically فـإن محطة إدارة الشـبكة يمكن أن توضع في مكـان مغلق في منطقة محظـور دخولهـا، وأن يسـمح بـدخولها فقط للمسـتخدمين

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.

مثـال: يسـتطيع مهنـدس الشـبكات تهيئة نظم عملاء منفصـلة وذلك بإجراء عملية انتخاب Polling لرصد أجزاء مختلفة من الشـبكة. ويمكن لبرنامج إدارة الشبكة استخدام تقنيات قاعدة البيانات التي تعمل بنظام الخادم/العميل Server/Client. في هـذه الحالة فـإن العملاء لا يكـون لها نظم قواعد بيانـات منفصـلة، ولكنها تسـتخدم قاعـدة بيانـات الخـادم المركزي من خلال الشبكة.
وبسبب أن وجود النظام المركزي في العمارة الهرمي مهم جدا، لـذلك يتم عمل نسخ احتياطية Backup لتحقيق فائض Redundancy.

مميزات برنامـــج إدارة الشبكـــة المعماري الهرمي منها ما يلي:
لا يعتمد على نظام منفرد.
توزيع وظائف إدارة الشبكة.
رصـــــد الشبكـــــة 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.

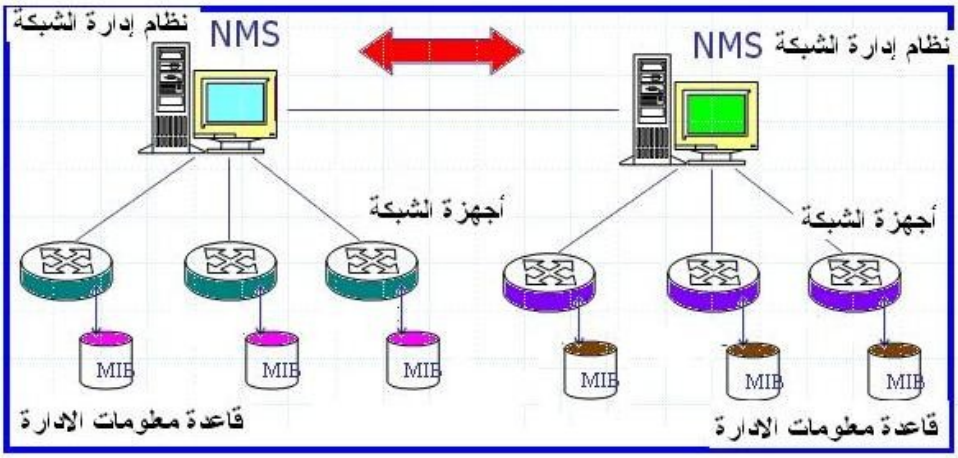
ومن أمثلة بعض الحزم البرمجية الشائعة التي تستخدم العمارة الهرمية ما يلي:

- برنامج من إنتاج شركة "صن" هو Sun Connect Sun Net Manager
- برنامج من إنتاج شركة هيوليت بيكارد (Hewlett Packard) HP 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 العمـارة الموزعة خصـائص كـلّ من العمـارة المركزية والعمـارة الهرمية. ويبين شكل2.6 نموذج للعمارة الموزعة. فبـدلا من اسـتخدام برنامج إدارة مركزي أو برامج هرميـة، فـإن العمـارة الموزعة تسـتخدم برامج إدارية نظيرPeer Platforms متعددة. أحد هذه البرامج يعمل قائدا لمجموعة من النظم الإدارية النظيرة. وكل برنامج نظـير منفـرد يمتلك قاعـدة بيانـات كاملة للأجهـزة خلال الشـبكة بأكملهـا. وهـذا يسـمح له بتحقيق وظائف مختلفة، ويرسل تقرير النتائج إلى النظام المركزي.



شكل2.6 يوضح نموذج لبناء العمارة الموزعة.

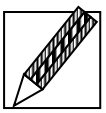
وبما أن الإدارة الموزعة تجمع معا كلاً من الطريقة المركزية والهرمية فهي بذلك تحقق مميزات كلا من الطريقتين.

مميزات برنامج إدارة الشبكة الموزعة :
تخصـيص مكان منفرد لكـل معلومات الشبكـة وكذلك التحذيرات والأحداث
تخصـــــيص مكان منفرد للوصـــــول إلـــــى التطبيقات الإدارية.
لا تعتمد على نظام منفرد.
توزيع وظائف إدارة الشبكة.
توزيع الرصد من خلال الشبكة.

وتع ة
كبي ط
بقو م

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)



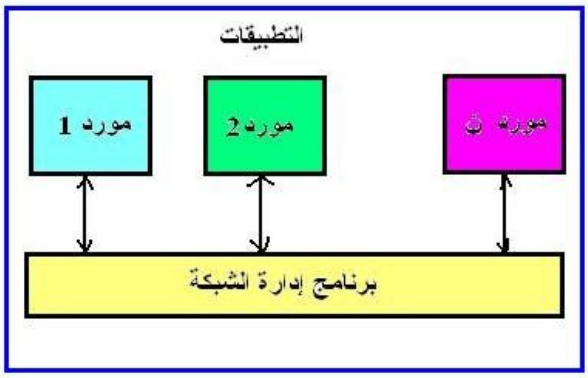
أجب بلا أو نعم

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.

4.

عزيز
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 النظـام، والاستفسـار من نفس قاعـدة بيانـات 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 برنـامج إدارة الشـبكة من خلال وحـدة API وقائمة النظام.

وكمثال على ذلـك: فـإن مصـنعي وحـدة المجمع Hub يسـتطيعون بنـاء تطبيقـات تظهر الوصـلات الفعلية الموجـودة على هـذه الوحـدة، وذلك عندما يقوم المستخدم بتحديد هـذه الوحـدة على خريطة الشـبكة. وقد يسـمح هـذا التطـبيق للمسـتخدم بتهيئة بعض خصـائص جهـاز المجمـع، وتشغيل بعض المنافذ Ports ويجعلها في حالة تشـغيل On أو حالة عـدم تشغيل Off، أو رصد معدلات الخطأ Error Rates، أو معرفة سرعة الأداء Throughput. وهـذا التطـبيق قد يسـاعد في إتمـام تأدية وظـائف إدارة الأداء بجهاز المجمع

إن تطبيقـات **إدارة الشـبكة لا ينبغي أن تنشئ تطبيقـات يمكن أن تتداخل مع برنامج إدارة الشبكة**، لأن هذا التـداخل قد ينتج عنه إيجاد طرق متعددة، يمكن أن تـؤدى نفس النتـائج الـتي يمكن الحصـول عليها من برنـامج إدارة الشـبكة. وربما يـؤدي ذلك إلى إربـاك الوحـدة البينية Interface للمستخدم. أيضا فإن إنتاج خصائص قد تكون موجـودة في برنـامج إدارة الشـبكة يـؤدي إلى ضـياع مجهـود مطـوري 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 اختيــار نظــام إدارة الشبكة

عزيزي الدارس، يتم بناء نظام إدارة الشبكة من جزأين أساسيين همـا: برنامج إدارة الشبكة، والتطبيقات المصاحبة له. وبواسطة اختيار هـذين المكونين بعناية فإنه يمكن أن يتم بناء نظام يساعد مهندس الشبكة في تحقيق الأعمـال المطلوبة في مجـال إدارة الشـبكات. وفيما يلي بيـان 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: محطـات العمل – الحاسـبات الشخصـية – معالجـات المقدمة والمؤخرة Front-end Processors – المتحكمات Controllers – بوابات الطريق Gate Ways – مفاتيح – موجهات – قنـاطر – وحـدات توصـيل Hub – طابعات – أجهزة مودم. ونحتاج معرفة إن كـانت هـذه الأجهـزة يمكن إدارتها بواســطة بروتوكــولات الشــبكة، ســواءاً كــانت هــذه البروتوكولات قياسية، أو غير ذلك (ذو ماركة مسـجلة Proprietary). إذا كان الجهاز لا يمكن إدارته بواسطة بروتوكول الشـبكة القياسـي، لا يتم حذفه من قائمة الأجهزة، فإن برنامج بوابة الطريق ربما يـتيح لنا توفـير ترجمة Translation بين بروتوكول الجهاز والـبروتوكول القياسـي. وبعد إنشاء قائمة الأجهـزة، فإننا نحتـاج عمل أولويـات للأجهـزة ذات المهـام الحرجة Critical Mission. فعلى سبيل المثـال: فبـالرغم من أنه يكـون من المرغوب فيه إدارة جميع طابعـات الشـبكة. ربما تكـون إدارة هـذه الأجهزة ذات أولوية أقل من إدارة معالجات المقدمة والمـؤخرة والـتي تقوم بتوفير عمليات الاتصال بالحاسب الكبير Mainframe.

الخطــوة الثانيــة: هي وضع أولوية لمجــالات إدارة الشــبكة الخاصة بالمؤسسة. في حـالات كثـيرة يمكن أن يكـون المجـال المهم جـدا في إدارة الشــبكة هو إدارة الأعطــال. على الــرغم من أن المؤسسة قد تعطي أولوية أولى لأمن الشـبكة أو لتهيئة الشـبكة، وبـذلك فـإن هـذه الخطــوة تكــون ضــرورية لأنها تحــدد الاحتياجــات الأكــثر أهمية لإدارة تطبيقات الشبكة وأجهزتها.

الخطوة الثالثة: هي إيجاد تطبيقات إدارة الشبكة الـتي تسـاعد على تحقيق المجـالات الأساسـية في إدارة الشـبكة وأجهزتها – والـتي تم تحديدها في الخطوة السـابقة. إن تطبيقـات إدارة الشـبكة تسـاعد في إتمـام مجـالات أعمـال إدارة الشـبكة. وبـدون هـذه التطبيقـات فـإن الوظـائف العامة لبرنـامج إدارة الشـبكة هي الـتي تسـاعد على إتمـام أعمال إدارة الشبكة. وباستعمال التطبيقـات المصـممة لإدارة الأجهـزة يستطيع مهندس الشبكة وضع أولويات تسـمح بتخصـيص مصـادر فعالة لإدارة الشبكة بدلا من بناء تطبيقات تسمح بتحقيق إدارة الشبكة.

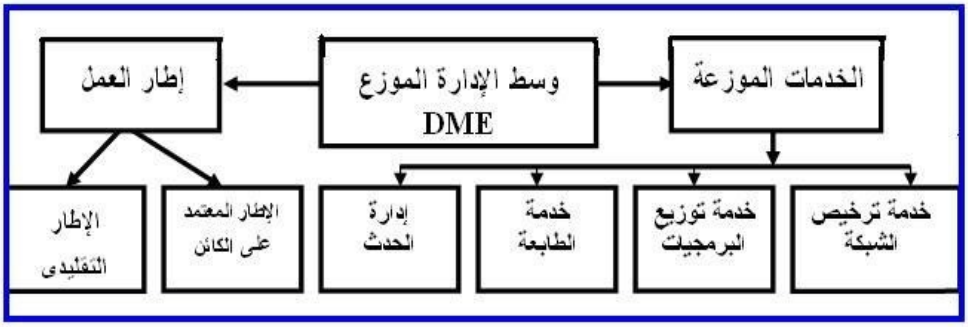
الخطوة الرابعة: هي اختيار برنـامج إدارة الشـبكة. من الطـبيعي أن تكون التطبيقات التي يتم اختيارها جميعها سوف تعمل بواسطة برنامج إدارة الشبكة. إذا كانت هذه التطبيقات تعمل على برنـامج إدارة شـبكة واحد فقط، فإن هذا الاختيـار يكـون مباشـرا. أما إذا كـان هنـاك اختيـار لعدة برامج لإدارة الشبكة، فإنه يجب اختيار برنامج إدارة الشبكة الـذي يناسب معمارية الشـبكة الـتي تزمع المؤسسة في التخطيط لإدارتهـا. على سـبيل المثـال، إذا كـانت المؤسسة تخطط لإنشـاء مركز إدارة شبكة مركزي واحد، دون الاحتياج إلى إنشاء شبكات عند مواقع أخـرى، فإن برنـامج الإدارة المركـزي أو الهـرمي يكـون هو الأفضـل. إذا كـانت المؤسسة تخطط لإنشاء مراكز إدارة شبكة ذات فائض متعدد Multiple Redundant من خلال الشبكة، فإن اختيـار إدارة شـبكة مـوزع يكـون هو الأنسـب. على سـبيل المثـال، إذا كـان برنـامج إدارة الشـبكة المناسب لشبكة البيانـات يتطلب عتـاد لا تملكه المؤسسـة، ولا تسـتطيع توفـيره فإنه يكـون من الأفضل اختيـار برنـامج إدارة شـبكة أقل من المناسب بحيث يمكن تشـغيله على العتـاد الـذي تملكه المؤسسة أو تسـتطيع توفيره. إن برنامج إدارة الشـبكة، يحتـاج وجـود عتـاد لتشـغيله، وإذا لم يتـوفر هـذا العتـاد فـإن ذلك يجعل مهمة برنـامج إدارة الشـبكة صـعبا. ويوجد متاحا في الأسواق، بـرامج إدارة شـبكات تعمل على نظم عتـاداً متنوعة (تشمل: الحاسبات الشخصـية – محطـات العمل – الحاسـبات الكبيرة) وكذلك برامج مناسبة لنظم عتاد متعددة.

وباتباع الخطوات السابقة فإن مهنـدس الشـبكة يسـتطيع اختيـار نظـام إدارة الشبكة الذي يعمل بطريقة جيدة على شبكة البيانات التي توفرها المؤسسة.

6. إدارة الوسط الموزع DME

قـــامت مؤسسة "إيجـــاد الـــبرامج المفتوحة OSF " وهي إحـــدى المؤسســـات الـــتي تستكشف التقنيـــات الـــتي تســـتخدم في صـــناعة

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 :

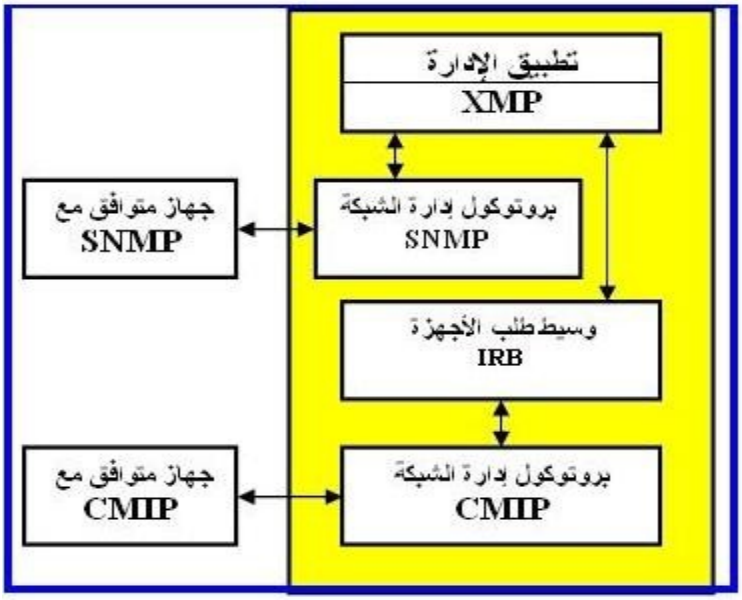
وهي تصنع من كل الخدمات التي تساعد في إدارة الوسط الموزع، مثل إدارة الحدث – خدمة الطابعة – طرق البرمجيات الموزعة – خدمات ترخيص الشبكات.

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 شـكل2.9. ويسـتعمل هـذا الإطـار في شـبكات الخادم/العميل، ويمثل الخادم نظام إدارة الشبكة ويمثل العميل أجهـزة الشبكة. **ويحدد إطـار العمل التقليـدي المواصـفات القياسـية الـتي يوفرها برنـامج إدارة الشـبكة والتطبيقـات المصـاحبة 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 القياسـية لوحـدة واجهة المسـتخدم الرسـومية GUI باسـتخدام X11 Motif (وهي مجموعة برمجيـات مكتبية تـوفر تطبيقات من خلال نظام نوافذ موزعة). ويستطيع مهنـدس البرمجيـات استخدامها في كتابة التطبيقـات، كما أنه يمكن تشـغيلها على محطـات عمل وحاسبات شخصية متنوعة. ويستخدم الإطـار التقليـدي طريقـتين لتجميع البيانـــات من الشـــبكة هما برتوكـــول SNMP وبروتوكـــول CMIS/CMIP. وبذلك يستطيع هذا البناء إدارة كل الأجهزة الـتي تـدعم بروتوكول SNMP وكذلك الأجهزة التي تدعم CMIS/CMIP.

ويتم بنـاء وحـدة مواجهة الـبرامج التطبيقية API باسـتخدام XMP (X Management Application Interface). وهذه الوحدة توفر طريقة اتصال

لكل من بروتوكـــول SNMP وبروتوكـــول CMIS/CMIP. ولكن هـــذين الـــبروتوكولين لهما قواعد مختلفة تحكمهما معلومـــات الإدارة الهيكلية لهمـــا. وهـــذا يجعل ضـــرورة أن يســـتعمل XMP طريقـــتين مختلفـــتين لتوصـــيل هـــذه الـــبروتوكولات. إن XMP يـــوفر اتصـــالاً مباشـــراً مع الـبروتوكول SNMP. ولكن يوجد مسـتوى آخر مجـرد هو وسـيط طلب الأجهزة (Instrumentation Request Broker) IRB الذي يحـاول توفـير وحـدة بينية مبسـطة للـبروتوكول CMIS/CMIP كي يسـمح لمطـوري التطبيقات برؤية أجهزة الشبكة ككائنات يمكن إدارتها. وهـذا المسـتوى المجرد Abstract يسـمح بتصـميم برتوكـول CMIS/CMIP المعتمد على الكائنـــات كي يعمل من خلال إطـــار العمل التقليـــدي. إن وحـــدة IRB تسمع بالتطبيقات بأن ترى أجهزة الشبكة ككائنات.

الجزء الاول إطار العمل .. الجزء المعتمد على الكائن والكـائن Object هو عبـارة عن كيـان بـرمجي تم تحديـده وله صفات خاصة به وكذلك دوال Methods تحكم سلوكه، وأعمال داخلية. إن الهيكل الداخلي للكـائن يكـون غـير معلـوم Hidden خـارج الكائن. إن التطبيقات الـتي تسـتخدم الكـائن تحتـاج أن تعـرف صـفات الكـــائن ودوال الكـــائن. إن الكائنـــات تخفي التعقيـــدات وتســـهل بنـــاء التطبيقات المعقدة بواسطة تقسيم الأسـطح الكثـيرة للتطـبيق وجعلها مكونات صغيرة غير قابلة للتجزيء Indivisible.

على سبيل المثـال: نفـترض أنه تم إنشـاء تطـبيق تقرير موضـحا نسـبة زمن بداية التشغيل Up-time لكل وصلات التوالي الموجودة في شـــبكة البيانات. يمكن اعتبار وصلة التوالي هي كـائن له الخصـائص الخاصة به (المتغيرات) وكـذلك الـدوال الخاصة بـه(سـلوكيات). ويمكن أن تكـون خصائص الكائن "وصلة التوالي" عبارة عن سـعة نطـاق نقـاط النهاية – التأخير الناتج عن الانتقـال Propagation Delay – معـدل الأخطـاء لكل ثانية – سرعة البيانات في الثانية – زمن بدء التشـغيل – محـدد الـدوائر. ويمكن أن تشمل الـدوال الخاصة بالكـائن "وصـلة التـوالي" على بداية التشغيل **استخدام اتساع النطاق Bandwidth Utilization** معـدل استخدام الخطأ Error Utilization . وإذا أراد التطـبيق **إنشـاء تقرير** لتوضيح نسبة بداية التشغيل لكل كائنات وصـلات التـوالي خلال الشـهر 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 رسـومية قياسـية شـائعة لكل تطبيقـات الإدارة. ومن وجهة نظر تقنية الكـائن، فـإن وحـدة MUI تمثل كائنـاً إداريـاً يقـوم بتوفـير دوال تستطيع الاتصال بعناصر شاشة العرض في نظام إدارة الشبكة.

ولتحـــديث وحـــدة DME لكي تتعامل مع تقنية الكـــائن، فإنه يمكن استخدام وحدة موائم للبروتوكول SNMP. يستطيع هذا المـوائم ترجمة العمليات الأساسية للبروتوكول SNMP كي يعمل مع دوال DME. وهذا يمّكن بروتوكـــول SNMP من إدارة الأجهـــزة ورؤيتها كأنها كائنـــات 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.

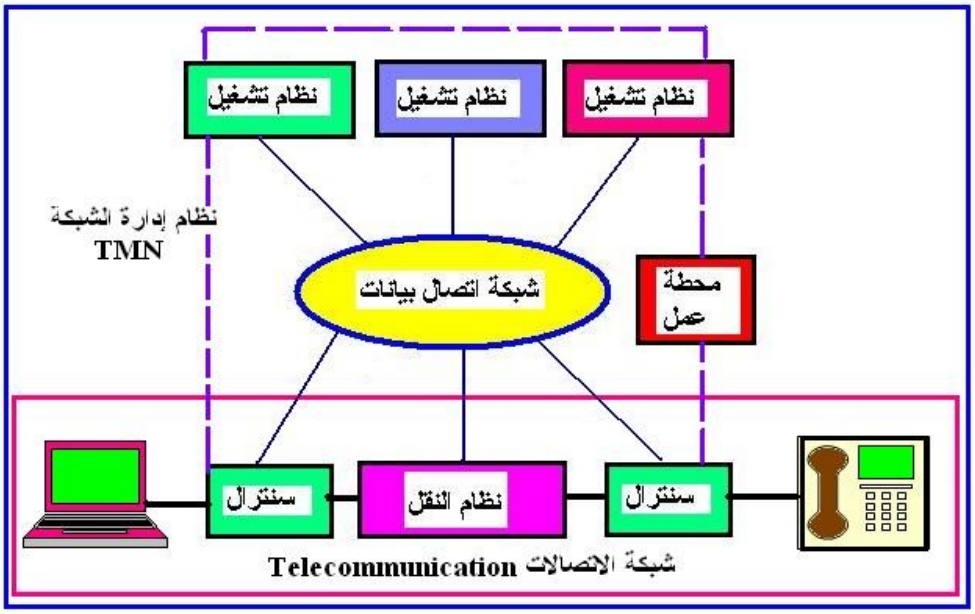
وتوفر خـدمات الحـدث وسـيلة لـدخول وترشـيح وتوجيه الأحـداث ذات العلاقة بالشـبكة في الوسط المـوزع. وتقـوم خـدمات الطابعة بتوفـير خدمة طباعة موزعة من خلال الشـــبكة. وتتم عملية التعامل مع رخص البرمجيات الخاصة بأعمـال الصـيانة والتحكم من خلال الخـدمات الـتي توفرها وحـدة خـدمات تـرخيص الشـبكة. وتسـاعد خـدمات الـبرامج الموزعة على تنصيب التطبيقات من أجل الاستخدام الموزع.

مما سـبق شـرحه نجد أن إطـار العمل التقليـدي يسـتطيع العمل جيـدا لإدارة مكونـــات إدارة الشـــبكة مســـتخدما الـــبروتوكولات القياســـية المتـوفرة في الأسـواق. أما إطـار العمل المعتمد على تقنية الكائنـات فهو يستخدم في بناء تطبيقات إدارة الشبكة المعقـدة (الكبـيرة)، وذلك بحسب تقنية ومعمارية الشبكة.

7. إدارة شبكات الاتصال TMN

عزيزي الدارس، نشأ مقترح إدارة شـبكات TMN من قبل هيئة التوحيد القياسية المعروفة باسم ITU-T والتي كانت تعرف سـابقا باسم هيئة الاتصـالات CCITT. وتعـرف الوثيقة رقم M.3010 التوصـيات الخاصة بإدارة شبكات TMN ، كما يوجد بها علاقة ترابط قوية مع نظـام إدارة OSI. يعمل نظام إدارة الشبكات TMN كشبكة منفصلة تربطها وحدات

بينية مع شـبكة الاتصـالات عند نقـاط اتصـال مختلفة متعـددة من أجل إدارتها. ويوضح شكل2.10 العلاقة بين نظام إدارة شـبكات TMN وبين شبكة الاتصالات الـتي يقـوم بإدارتهـا. ولتحقيق أغـراض إدارة الشـبكة، يتم ربط السـنترالات Exchanges، ونظم النقل Transmission systems من خلال شبكة اتصـالات البيانـات، والـتي توصل بها مجموعة من نظم التشغيل Operations Systems.

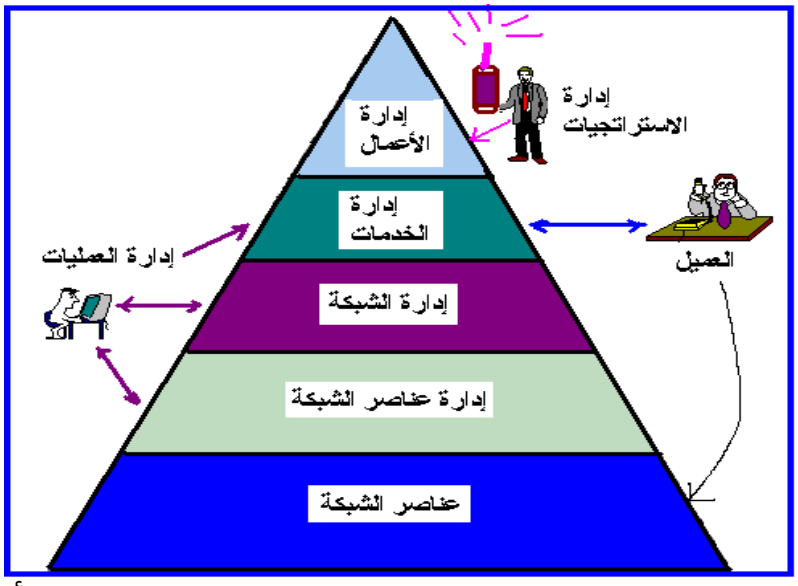


شكل2.10 نظام إدارة الشبكة TMN.

تقوم نظم التشغيل بتحقيق معظم وظائف الإدارة، والـتي يمكن أن تتم آليا أو بواسطة مهندس إدارة الشـبكة. كما يمكن أن يتم تحقيق وظيفة إدارية واحدة بواسطة العديد من نظم التشغيل. في مثل هذه الحـالات، فـإن شـبكة البيانـات سـوف تقـوم بـإجراء عمليـات تبـادل المعلومـات الإدارية بين نظم التشغيل. وتقوم شبكة اتصـال البيانـات أيضا بتوصـيل محطات العمل Work Stations، التي تسمح لمهندس الشبكة بتفسـير معلومـات الإدارة. وتحتـوى محطـات العمل على وحـدات مواجهة بينية مع المسـتخدمين. وتقسم أعمـال إدارة الشـبكات TMN إلى عـدة مستويات بنائية هي:

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

- البنـــاء الفعلي Physical Architecture : وهو مختص بكيفية تحقيق الوظائف الإدارية على الأجهزة الفعلية الموجودة في الشبكة.
- البناء المعلوماتي Information Architecture : ويصف الأعمال الـتي تم تطويعها من نظـام إدارة OSI لتلائم نظـام TMN ، ويسـتخدم التقنيات المعتمدة على الكائن Object Oriented.
- البناء الطبقي المنطقي Logical Layered Architecture: وهو يشتمل على واحد من أحسن الأفكـار الـتي اسـتخدمت في إدارة شـبكات TMN، وهو بنـاء نمـوذج يوضح كيفية تقسـيم الأعمـال 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 مسـتويات، كما هو موضح في شكل2.11، هي:

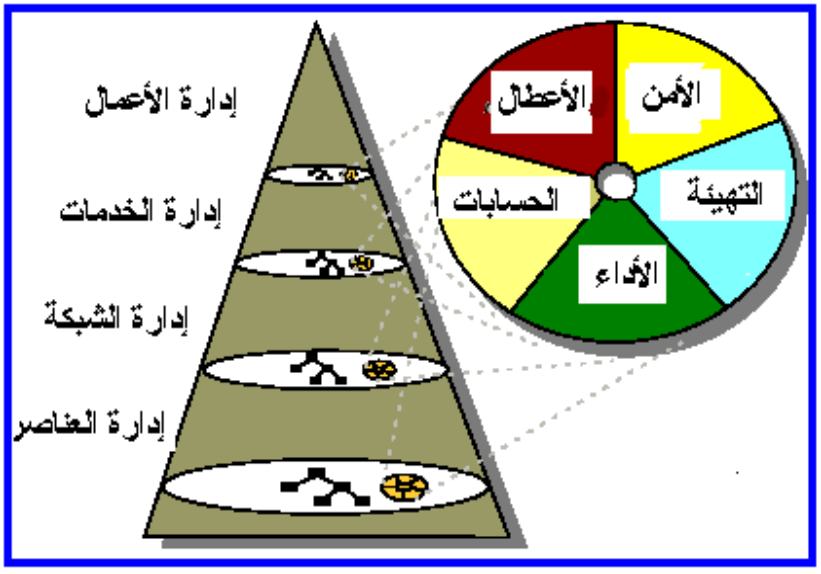
- **مســـتوى إدارة الأعمـــال:** لتحقيق الوظـــائف الخاصة بالأعمال، وتحليل الاتجاهات، وعوامل الجودة، وتوفير فواتير الدفع المبنية على هذه الأسس وكذلك التقارير المالية.
- **مســتوى إدارة الخــدمات:** يحقق مهــام متعلقة بتقــديم خدمات الشبكة، مثل أعمال الإدارة وتحديد تكلفة الخدمات.
- **مســتوى إدارة الشــبكة:** يحقق وظــائف متعلقة بتوزيع مصــادر الشــبكة، مثل التهيئة والتحكم في الإشــراف على إدارة الشبكة.

- **مستوى إدارة العناصر**: يختص بالمهام المتعلقة بالتعامل مع عناصر الشـبكة. ويشـمل ذلك إدارة الإنـذارات، معالجة المعلومـات، النسخ الاحتياطيـة، عمليـات الـدخول للشـبكة، وصيانة عتاد وبرامج الشبكة.

ويمكن أيضا أن ننظر إلى نمـوذج إدارة الشـبكات TMN من وجهة نظر وظيفيـة، كما هو موضح في شـكل2.12، والـتي يمكن من خلالها أن نصف النموذج على أنه يتكون من خمسة مكونات وظيفية هي:

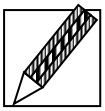
- **إدارة الأعطـال**: وهي تختص بـالتعرف على العطل وعزله وتدوينه وتصليحه إن أمكن.
- إدارة **الحسـابات**: وتختص بتجميع وتخـزين، وتحديد الفواتـير ومعلومات الحسابات.
- **إدارة الأداء**: و تختص بتجميع البيانات الإحصائية وتحديد خطة اتساع الشبكة.
- **إدارة التهيئة**: وتختص بتنصيب أجهـزة الشـبكة، وضـبط معـاملات الشبكة، وتهيئة سعة الشبكة.
- **إدارة الأمن**: وتختص بمهـام متعلقة بتوثيق الإدارة، والحماية من الاختراقات والمستخدمين غير المفوضين.

وهذه المجالات الوظيفية الخمسة السابقة، تكون الأساس لجميع نظم إدارة الشـبكات لكل من شـبكات البيانـات، وكـذلك شـبكات الاتصـال Telecommunication .



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.

الخا

عزيز
بالتفصيل
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، وناقش 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 يشـتمل على واحد من أحسن الأفكـار الـتي اسـتخدمت 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

المصطلح بالإنجليزية	معناه بالعربية
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
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

المصطلح بالإنجليزية	معناه بالعربية
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

الموضوع	رقم الصفحة
مقدمة	**73**
تمهيد	**73**
أهداف الوحدة	**74**
1. فوائد عملية إدارة الأعطال	**75**
2. تحقيق عملية إدارة الأعطال	**76**
3. تجميع المعلومات اللازمة لتحديد المشكلة	**79**
4. تحديد الأعطال الواجب إدارتها	**82**
5. إدارة الأعطال في نظام إدارة الشبكة	**84**
6. تأثير الأعطال على الشبكة	**99**
7. أشكال تدوين الأعطال	**102**
1.7 مميزات استخدام الرسومات الملونة	103
2.7 استخدام الخرائط الهرمية والألوان	103
الخلاصة	**109**
لمحة مسبقة عن الوحدة التالية	**109**
مسرد المصطلحات	**110**
المراجع	**113**

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).

نســتعرض في هــذه الوحــدة فوائد عملية إدارة الأعطــال، وننــاقش الخطوات الثلاثة المتعلقة بإتمـام صـيانة الأعطـال في شـبكة البيانـات. ونصف ثلاثة احتمالات ممكنة للأدوات الـتي يمكن اسـتخدامها. ونشـرح 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 الوحدة ينبغي 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 الأعطـال **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 مهمـا، لأن كثــيراً من المســتخدمين يعتمد كلية على شــبكة البيانــات لتأدية أعمـالهم تماما مثل اعتمـادهم على خـدمات شـبكة التليفونـات. 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.

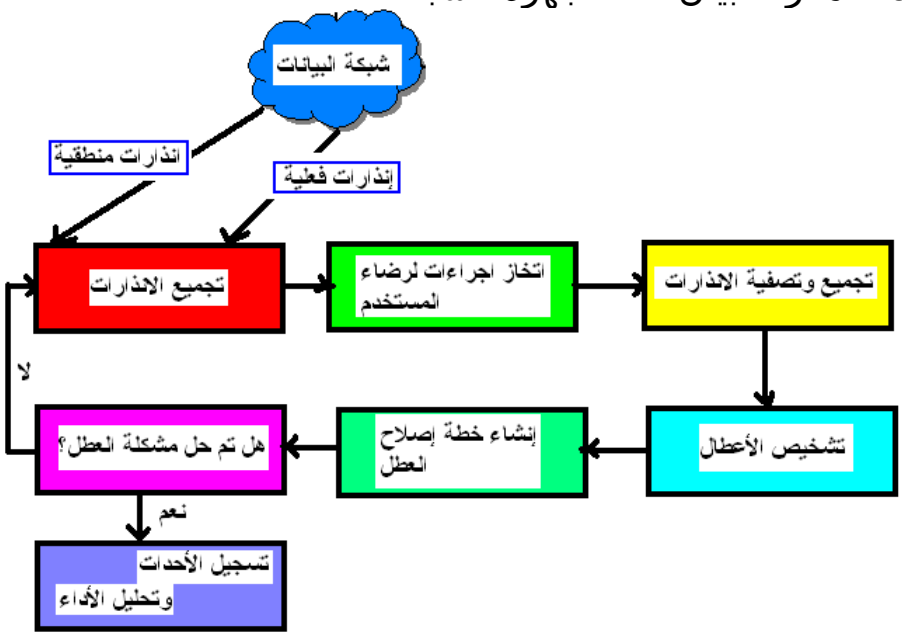
الخطوة الثالثة تصليح العطل (إن أمكن).

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 وتـدوين الإنـذارات، فإنه يتم اتخـاذ إجـراءات خدمية مؤقتة لسد الثغرة الناتجة عن وجـود العطـل، بينما يتم إجـراء عملية تشـخيص العطـــل، كي نضـــمن أن المســـتخدم لا يعـــاني من فقد أو نقص في الخـدمات. على سـبيل المثـال، يمكن تحويل حركة مسـار الرسـائل لمسارات بديلة، أو تغيير أجزاء العتاد التالف بأجزاء أخرى بديلة صـالحة قريبة من موضع الخطأ.

وبعد ضمان عملية رضاء العميل، فإن الخطـوة التالية هي أن يتم إيجـاد علاقات الارتباط Correlations بين الإنذارات، و تصفية Filter الإنذارات. وذلك بواسطة تحليل الإنذارات وحذف الزيادات Redundant (الإنـذارات المتكررة) منها. ويتم تحديد الأعطال بواسطة تحليل الإنذارات الـتي تم تصـفيتها وإيجـاد العلاقـات بينهـا، وكـذلك بواسـطة اختبـارات الانتخـاب Polling لمعرفة بيان حالة أجهزة الشبكة.



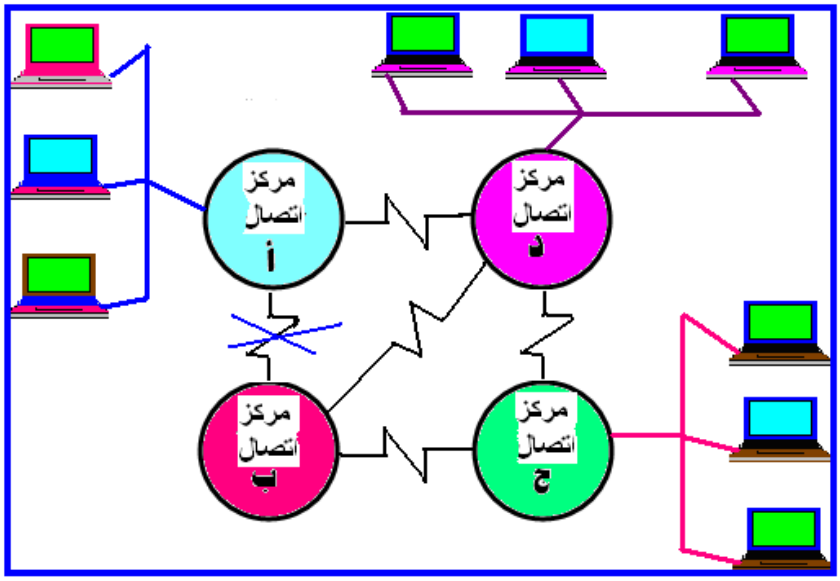
شكل1-3 مراحل عملية إدارة الأعطال في شبكة البيانات.

وبعد تشخيص العطل، يتم اتخاذ إجراءات الإصلاح، وذلك بواسطة عـزل سبب العطل. حيث يقوم نظام إدارة الأعطـال بعملية الإصـلاح، واتخـاذ بعض الإجـراءات طبقا للخطة الموضـوعة للإصـلاح. تتم عملية الإصـلاح إما آليا بواسطة برامج وأجهزة التحكم في تشغيل الشبكة، أو بواســطة مهندس الشبكة، وذلك بواسطة إحلال مكونات صـالحة للعمل بـدلا من التالفة. يتم بعد ذلك تسجيل الأحداث التي وقعت في الشـبكة وتشـمل الأعطـــال ويتم عمل تحليل إحصـــائي بعد ذلك يفيد في بنـــاء 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

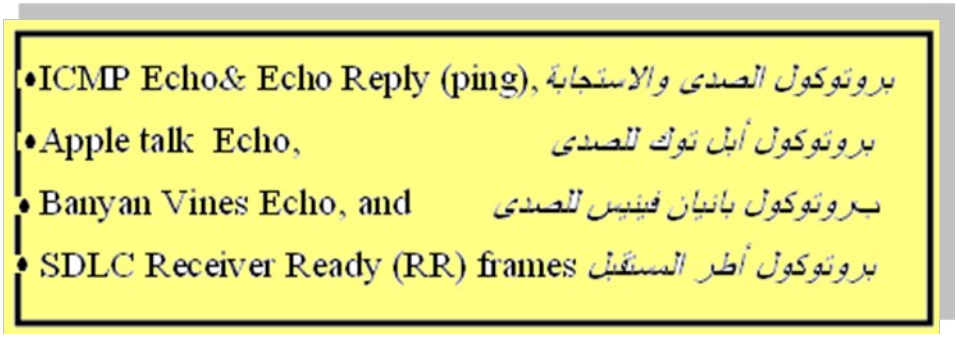
يتم إرسال هذه الأحداث بواسطة جهاز الشبكة عندما يحدث شرط العطل. إن أحداث الشبكة الحرجة قد تكون على سبيل المثال: عطل في إحدى الوصلات – إعادة تشغيل جهاز – أو عدم استجابة من الحاسب المضيف Host. في معظم الحالات، فإن الاعتماد على هذه الأحداث بشكل مطلق، لا يوفر كل المعلومات اللازمة لإدارة الأعطال بفاعلية. على 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 172,800,000بايت (,00048 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 (,00048 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:



ملحوظة: إن هذه الطريقة في حد ذاتها تـوفر فقط المعلومـات الـتي تساعد في تحديد شرط عطل ممكن.

4. تحديد الأعطـــال الـــواجب إدارتها في الشبكة

عزيزي الدارس، ليس لكل الأعطال الـتي قد تحـدث في الشـبكة 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 الأعطـال الـتي ينبغي إدارتها هي أنـواع الأعطـال الأكـثر أهمية في الوسط المحيط بشبكة معينة. وينبغي إجراء ذلك لعدة أسباب:

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

ثانيـا: بواسـطة تحديد حركة الحـدث Event Traffic، نسـتطيع تقليل عمليـات الإرسـال الزائد أو المعلومـات غـير المفيـدة وتقليل الفقد في سعة نطاق الشبكة.

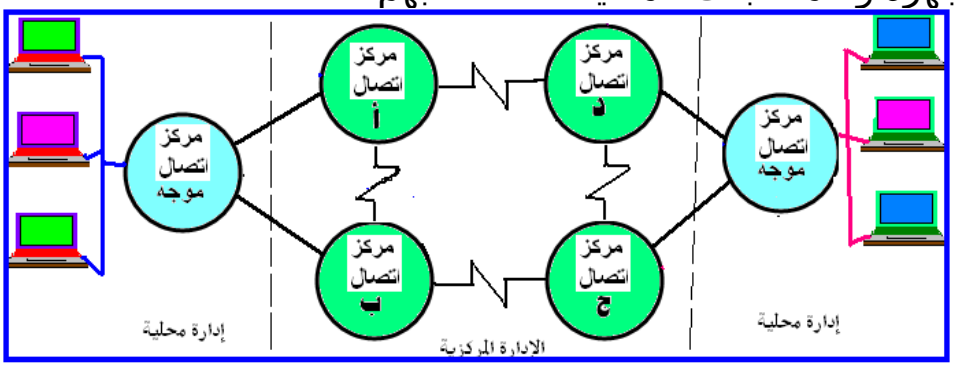
على سبيل المثال، نفترض أن صانع محطة العمل قد قرر توليد أحـداث الشبكة عندما يقوم المسـتخدم بالـدخول على النظـام. بـالرغم من أن هذا الحدث يوفر معلومات مفيدة من أجل الحسـابات، فإنه غـير مفيد (Irrelevant Event)ـ لإدارة الأعطـال. والآن نفـترض أن أحد أقسـام مؤسسة اشترى 100 محطة عمل. فـإن مـديري وحـدات العمل تقـوم بتهـيئتهم ليس فقط باسـتخدام التهيئة المتـوفرة من قبل المصـنع (Default Configuration)، ولكن أيضا باسـتخدام التعليمـات الـتي يتم إرسالها إلى أدوات إدارة الأعطال المركزية لكل أحـداث الشـبكة. ويتم ذلك في كل وقت يتم فيه دخـول المسـتخدم. ويمكن لهـذه الأحـداث الدخيلة Extraneous Events أن تملأ بسرعة قاعـدة بيانـات نظـام 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 البيانـات المعروفة باسم ميجـانت، فـإن بروتوكـول الاتصـال X.25 يسـتخدم في تنفيذ اختبـار الصـدى وذلك بمحاولة إنشـاء دائـرة تخيلى Virtual Circuit لكل عنــوان هــدف باســتخدام X.121 (منظم العناوين) من خلال الشبكة. يتم تدوين الإخفاقات في عمليات الاتصال بالشبكة وذلك لإجراء فحوصـات إضـافية عليهـا. وتكـون هـذه الوسـيلة مفيدة بالتحديد إذا كانت الحاسبات المضـيفة أو الأجهـزة ليست ممزقة بدرجة كافية كي تقوم بإرسال أحداث الشبكة.
إن الخــرج النــاتج عن هــذه الأداة البســطة، يكــون بســيطا مثل ملف الدخول أو معقدا مثل تغيير الألـوان في الخريطة الهرميـة. بعد أن يفقد الجهاز التوصـيل، فـإن الأداة البسـيطة تنبه مهنـدس الشـبكة كل فـترة زمنيــة. من الممكن ضـبط تنفيذ الأداة البسـيطة كي توصل إلى جهـاز الاستدعاء (Pager) مباشرة وترسل رسالة عددية بعنوان الشبكة لبيــان الجهاز غير المستطاع الوصول إليه.

اسئلة تقويم ذاتي

؟

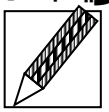
لتحقيق عملية إدارة الأعطال في شبكة البيانات نتبع الخطوات الثلاثة التالية
1- .....
2- .....
3- .....

تأثير تبولو
إن الوسط ا ة
ربط مثل المكرر – الجسور – المجمع Hub. وقد يوجد للشــبكة المحلية نــوعين من التبولــوجي Topology هما التبولــوجي الفعلي Physical و التبولوجي المنطقي Logical. ويمكن تخطيط الشـبكة المحلية بإمكانية أن يتم نقل منطقي لقطاعــات Segments فعلية من أجهــزة الشــبكة. وهــذا يعــني أنه يوجد اختلاف في التبولــوجي الفعلي عن التبولــوجي المنطقي للشبكة. وعندما تقوم الأداة البسيطة بعملية تبليغ المعلومات فإن الجهـاز أو القطـاع لا يمكن الوصـول إليـه. ولهـذا يجب أيضا وصف الشــبكة المحلية التصــورية الموجــود بها تبولــوجي الشــبكة المحلية الفعلي، لمساعدة مهندس الشبكة في تشخيص المشكلة في وقتها.

وباســتخدام الأداة البســيطة، فــإن الحاسب المضــيف قد لا يســتطيع الوصول إليه من خلال الوحدة البينية لموجهات معروفة. إذا حــدث ذلك

فإن الأداة تغير لون الوحدة البينية للموجه لتبين أن الحاسب المتصل به لا يمكن الاتصـال بـه. في الواقـع، فـإن الوحـدة البينية للموجه يمكنها الاتصال بالشبكة المحلية التصـورية، ويعـني ذلك أن الحاسب المضـيف الـذي لايسـتطاع الوصـول إليه ربما يكـون في أي مكـان في تبولـوجي الشبكة. وتقوم الأداة البسيطة بعزل المشكلة الخاصة بحاسب مضـيف موجـود على الشـبكة المحلية التصـورية. ولكن لإيجـاد المكـان الفعلي بالضـبط لهـذا الجهـاز ربما يتم ذلك مباشـرة. أو ربما بواسـطة اختبـار 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.

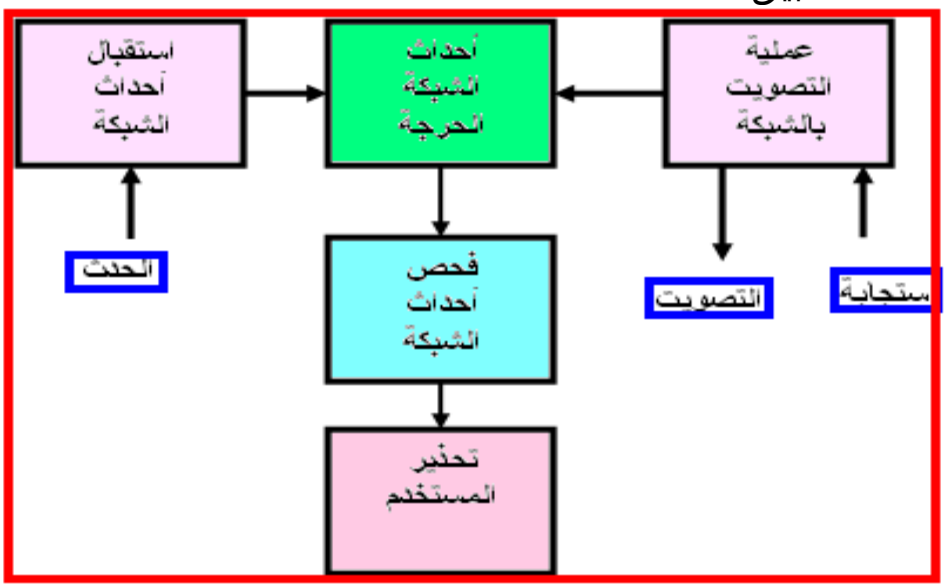
- **برمج**
الأعـ

يوجد هـــذا
الشبكة المت
نوعية للاست
حالات الأجه
الشـبكة تقـ

أمكن فحص إحصائيات حيوية مثل تشغيل الوحدة البينية لكل جهـاز. إن برنامج إدارة الشبكة يستطيع غالبا إيجـاد حالة التشـغيل للوحـدة البينية لكل جهاز، حتى وإن لم يكن لهذه الوحدة البينية عنوان بالشبكة.

2.5 لأداة المركبة لإدارة الأعطال

إذا كـانت الحاسـبات المضـيفة والأجهـزة الأخـرى الموجـودة بالشـبكة متطورة بدرجة كافية لتدوين أحداث الشبكة، فـإن الأداة المركبة يمكن تطويرها للاسـتفادة من هـذه الإمكانيـة. إن هـذه الأداة سـوف تقـوم بالتبليغ عندما تكتشف مشكلة، إما بواسـطة دخـول أحـداث الشـبكة أو بواسطة إجراء عمليةانتخاب Polling. إن عملية إيجـاد العطل من خلال الأحداث الحرجة للشبكة يسـاعد أيضا في عـزل السـبب، أو على الأقل يقوم بتدوين الجهـاز. ويوضح شـكل4-3 خريطة التـدفق لتوضـيح كيفية أداء هذا التطبيق.

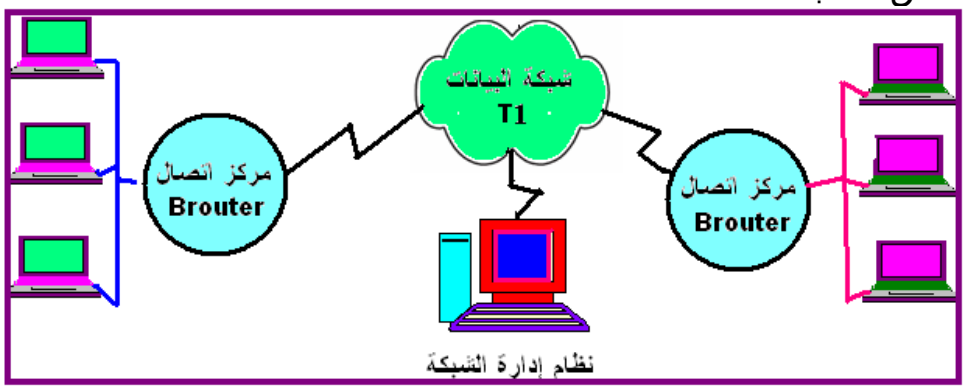


شكل4-3 خريطة تدفق تبين تتبع أداة مركبة لإدارة الأعطال في الشبكة.

كيفية عمل الأداة المركبة:

مثال1: لتوضيح كيفية عمل الأداة المركبة، نفترض نظـام إدارة شـبكة ميجانت الموضح في شكل 5-3. يقوم الجهاز T1 بتوفير دائرة سـرعتها 1.544 ميجـابت / ثانية بين وحـدتين لجهـاز موجه / قنطـرة (بروتر Brouter) يسـتخدم بروتوكـول الاتصـال TCP/IP. إن الجهـاز T1 يـؤدي

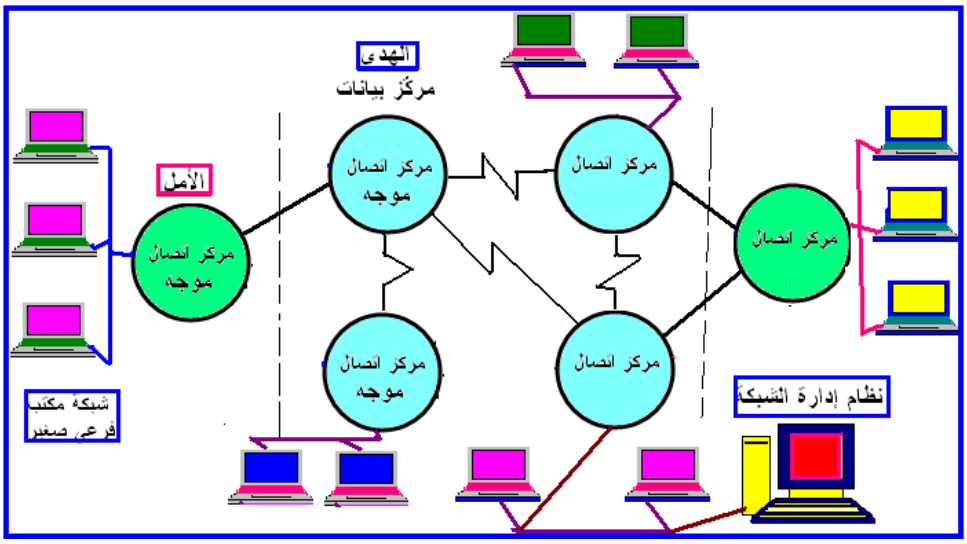
عمله بشكل صحيح، ولكن الدائرة الموجـودة من قبل شـركة التليفـون المحلية تعطلت بسبب مشكلة العتـاد Hardware. في هـذه الحالة فـإن كل "بروتر" يقوم بإرسال حدث شـبكة حـرج إلى نظـام إدارة الشـبكة. ويقــوم التطــبيق بعد ذلك في الحــال، بتحويل هــذه المعلومــات إلى مهندس الشبكة.



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

مثال2: تقوم شبكة ديكنت الموضحة في شكل 6-3 بتوفير مثال أكـثر تعقيدا لكيفية استخدام القدرة التدوينية لأجهـزة الشـبكة. تشـمل هـذه الشـبكة محطة عمل تسـمى "الأمـل" وهي عبـارة عن موجه لشـبكة ديكنت متوفر به ذاكرة مقدارها واحد جيجا بـايت لإجـراء جميع عمليـات المعالجة اللازمة للشـبكة بما في ذلك مخـزن البفر (Buffer Storage). غير معروف لنـا، إن هـذه الـذاكرة غـير كافية لمعالجة أنشـطة الشـبكة المتوقعة من هذا النظام.

إن محطة العمل بمركز اتصال "الأمل" بها شبكة واحـدة محلية متصـلة بخط توالي بموجه شبكة مماثل يسمى "الهدى"، والذي تم تهيئة ذاكرته لتحتوى 5 جيجابايت لأغراض الشبكة. كما هو موضح بالشكل 6-3، فإن "الأمـل" يقيم في مكتب فـرعي صـغير. بينما "الهـدى" هو عبـارة عن مركّز بيانــات مركــزي (Concentrator) متواجد في منتصف الشــبكة. المسار المتوفر فقط للبيانات من "الأمل" إلى باقي الشبكة يكـون من خلال وصلة توالي متصلة بجهازي الموجهين.



شكل3-6 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 Signalوهي 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:**

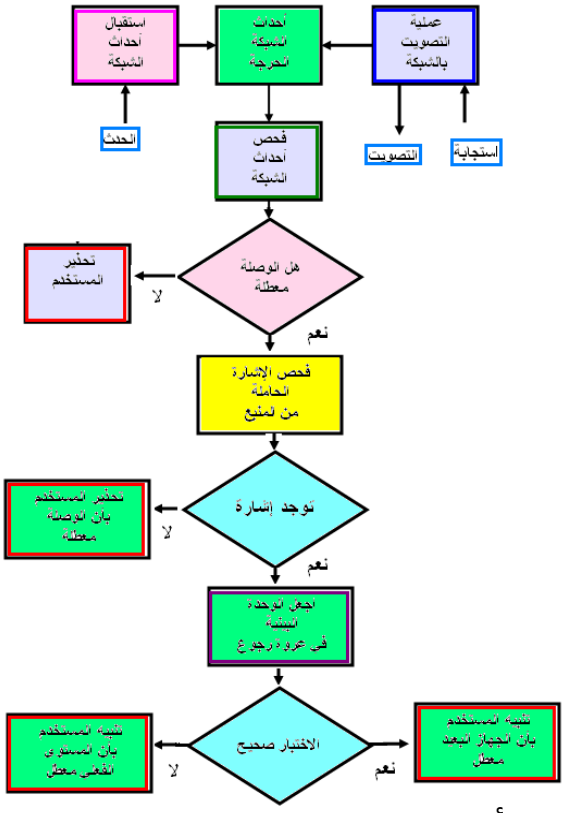
لعزل العطل، فإن أداة إدارة العطل تستطيع اختبار الوصلة بواسطة وضع وحدة التوالي البينية في "الهدى"، وتعمل حلقة رجوع (Loop Back)، ويتم إعطاء تعليمات للموجه باختيار الوحدة البينية الخاصة به. بإجراء هذا الاختبار سيتم اختبار العتاد والتوصيلية لجزء من الوصلة. إذا أخفق هذا الاختبار، فإن الأداة يجب أن تدون ذلك، 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 7-3 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

بالـذات. إن المعلومـات الإضـافية كـان باسـتطاعتها تعجيل عملية إدارة العطل. من الناحية العملية، فإن الأدوات الـتي تـؤدى كل هـذه الخطـوات تكـون نـادرة، أو لا وجـود لها مطلقـا. ولكن يوجد أدوات كثـيرة منفـردة تسـتطيع أداء (تحقيـق) كل جـزء معين من مجموعة التقنيـات الشـائعة (اختبار إشارة الحمل – وضع الوحـدات البينية في حالة عـروة رجـوع عن بعد – فحص ملفـات الـدخول من أجل تصـحيح الأعطـال – الخ). ولا يوجد أداة منفردة تستطيع أداء وفعل كل شيء.



شكل3-7 تشغيل أداة إدارة العطل بعض الفحوصات لاختبار العتاد الفيزيقي للشبكة.

3.5 أدوات المتقدمة لإدارة الأعطال

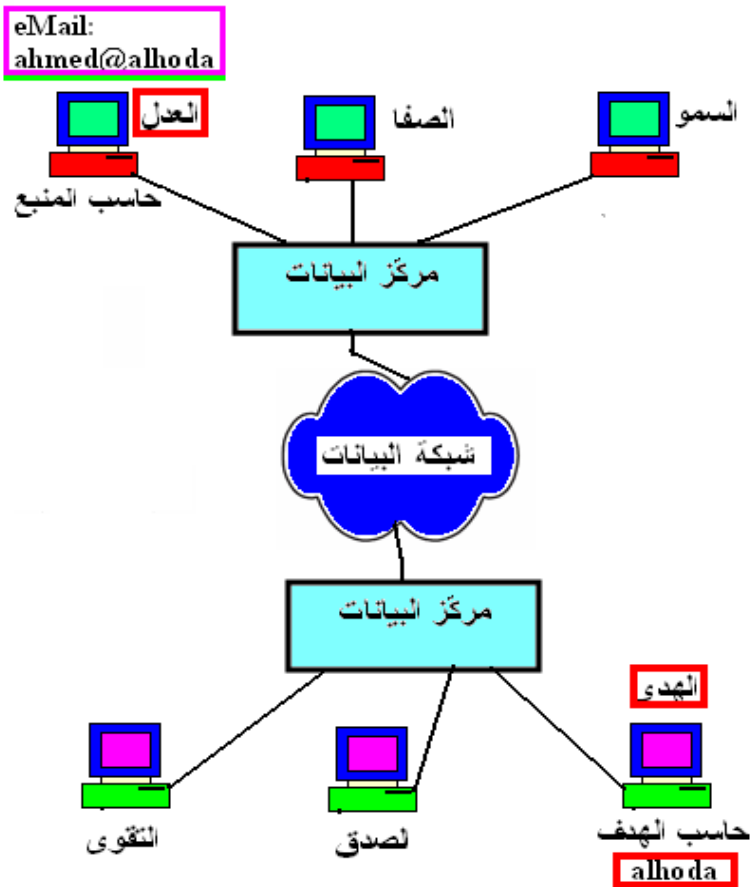
عزيزي الدارس، إن الأداة المركبة التي تم شـرحها سـابقا، تحقق إدارة الأعطـال إلى حد مـا، ولكنها لا تحقق الخطـوة الأخـيرة، وهي تصـليح المشكلة. في المثـال التـالي سنشـرح كيف تسـتطيع أداة إدارة العطل

التغلب على هـذا الضـعف في الاتصـال بين الحاسـبين المضـيفين. 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 نظامـان لا يسـتطيعان الاتصـال من خلال الشبكة. في شبكة ميجانت، الموضحة في شكل 8-3، يوجد مسـتخدم على الحاسب المسمى "العدل" هو نظام المنبع، والذي قام بمحـاولات عديـدة غـير ناجحة لإرسـال رسـالة بريد الكـتروني إلى نظـام الهـدف المسمى "الهدى". تبين أداة إدارة الأعطـال كل أجـزاء أجهـزة الشـبكة التي يمكن أن تعمـل، دون أن ترسل هـذه الأجهـزة أي أحـداث حرجـة، ولكن من الواضح أن هذا الجزء من الشبكة به تلف (معطل).

- **حل مشكلة الشبكة:**

لحل مشـكلة الشـبكة، يتم فصل الوظـائف إلى وحـدات صـغيرة يمكن تميزهـا. في هـذا الوضع يتم أولا، تحديد الأجهـزة الـتي تـوفر الوصـلة الحالية بين حاسب "العـدل" وحاسب "الهـدى". بعد ذلك نقـوم بفحص كل خطوة عبر المسـار، بداية من المنبـع. إذا وجد خطأ عند أي خطـوة، نقوم بفحص هذا الجزء بـالقرب من هـذه الوحـدة أكـثر حـتى يتم إيجـاد 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 بروتوكـول إدارة الشـبكة. وذلك لفحص كل جهاز موجود بالمسار حنى يتم الوصول للجهاز الموجود قبل حاسب "الهدى". نفترض أن كلا الحاسبين يستطيعا الاتصـال بكل جهـاز موجود على المسـار بينهمـا، ولكن لا يسـتطيعان الاتصـال مع بعضـهما. بنــاء على بروتوكــول الشــبكة المســتخدم، فــإن طريقة الفحص تتم بواسطة الاستفسار من جدول المسارات Routing Table عن كل جهاز موجـود بالمسـار، بداية من المنبع حـتى الوصـول إلى حاسب الهـدف. وبالعودة إلى المشكلة، نجد أن الأداة اكتشـفت عـدم وجـود عطل على أي من هذه الأجهزة الموجودة في المسـار. ولكن المسـتخدم مـازال لا يستطيع إرسال بريد الكتروني خلال الشبكة. عند هـذه النقطـة، سـوف

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 (Maximum Transmission Unit) MTU 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. تأث

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.

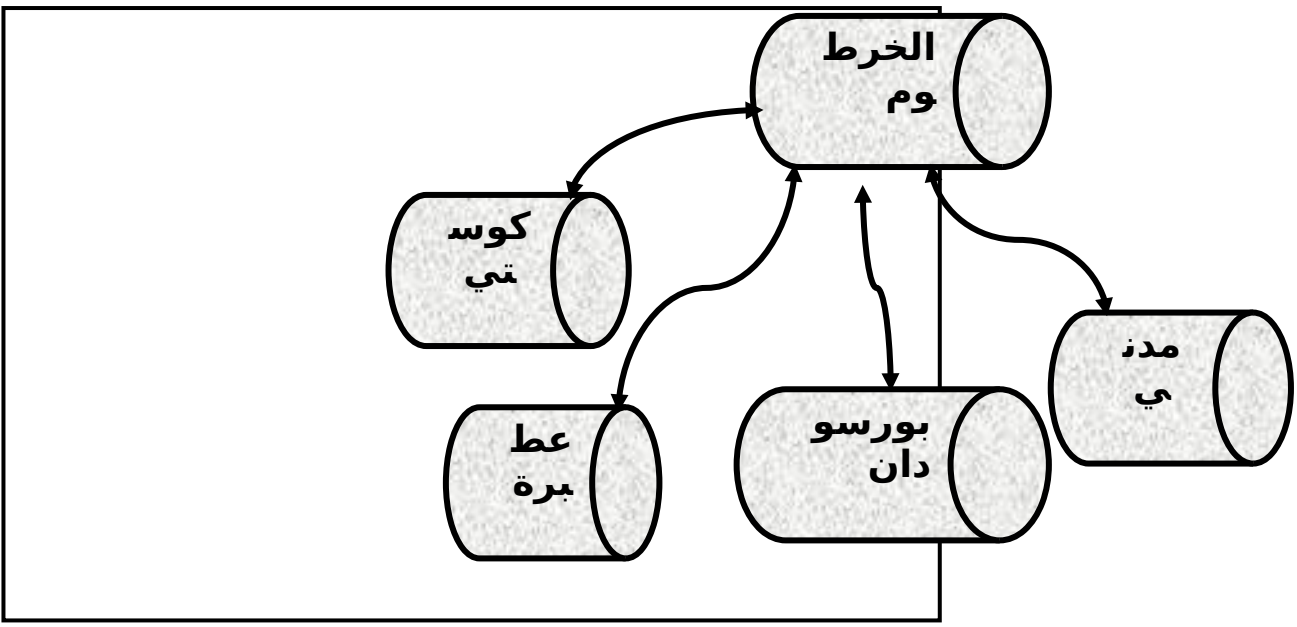
ولكن الآن، دعنا نقـول إن شـبكة بيانـات المؤسسة بها وصـلة أرضـية Terrestrial بين مصر وفرنسا بالإضـافة إلى وصـلة القمر الاصـطناعي. وأن كلا من هـاتين الوصـلتين تخـدم حركة نقل الرسـائل بين شـبكة "ديكنت" وشبكة "سـنا". والآن عنـدما تجد أداة إدارة العطل أن وصـلة القمر الاصطناعي معطلة، فإن الرسالة قد تأخذ هذا 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 بـبروتوكول الاتصـال X.25 و بها مفتـاح ضـخم في الخرطـوم يقـوم بتوصـيل المـدن مـدني، عطبرة بورسودان، كوسـتي ، سـيناء، المنصـورة مع بقية الشـبكة، 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، كوستى

في هـ ـضا
كيف يو



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

إن تصميم أداة إدارة العطل يكون لها المقدرة على تدوين هـذه الأنـواع من الأخطاء، وكـذلك تأثيراتهـا، فليس ذلك عملا مسـتحيلا. حيث سـنجد عند دراسة إدارة الأداء، أن معلومات عن نـوع البيانـات الـتي تنتقل من أجهزة الشبكة يمكن تخزينها عن طريق نظام إدارة الشبكة، لكي يمكن استعمالها من قبل أدوات إدارة الأعطال.

7. أشكال تدوين الأعطال

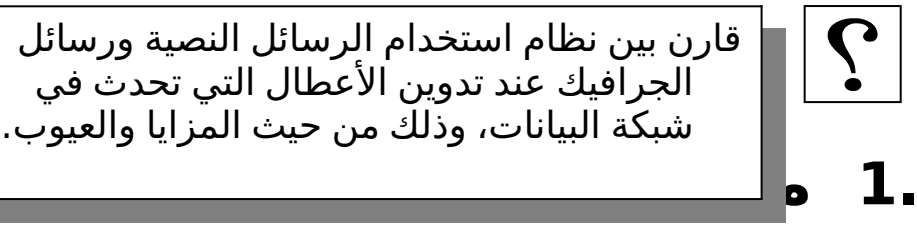
عزيزي الدارس، إن الشكل الذي تدون به الأعطال قد يكون على درجة من الأهمية بقـدر عملية إدارة الأعطـال. إن معظم أشـكال الرسـائل المألوفة قد تكـون على شـكل: رسـائل نصـية – رسـائل جرافيك – أو رسائل صوتية.

تعتبر الرسائل النصية أحد الخيارات المقبولة لأنه يصلح استعمالها في كل أنواع الطرفيات سـواء أكـانت ملونة أو غـير ملونـة. ولكن الرسـالة المصـورة تكـون أكـثر فاعلية وتـأثيراً. ولكن لإرسـال هـذا النـوع 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



1.7 ه 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 الرسـومية 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 تعـبر عن بنايـة، مدينـة، أو حـتى مـدن كثـيرة. كل مركز اتصــال من هــذه المراكز يمكن أن يــؤدي إلى خريطة أخــرى بها مراكز فرعية أصـغر، كما هو موضح في شـكل 3-10. وأخـيرا ربما من خلال خطوات متعددة، فإن كل جهاز محدد في الشـبكة يمكن إظهـاره. 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 الثانيـة، فإذا أخفقت، سوف يتم تغيير لون الجهاز إلى الأحمر. أما إذا تحول لون الجهـاز من الأخضر إلى الأحمر في كل مـرة يتم فيها إجـراء انتخـاب منفرد، ولا يوجد استجابة، فـإن هـذا يشـير إلى أن الأجهـزة تعمل وتقف عـدة مـرات. يسـتخدم اللـون الأصـفر أيضا عنـدما يوجد إمكانية إجـراء عمل نسخ احتيـاطي آلي (Automatic Backup) لبعض المكونـات الـتي 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

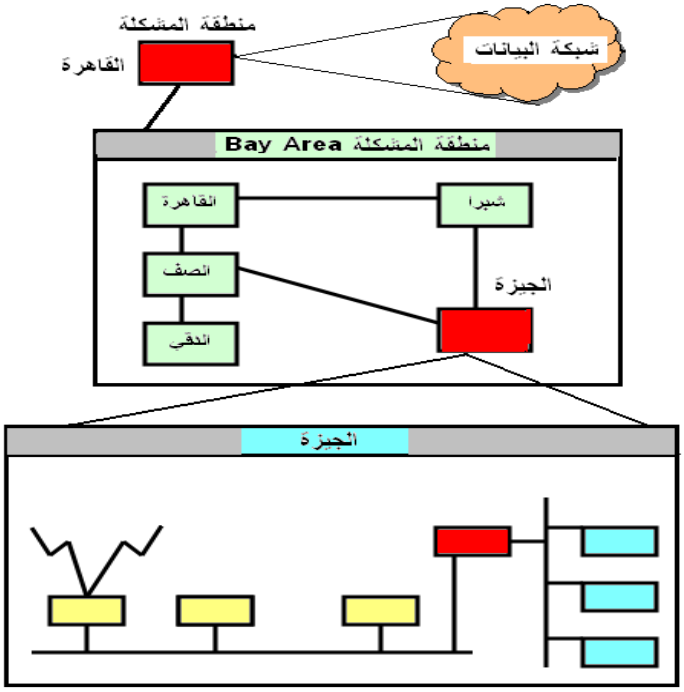
- **الاتصال الاحتياطي Dial Backup**

مثال: يوجد أجهزة عديدة مثل: المجمع – الموجهات – وصلات الشبكة ويكون لها منبع جهد كهربي احتياطي، عندما يتعطل أحدهما فإن الثـاني يعمل بـدلا منه آليـا. بالمثل يوجد في بعض الأجهـزة الأخـرى خصـائص مشابهة من مكونات العتاد، مثل: المعالجـات، ووحـدات المواجهـة. إن اللــون الأصــفر قد يعــني أن الجهــاز ليس به خطأ ولكن حالته لم تصل للحد الحرج بعد. على الرغم من أن اللـون الأصـفر قد يعـني أن الجهـاز قد قام بتصليح مشكلة الشـبكة بـدون تـدخل يـدوي. بعض الأجهـزة لها المقـدرة على إجـراء ما يسـمى بالاتصـال الاحتيـاطي "Dial Backup" لرصد وصـلة Link وإذا فشـلت، فإنها تشـغل وصـلة أخـرى بديلة آليـا. ويتطلب ذلك وجود جهاز مودم متوافق مع نظام V.24. إذا كـان الجهـاز في حالة خطأ وعاد بعد ذلك إلى حالته العاديـة، فـإن الجهـاز يتغـير لونه إلى الأزرق. ليـبين لنا أنه الآن يعمل في حالة عادية بعد أن كـان يعـاني من عطل حديث سابق.
الجهاز الذي كان لونه برتقالياً، يظهر أنه كان غـير مهيـأ، وهـذا ربما ينتج عن أن له (كلمة سر Password غير صحيحة – عنوان شبكة غـير صـحيح – عدد الوحـدات البينية غـير صـحيح – أو ما يشـابه ذلـك). كـذلك ينبغي فحص خصـائص التهيئة الخاصة لهـذه الأجهـزة البرتقالية اللـون. إذا لم يوجد أي معلومات عن أحد هذه الأجهزة، فيجب تلوينه باللون الرمـادي، لبيــان أنه ربما لم يتم إجــراء عملية التصــويت عليــه، أو ربما لم يجيب مطلقا على عملية الانتخــاب. وأخــيرا فــإن الأجهــزة الملونة بــاللون الأرجواني، تكون هي الأجهـزة الـتي تم إجـراء عمليـات الانتخـاب عليها حاليـا، ويجب على مهنـدس الشـبكة متابعتها لـيرى مـدى تقـدم عملية الانتخاب.

- **استخدام الخريطة الهرمية لعزل الأعطال**

إن الأحداث التي تؤثر على الأجهزة، يمكن أن تغير لـون مراكز الاتصـال Nodes ذات المســتويات العليا في الخريطة الهرميــة، وســوف يتم تحديــدها بواســطة نظــام إدارة الشــبكة. من الناحية العمليــة، فــإن

المستويات الفوقية المباشرة للأجهزة التي تم إظهارها، سوف يتم تغير لونها تبعا لاستجابة الأحداث الحرجة بالشبكة.



شكل10-3 استخدام الخريطة الهرمية لعزل الأعطال.

لبيـان كيفية عمل الخريطة الهرمية مع تخصـيص الألـوان، يتم تلـوين صورة شبكة البيانات بكاملها مثل سحابة (a Cloud). يعبر لون السحابة الخضراء على أنه لم تقع أي أحداث حرجة داخل الشبكة. إذا تغـير لـون السـحابة إلى الأحمـر، فـإن هـذا يجعل مهنـدس الشـبكة يقـوم بفحص الوحـدة البينية الرسـومية الهرمية لإيجـاد الجهـاز المعطـل. ربما تنتشر السحابة إلى خريطة العـالم الـتي يوجد بها مدينة واحـدة محـددة قد تم تلوينها باللون الأحمر. يمكن الوصول بعد ذلك إلى تبولوجي شبكة هــذه المدينة، والوصول إلى الجهاز ذي اللون الأحمر. ثم يتم تدوين التفاصيل إلى مهندس الشبكة لبيان الخطوات التي قد قـام النظـام باتخاذها فعلا لتصـــــــــــــــــــــــــــليح الخطـــــــــــــــــــــــــــأ.

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 هـذه الوحـدة فوائد عملية إدارة الأعطـال، و الخطـوات الثلاثة المتعلقة بإتمام صيانة الأعطال في شـبكة البيانـات. ووقفنا على ثلاثة احتمالات ممكنة للأدوات الـتي يمكن اسـتخدامها. و بعض الطـرق 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 توك 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
Automatic Backup	نسخ احتياطي آلي
Buffer Storage	مخزن مؤقت
Burst of Traffic	حركة مرور بيانات زائدة
Carrier Signal	إشارة حمل

المصطلح بالإنجليزية	معناه بالعربية
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
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	بروتوكـــول نقل البريد البسيط

المصطلح بالإنجليزية	معناه بالعربية
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



محتويات الوحدة

الموضوع	رقم الصفحة
مقدمة	**117**
تمهيد	**117**
أهداف الوحدة	**118**
1. فوائد إدارة التهيئة	**119**
2. تحقيق عملية إدارة التهيئة	**121**
1.2 تجميع البيانات يدوياً	122
2.2 الاستكشاف الآلي لأجهزة الشبكة	123
3.2 رسام الخرائط الآلي	124
3. تعديل وتخزين معلومات التهيئة	126
4.تخزين معلومات تهيئة الشبكة	**126**
5. إدارة التهيئة في نظام إدارة الشبكة	130
1.5 الأداة البسيطة والمركبة والمتقدمة لإدارة التهيئة	130
6. توليد تقارير إدارة التهيئة	**143**
الخلاصة	**146**
لمحة مسبقة عن الوحدة التالية	146
مسرد المصطلحات	**147**
المراجع	**150**

مقدمة

تمهيد

عزيزي الدارس، مرحبا بك إلى هذه الوحدة التي تتناول إدارة التهيئة بالحصول على البيانات من الشبكة، واستخدام هـذه البيانـات في إدارة وتنصـيب كل أجهـزة الشـبكة. سـنتناول تجميع معلومـات عن التهيئة الحالية للشبكة، واستخدام هذه البيانات في عملية تعـديل تهيئة أجهـزة الشبكة، وتخزين البيانات، والاحتفاظ بقائمة حديثة، وتدوين تقارير مبنية على البيانات. في هذه الوحدة الدراسية سوف نشرح أيضاً فوائد إدارة

التهيئة بالنسبة لمهنـدس الشـبكة. ونناقش الخطـوات اللازمة لإدارة عملية التهيئـة. ونشـرح ثلاثة مسـتويات من أدوات إدارة التهيئـة. 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 قـدرة مهنـدس الشـبكة على التحكم في تهيئة أجهزة الشبكة، وذلك بأن تمكنه من الوصول السريع إلى بيانـات 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:**

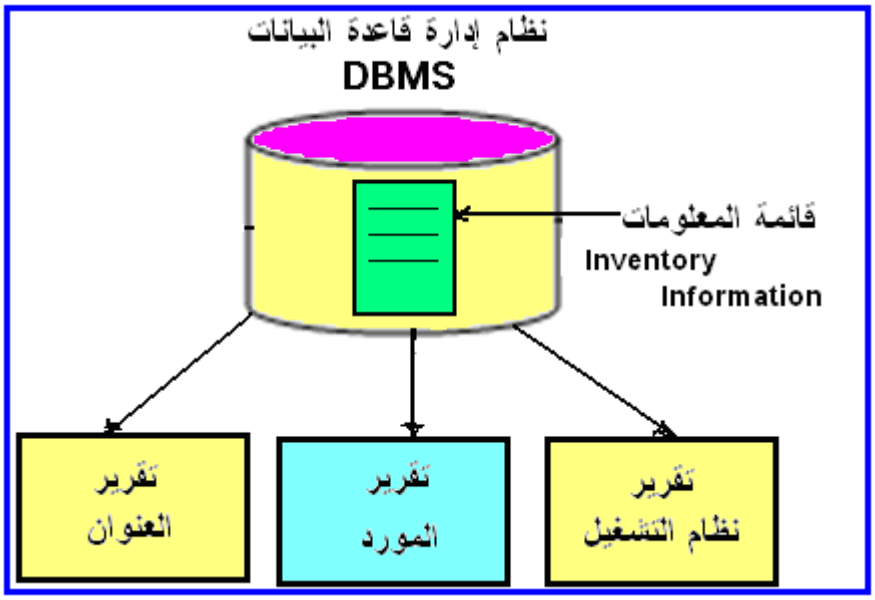
على سبيل المثال، يعتبر التنصيب الحالي لكل جهاز من أجهزة الشبكة، هو أحد مظاهر بيان التهيئة. دعنا نفترض أنه توجد وحدات بينية إضافية لجهاز معين ونريد أن نعرف أولاً، عدد الوحدات البينية الفعلية الموجودة في الجهاز، وكذلك عناوين الشبكة المخصصة لهذه الوحدات، وذلك للمساعدة في تهيئة البرامج الموجودة بالجهاز. 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 بالشـبكة: إن الفشل في هذه الخطوة يمكن أن يـؤدي إلى ضـياع وقت مهنـدس الشـبكة في حصر مشاكل الشبكة التي سـببتها أخطـاء تهيئة بسـيطة. ويمكن تجميع هذه المعلومات، إما يدويا بواسطة مهندس الشـبكة أو بواسـطة نظـام إدارة الشبكة.

2- استخدام هذه البيانات لتعـديل تهيئة أجهـزة الشـبكة. بما أن الوسط المحيط بشـبكة البيانـات يتغـير باسـتمرار، فـإن قابلية تعـديل 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- تخـزين البيانـات، والاحتفـاظ بقائمة بيانـات حديثة لكل مكونـات الشبكة، وتوليد تقارير مختلفة.

1.2 تجميع البيانات يدويا

يتم غالبا الحصـول على المعلومـات من الشـبكة بمجهـود يـدوي. حيث يمكن لمهنـدس الشـبكة الـدخول إلى الشـبكة عن بعد ، للوصـول إلى معرفة الأجهـزة المتصـلة بالشـبكة، ثم يتم بعد ذلك تسـجيل الـرقم التسلسـلي للأجهـزة، والعنـوان المخصص للجهـاز في ملف مفكـرة، أو ملف مكتوب بشفرة أسكي، أو ملف جدول قاعدة بيانات. وعلى الرغم من أن عملية التسجيل اليدوي للمعلومـات سـوف يـؤدي إلى الحصـول على النتائج المطلوبة، لكن استخدام هذه الطريقة للاحتفـاظ بسـجلات حديثة عن كل تغيير يحدث في الوسط المحيط بشـبكة البيانـات، 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 قـدرة تحكم مهنـدس الشـبكة على تهيئة أجهـزة الشبكة.

ب- .....

ج- .....

2) اذكر بعض عيـوب طريقة التجميع اليـدوي لبيانـات في نظـام إدارة تهيئة أجهـزة الشـبكة؟ 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

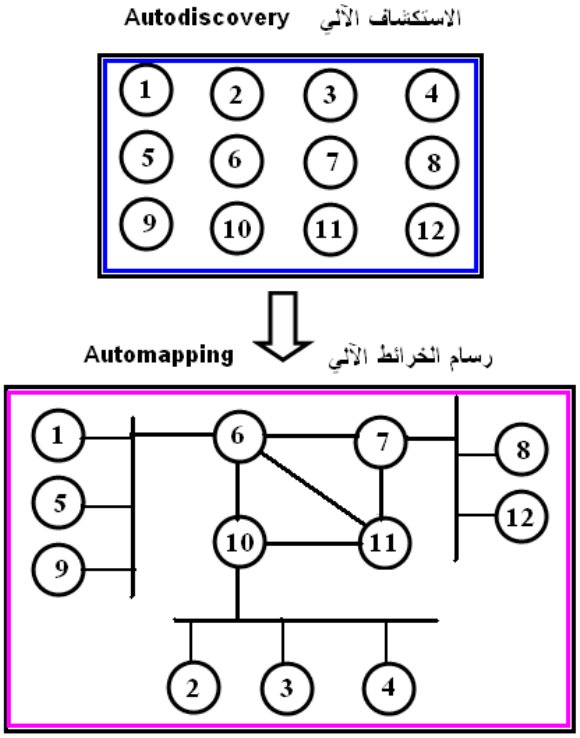
يوجد وسيلة أخرى يمكن استخدامها وهي الاستكشاف الآلي Auto-discovery، والتي تمكننا من الحصول على قائمة البيانات الحالية لجميع أجهزة الشبكة. ويوجد طريقتان شائعتان تستخدمان لتنفيذ عملية الاستكشاف الآلي:
الطريقة الأولى: هي أن يتم إرسال رسالة استفسار Query، وذلك باستخدام أمر الصدى "بنج" ICMP Echo(ping) ، إلى 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

عنـدما يتم الحصـول على معلومـات إدارة الشـبكة، سـوف نحتـاج إلى إجـراء عملية تحـديث. نفـترض شـبكة بيانـات بها 6000 مركز اتصـال، الـتي تم مناقشـتها سـابقا. فـإذا احتـاج 1% فقط من مراكز الاتصـال تخصيص عنوان، أو تغير كل أسبوع، فسوف نحتاج إلى إجراء 60 تعديل في الأسـبوع. وأكـثر من ذلـك، فـإن عنـاوين الشـبكة تكـون واحـداً من العديد من بيانات تهيئة الشبكة. إن أي جهاز منفرد سوف يتطلب الكثير من التعـديلات الـتي سـوف تتم في المعـاملات الخاصة به والـتي ينبغي تتبعها أثناء عملية التهيئة.

من الواضح أن عملية تجميع البيانات وتعديلها يدويا ، تكـون طريقة غـير فعالـة، إذا لم يقـوم مهنـدس الشـبكة الـذي أدى عمليـات التهيئة يـدويا بتسجيل الخطوات، وأن سجل تغيرات التهيئة ربما لم يتم حفظه. يمكن أن يؤدي ذلك إلى حدوث إرباك، خاصة عندما يقم مهندس آخر للشـبكة بفحص الجهاز الذي تم تغيير تهيئته ولم يجد سجل حفظ التهيئة السابق. على النقيض من ذلك، إذا سمحت إدارة التهيئة في نظام إدارة الشـبكة بإجراء تغيرات تهيئة الجهاز فإن هـذه التغـيرات يمكن تسـجيلها قبل أن يتم إرسالها إلى الجهاز. كميزة إضـافية، فـإن نظـام إدارة الشـبكة ربما يكون قادرا على التحقق من أن تغييرات التهيئة كـانت مناسـبة للجهـاز، ويقوم بتنبيه مهنـدس الشـبكة قبل أن يقـوم بـإجراء تهيئة غـير مناسـبة للجهاز بدون قصد.

4.تخزين معلومات تهيئة الشبكة

ينبغي على إدارة التهيئة توفـير وسـيلة لتخـزين المعلومـات. إن نظـام الإدارة الفعال هو الذي يسـتطيع تخـزين كافة تهيئة شـبكة البيانـات في مكان مركزي. وهذا يجعل بيانـات التهيئة متاحة بشـكل سـريع وفعـال ، يمكن الوصول إليها بسهولة بواسطة مهندس الشـبكة. يمكن أن يكـون مكان التخزين المركزي لبيانات التهيئة عبارة عن ملف مفكرة، أو ملف مكتـوب بشـفرة أسـكي ، أو جـدول في مركز تحكم الشـبكة. وبغض النظر عن الطريقة المستخدمة، فإن وجود هـذه البيانـات بشـكل متـاح ومنسق سوف يكون ذو فائدة كبيرة لمهندس الشبكة.

1.4 ملفات شفرة أسكي

إن اسـتخدام ملف مكتـوب بشـفرة أسـكي هو أحد وسـائط التخـزين الشائعة، وله ثلاثة **مميزات هي:**

- أن شفرة أسكي سهلة القراءة.
- يسهل الوصول إليها من أماكن بعيدة.

- ولها هيكل ملف يكون عادة سهل الإدارة والفهم.

ولهـــذا، فـــإن معظم الـــبرامج التطبيقية (بغض النظر عن العتـــاد المستخدم) تستطيع قراءة ملفات أسكي.

من عيوب استخدام شفرة أسكي:

- أن حروف شفرة أسـكي تسـتخدم ذاكـرة تشـغل حـيز كبـير في نظام الكمبيوتر.
- وأن كمية كبـيرة من البيانـات المخزنة بهـذه الشـفرة يمكن أن يستهلك مساحة ضخمة من حيز قرص التخزين.
- علاوة على أن هياكل ملفات أسكي غير المعقدة يمكن أن يـؤدي إلى بطء عملية الوصول للبيانات، أثناء عملية البحث.
- ولكن العيب الأكثر أهمية في ملفـات أسـكي هو أنها لا تسـتطيع 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 د البيـ

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.

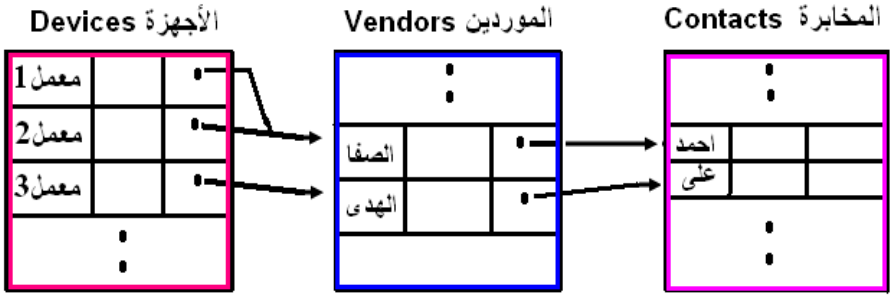
مثال: نظام قاعدة بيانات علاقية لإيجاد علاقات بين بيانات الشبكة:

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 قاصـرا على أجهـزة الشـبكة، إذ إنه يمكن أن يشمل جميع المعلومات الضـرورية لإدارة التهيئـة. وبـذلك فإن استخدام قاعـدة البيانـات في التخـزين، يمكن أن يسـاعد مهنـدس الشبكة في جميع النـواحي المتعلقة بعملية إدارة التهيئـة. ونلاحظ على الرغم من ذلك **أن نظام إدارة قاعدة البيانات لها بعض العيـوب 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 صـعوبة في عملية نقل ملفـات البيانـات المخزنة بنظـام قاعـدة البيانـات إلى نظـام آخـر. ولكن معظم مـوردي نظم قواعد البيانـات قد قاموا بحل هذه المشكلة بواسطة السـماح بوضع البيانـات المخزنة في قاعدة البيانات على شـكل شـفرة أسـكي، وبـذلك يمكن بسـهولة نقلها واستخدامها. وبذلك فـإن المميـزات الـتي توفرها نظم قواعد البيانـات تعوض بشكل جيد عن عيوبها.

5. إدارة التهيئة في نظــام إدارة الشبكة

عزيـزي الـدارس، إن أدوات إدارة التهيئة يمكنها زيـادة إنتاجية مهنـدس الشبكة بواسـطة تجميع وتحـديث بيانـات أجهـزة الشـبكة آليـا، وتوفـير مخـزن مركـزي لبيانـات التهيئـة، وتمكين إجـراء التعـديلات في بيانـات الشبكة، وتوفير قائمة بيانات، وتوليد التقـارير. إن الأداة الـتي تسـتطيع تقديم هذه التسهيلات سوف يحـدد مـدى سـهولة وصـعوبة هـذه 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 جهـاز مثـل: اسم الجهاز – عنوان الشبكة – أو عدد الوحدات البينيـة. بـالرغم من أن هـذه المعلومات تكون مفيدة، لكن هذا يضعف من وظائفهـا، ويعـني هـذا أنه يجب على مهنــدس الشــبكة الاستفســار عن كل جهــاز بطريقة يدوية وتجميع المعلومات الإضافية اللازمة لإدارة التهيئة.

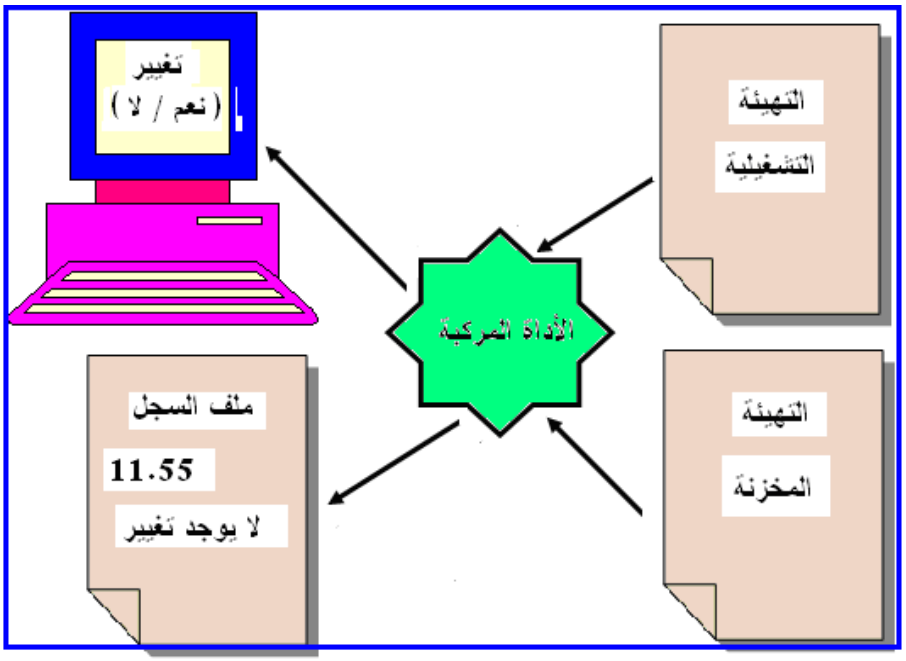
2.5**الأداة المركبة لإدارة التهيئة:**

يمكن تطـــوير أداة مركبة تســـتطيع مقارنة تهيئة الأجهـــزة الحالية مع التهيئة المخزنة في قاعـدة بيانـات النظـام. كما تسـتطيع أن تمكننا من رؤية التهيئة الجغرافية المنصبة، وإجراء عمليات تغيـير التهيئـة. وأخـيرا مثل الأداة البسـيطة، فـإن إصـدار الأداة المركبة يجب أن يـوفر مخزنـاً مركزياً ووسيلة سهلة لاسترجاع البيانات.

وكما هو مبين في شـكل4.3 ، فـإن الأداة ينبغي أن تمكننا من **إجراء عملية المقارنة بين التهيئة التشغيلية مع التهيئة المخزنة** في قاعدة بيانات النظـام. بالإضـافة إلى أنه ينبغي للأداة إما أن تبـدأ عملية تشغيل التهيئة التي تمكنا من تغيير التهيئة أو أن تحقق هي عملية تغيـير التهيئة بنفسها آليا. أثناء إجراء حـوار مشـترك بين الأداة والجهـاز، فـإن الأداة ســوف تتحسس الجهــاز لمعرفة التشــغيل الحــالي وبعد أن تتم عملية مقارنته مع التهيئة المخزنــة. إذا وجد أي اختلافــات، فــإن الأداة تقوم بالسؤال عن ما إذا كنا نريد تغيير تهيئة الجهاز ليتوافق مع الإصـدار المخزن. ربما يتم تشغيل هذه الخاصـية آليا (دون إجـراء تغـيرات) على فـترات، ويمكن إرسـال بريد إلكـتروني إلى مهنـدس الشـبكة لإحاطته علما عن أي اختلافات تم إيجادها.

نلاحظ أن جميع تفاصيل التهيئة تكون على درجة متسـاوية من الأهميـة. من أجل العمل الجيد في الوسط المحيط المتنـوع في شـبكة البيانـات، ينبغي على الأداة أن تحتــوي على **وســائل لتحديد نــوع أخطــاء التهيئة**، وأن تقوم بتوليد رسائل تحذير وتعـرض إنـذارات. على سـبيل المثال: نفترض أن أحد اختيارات التهيئة في جهاز خـادم الطرفيـات هي تهيئة معدل إرسال المعلومة Bit Rate لوصـلة القـدوم، وهـذه التهيئة تكــون مفيــدة في إجــراء الاتصــالات في نفس الــوقت مع العديد من الأجهـزة عند معـدلات معلومة مختلـف. نفـترض أن معلومـات التهيئة المخزنــة، أوضــحت أن كل خط غـير مـتزامن خـارج من جهـاز خـادم الطرفيــات تم ضــبطه عند معــدل معلومة 9600 بــايت /ثانيــة. ولكن عنــدما تقــوم الأداة باستفسـار الجهـاز وجـدت أن أحد الخطـوط كـان مضبوط عند 2400 بيت/ثانية، في هـذه اللحظة ، فـإن الأداة ربما تهتم بالتهيئة، ولكنها ببساطة سوف تصـدر رسـالة تحـذير إلى ملف السـجل

Log File. وعلى النقيض، إذا وجدت الأداة خط آمن Secure Line متصل بخادم الطرفيات بدون وجود كلمة سر لـه، فسـوف تقـوم الأداة بالتنبيه عن هذه الحالة بواسطة عرض إنذار.

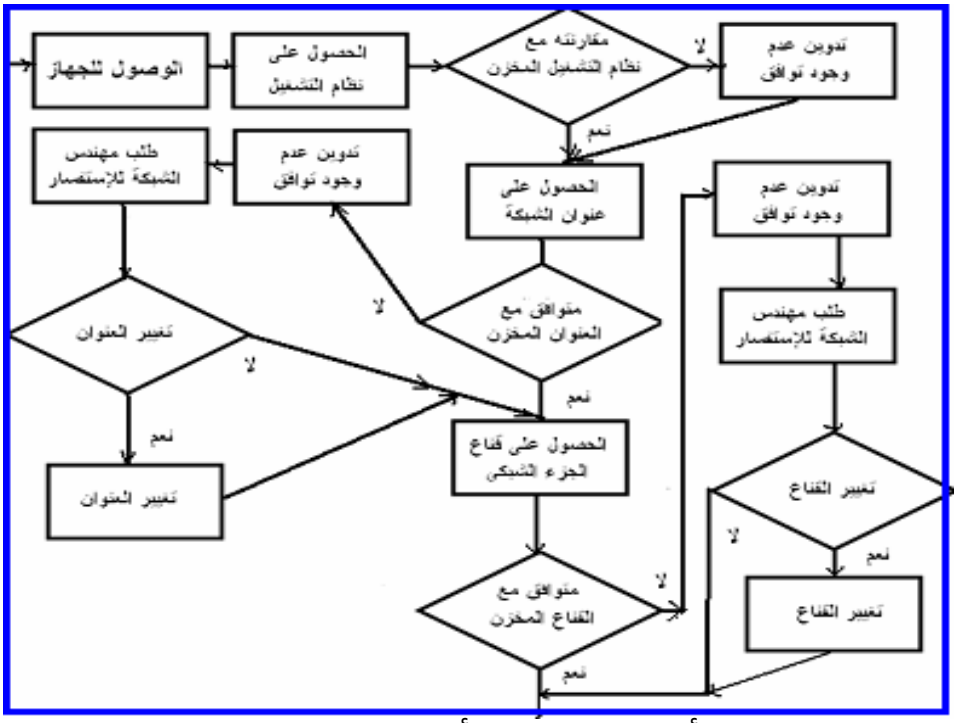


شكل4.3 استخدام الأداة المركبة لمقارنة التهيئة التشغيلية مع التهيئة المخزنة،

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 عنـوان 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 (Fiber Distributed Data Interface) FDDI .

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 الموجـودة في الشـبكة المحلية االتخيليـة: ربما تكـون متصلة بجهاز التوصـيل في مبـنى واحـد، بينما أجهـزة أخـرى نريـدها أن تكون في نفس الشبكة المحلية التخيلي، ربما تكون متصـلة بجهـاز آخر في مبنى مختلـف. إن الأداة المركبة تسـمح لنا بـأن نبـدأ تهيئة الشـبكة المحلية التخيلية، وذلك بأن يتم أولا تحديد المنافذ ذات الصلة بالمشـاهد الفعلية أو المنطقية لكل الأجهــزة المتــأثرة. بعد ذلك يتم إخبــار الأداة المركبة لكي تجعل كل منفذ من هـــذه المنافذ بـــأن ينتمي إلى نفس الشبكة المحلية التصـورية (ربما بواسـطة إسـقاط المنافذ المعـبر عنها بالرســومات إلى أيقونة الشــبكة المحلية التصــورية). تســتطيع الأداة المركبة بعد ذلك تهيئة كلا من الأجهزة المتأثرة والمنافذ.

- **برمجيات الأداة المركبة:**

بعض تطبيقـات إدارة الشـبكات المتـوفرة في الأسـواق تقـوم بتوفـير معظم الوظائف الـتي تم وصـفها بخصـوص الأداة المركبـة. ويوجد عند بعض المــوردين أداة تســتطيع فحص التهيئة الحالية للجهــاز، ومقارنتها بالتهيئة المخزنة في قاعدة البيانات. أيضا يوجد بعض المـوردين، لـديهم بعض التطبيقــات الــتي تظهر رســومات تهيئة الأجهــزة الخاصة بهــذه التطبيقـات. تكـون هـذه المواصـفات غالبا محـددة من قبل المـوردين، ويكون لها وحدات مواجهة بينية للمستخدم مختلفة حسب كل جهاز يتم توريده. ويعـنى هـذا أن مهنـدس الشـبكة يحتـاج أن يتعلم كيفية تحقيق هذه الوظائف على أسـاس المعلومـات المتـوفرة من المـورد، وكـذلك باستخدام برنامج إدارة الشبكة المناسب.

3.5 الأداة المتقدمة لإدارة التهيئة

بينما الأداة المركبة كما تم شرحه في الفقـرات السـابقة تسـمح بتغيـير التهيئة التشغيلية للجهاز، فإن الأداة المتقدمة سوف تكـون أكـثر فاعلية إذا اســتخدمت نظــام إدارة قاعــدة البيانــات في تخــزين البيانــات والاستفسارات ذات الصلة، و تسـجيل قـوائم معلومـات إدارة الشـبكة. وتكــون قــادرة على تقــييم تهيئة الجهــاز، كي تــؤدي عملها في صــورة مثالية.

إن قدرة الأداة على إيجـاد علاقة بين مجموعـات متعـددة من البيانـات يكــون مهما في إدارة التهيئــة. على ســبيل المثــال، إذا كــان أحد المهندسين في الشبكة مسئولا عن 150 جهـازاً، فـإن إسـناد اسم هـذا المهندس إلى كل هذه الأجهزة مرة واحدة، سـيكون أسـهل من إدخـال وتخزين نفس الاسم في كل مرة لكل جهاز على حدة.

أسئلة تقويم ذاتي

؟

1) أذكر ممــيزات وعيــوب طريقة تخــزين بيانــات 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 البياناتDBMS (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 هـذا الأمـر، كل أجهـزة الجسـور 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
البيانات، وهذه التقارير قد تحتوي على البيانات التالية:

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

ها
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 الوظـائف إلى المسـتخدمين. وهـذا ربما يعـبر عن وجـود فـائض Redundancy ، أو ربما يعبر عن وجود مشـكلة في إدارة التهيئة تحتـاج معالجة.

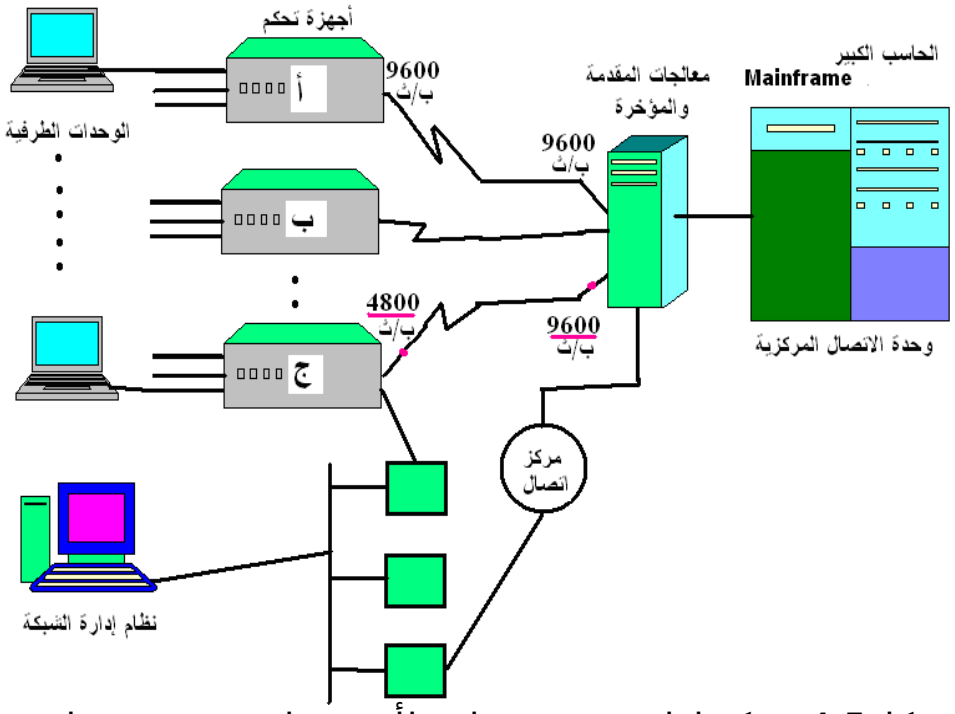
تسـتطيع الأداة المسـتخدمة **تقييم تهيئة الشـبكة لتحديد قـدرتها الاتصالية**. على سبيل المثال، نفترض أن الشبكة الموضحة في شكل 4.5 ، تحتوى شبكة إقليمية WAN ، تتكون من أجهزة تحكم وحاسبات مقدمة ومؤخرة Front–End Hosts. والمطلوب تهيئة وحداتها البينية كي تقوم بإجراء عمليـات الاتصـال عند سـرعات مناسـبة. نفـترض أن زمن الاسـتجابة من الوحـدات الطرفية لأحد أجهـزة التحكم أبطأ من زمن الاستجابة الناتج من الوحدات الطرفية لأجهزة التحكم الأخـرى. لتقـييم هذه الحالة عند بـدء التشـغيل، فـإن أداة إدارة التهيئة سـوف تـدرك أن سرعة إرسال مجموعة أجهزة التحكم قد تم ضـبطها عند القيمة 4800 بايت/ثانية، وأن سرعة حاسبات أجهزة المقدمة والمؤخرة عند الجـانب الآخر قد تم ضبط سرعة الاسـتقبال بها بحد أقصى 9600 بـايت/ثانيـة. وهـذا ينتج عنه أن تصـبح السـرعة القصـوى تكـون 4800 بـايت/ثانيـة. وعلى النقيض من ذلك، فإن مجموعة أجهـزة التحكم الأخـرى في نفس الجانب والمتصلة بنفس حاسبات المقدمة والمؤخرة كـان قد تم ضـبط سرعتها لتعمل عند 9600 بايت/ثانية في كلا الجـانبين. سـوف تسـتنتج الأداة أن هذا الاختلاف في معدلات سرعة أجهزة التحكم هو الذي سبب بطء زمن الاستجابة. وكخطوة أخـيرة في عملية التقـييم، سـوف تقـوم الأداة باستخدام قاعدة البيانات العلائقية لتحديد سـرعة وصـلة الشـبكة الإقليمية WAN. وبـذلك فـإن الأداة تكـون قد وجـدت مشـكلة تهيئة الشبكة آليا بواسطة تقييم معلومات إدارة التهيئة.

تعتمد الأداة المتقدمة على مجموعة الخصائص الوظيفية التي تقـوم بها على وجود نظام إدارة قواعد البيانـات. إن الأدوات المتقدمة المتـوفرة في الأسـواق، تقـوم بتخـزين المعلومـات في قواعد بيانـات أيضـا، كما تساعد في بناء استفسارات باستخدام لغة "SQL".

معدل سرعة الإرسال والاستقبال، يتم كشفه بواسطة الأداة المتقدمة لإدارة الشبكة.

ويوجد بعض المنتجـات تـوفر لمهنـدس الشـبكة إمكانية توليد تقـارير متنوعة عن أجهزة الشـبكة وأسـماء المـوردين. وبعضـها يـوفر وسـائل لتوليد تقارير يمكن للمستخدم أن ينشئها بحسب احتياجاته. أما خاصـية تقـييم إدارة تهيئة الشـبكة، فيمكن أن تتم من خلال بنـاء أداة تسـتطيع

تقييم تهيئة الشبكة بشكل إجمالي. حيث أن المتوفر حاليا في الأسـواق أن كل مـورد ينتج برمجيـات تختص بإيجـاد أو وصف تهيئة أجهـزة معينة خاصة بمنتجاتهم.



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

6. توليد تقارير التهيئة

عزيـزي الـدارس، كما شـرحنا في الفقـرات السـابقة، أنه ينبغي على الأداة المتقدمة لإدارة التهيئة أن تقـوم بتوليد التقـارير اللازمـة، الـتي تمكن مهنـدس الشـبكة من معرفة التطـورات الجديـدة حـول التهيئة الإجمالية للشبكة.

على الـرغم من أن هـذا النـوع من الأداة غـير مطلـوب أن يرحل المعلومـات بسـرعة -مثل أداة إدارة الأعطـال- فإنه في أحيـان كثـيرة يكون عرض هذه التقارير ضروريا، وخاصة عندما تجد الأداة تكـراراً في العنـوان أو تكـراراً في أسـماء أجهـزة الشـبكة. على عكس أداة إدارة

الأعطـــال، فـــإن أداة إدارة التهيئة لا تعتمد على اســـتخدام الألـــوان أو وحدات بينية رسومية لكي تعمل بشكل متكامل. فإذا استطاع مهنـدس الشـبكة الـدخول إلى البيانـات من خلال وحـدة طرفية تعمل بشـفرة أسكي، فإن كل التسهيلات المتعلقة بإدارة تهيئة الشـبكة سـوف تكـون متاحة أمامه. بالطبع، كلما كانت الأداة سهلة جعل ذلك مهندس الشبكة يستطيع توليد التقارير الضرورية بسهولة.

يمكن أن يحتـــوي التقرير على تفاصـــيل عن التهيئة الإجمالية لأجهـــزة الشـبكة، وقـدراتها ويشـمل ذلـك: أسـماء الأجهـزة، وعنـاوين الشـبكة، والأرقام المسلسلة، أسماء الموردين ونظام التشـغيل، الاسم المحلي للشخص المسئول عن الشبكة. إذا كـان الجهـاز موصل بوصـلة تـوالى، فإن التقرير يمكن أن يشـمل أيضـا، أرقـام الـدوائر، وهي تكـون مفيـدة عندما يتم كتابة تقرير عن أعطال الوصلة، خاصة عندما يتم إرساله إلى مورد الدوائر. يوجد بعض البيانات الإضافية الاختيارية الأخرى، يمكن أن تحتـوي على اسم الشـخص المسـئول في الشـركة المـوردة للأجهـزة للاتصـــال به عند الحاجـــة، والمكـــان الفعلي لوجـــود الجهـــاز. وهـــذه المعلومات تمثل الحد الأدنى الذي يمكن أن يعبر عن أجهزة الشبكة.

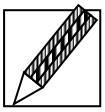
إن معدل التكرار الذي يتم عنده توليد هذا التقرير يتغير حسب حالة كل شبكة. يمكن على سبيل المثال، أن يتم توليد هـذا التقرير أسـبوعيا، إذا كانت الشبكة تتغير بمعدل سريع، أو شهريا إذا كانت الشبكة مستقرة.

يمكن الاستعانة بهذا التقرير في تشـغيل الشـبكة الحاليـة، وربما نحتـاج بعد ذلك إلى ملخص بكل التعديلات المطلوبة لتحديث الشـبكة. إن هـذا التقرير يحتوي على قائمة التغيرات المطلوبة للشبكة، مصنفة ومـذكور بها اسم الشخص الذي يطلب التغيير، والمكـان الـذي سـوف يحـدث به التعديل. يمكن أن يشـمل المصـنف على الأجهـزة الجديـدة المطلوبـة، والعتاد المطلوب تغييره، والبرمجيات والإدارات. إن تقسيم المعلومات المـــذكورة في التقرير إلى مصـــنفات يجعلنا نحصل على المعلومـــات المهمة بسرعة.

إن معدل إنشاء هذا التقرير يتغير حسب معـدل التغـيرات الـتي تحـدث بالشبكة. وأخيرا فإنه على أداة إدارة التهيئة إنشاء تقرير ملخص بقائمة البيانات الإجمالية للشبكة. وهذا التقرير يتم الاحتفـاظ به لبيـان الجهـود اللازمة لأي شـــبكة بيانـــات، وينبغي أن يركز التقرير فقط على أجهـــزة الشبكة. ويتضمن هذا التقرير: كل جهاز يتم شراؤه، الرقم المسلســـل، والمكان الفعلي، وتاريخ وضع الجهاز في الخدمة، ومدة ونـوع الضـمان، وتاريخ شامل وحديث . وبناء على الوسط المحيط للشبكة، فإن إضـافة

معلومـات عن كل جهـاز يكـون مطلوبـا. بسـبب أن ذلك عـادة يكـون ضروريا . ويمكن إنشاء هذا التقرير بشكل دائم شهريا.

تدريب (1)



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

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

ب- تتعـــاون إدارة التهيئة في إجـــراء تعـــديلات تهيئة الأجهزة.

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

د- يتمـيز ملف التهيئة المخـزن في نظـام إدارة قاعـدة 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- تســتطيع الأداة البســيطة لإدارة التهيئة عمل مقارنة بين التهيئة التشغيلية والتهيئة المخزنة.

ز- تســتطيع الأداة المتقدمة لإدارة التهيئة تقـــييم تهيئة أجهزة الشبكة كي تؤدي عملها بصورة مثالية.

ح) تسـتخدم لغة SQL للاستفسـار عن أجـزاء معينة في قاعدة البيانات الخاصة بتهيئة أجهزة الشبكة.

ط) يمكن أن تسـاعد إدارة التهيئة مهنـدس الشـبكة في تحديد قطع غيار أجهزة الشبكة.

ك) يستخدم رسام الخرائط الآلي لإيجاد أجهـزة الشـبكة 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 ايضاً 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 بـالمورد على: الاسم - العنـوان – رقم الهاتف. وقد تشمل قائمة بيانات الدوائر المؤجرة علي: رقم الـدائرة – السـرعة – اسم المـورد – عـدد نقـاط النهايـات بالشـبكة – المـدة المسموحه و المدة التي سوف تتوقف عندها الخدمة.

ملف السجل Log File.

وعلى النقيض، إذا وجـدت الأداة خط آمن Secure Line متصل بخـادم الطرفيـات بـدون وجـود كلمة سر لـه، فسـوف تقـوم 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

المصطلح بالإنجليزية	معناه بالعربية
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"ـ
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
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.



محتويات الوحدة

الموضوع	رقم الصفحة
المقدمة	**153**
التمهيد	**153**
أهداف الوحدة	**154**
1. فوائد إدارة أمن شبكة البيانات	**155**
2. تحقيق إدارة أمن الشبكة	**156**
1.2 تحديد المعلومات الحساسة	**160**
2.2 إيجاد نقاط الاتصال وتأمينها والحفاظ عليها	161
3.2 تأمين نقاط الوصول	**169**
4.2 الحفاظ على نقاط الاتصال	**184**
3. الاتصال بالشبكة العامة	**186**
4. تحقيق نظـــام الأمن في نظـــام إدارة الشبكة	**190**
5. تدوين حوادث الأمن في الشبكة	**196**
6. برامج تطبيقية لأمن الشبكة	**200**
الخلاصة	**203**
لمحة مسبقة عن الوحدة التالية	**203**
مسرد المصطلحات	**204**
المراجع	**208**

مقدمة

تمهيد

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

تحتوي هذه الوحدة على **أربعة أقسام** رئيسة، تتنـاول أهم المفـاهيم التاسيســـية في إدارة الأمن تبـــدأ **بتعريف فوائد إدارة الامن.** ثم اختصاصـات إدارة الأمن الأربعة وهي: تحديد المعلومـات الحساسة من أجل حمايتها، و إيجاد نقاط الاتصال، والعمل على تأمين نقاط الاتصال، ثم الحفاظ على نقاط الاتصال.
وفي القسم الثـاني تنتنـاول ادوات إدارة الأمن من خلال التعـرف على أمن الحاسب وأمن المستخدم ثم أمن المفتاح السري .
. وأخيراً نناقش في هذه الوحدة ممـيزات سـجلات الفحص الـتي يمكن الحصول عليها من تقارير حوادث الأمن.
أهلا بك مرة أخرى إلى هذه الوحـدة، عسـى 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

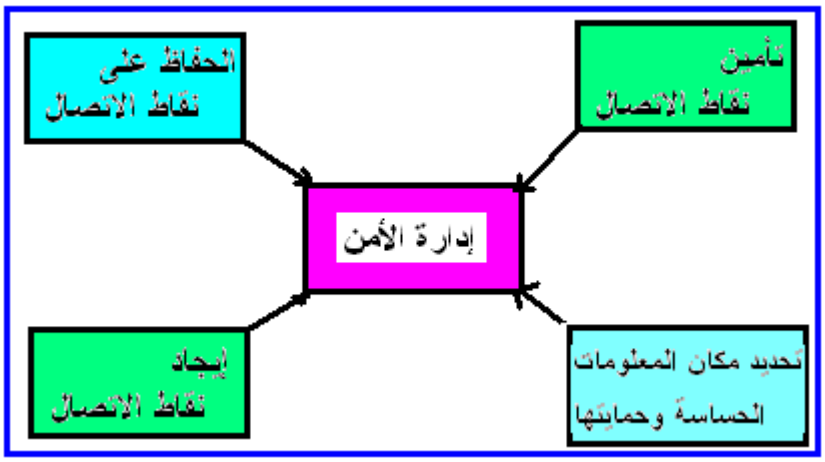
عزيزي الدارس إن الاهتمام المبدئي للعديد من المستخدمين عند توصيل حاسبات مضيفة إلى شبكة البيانات يكون ضعف الجهد المبذول في أمن المعلومات الحساسة الموجودة في الحاسب المضيف. وللتغلب على هذه المشكلة، يمكن **للحاسب المضيف** الذي يحفظ

المعلومـــــات الحساسة **منع الوصـــــول للشـــــبكة ومنع نقل المعلومات على وسط متنقـل،** ويشـمل هـذا الوسـط: الشـرائط الممغنطة أو الأقـــراص الضـــوئية. بهـــذه الطريقـــة، يســـتطيع فقط المستخدمون الذين لهم اتصال فعلى بالحاسب المضـيف الوصـول إلى المعلومـات الحساسـة. ولكن هـذه الطريقة بـرغم الأمن، ليست ذات كفاءة، فهي تزيح بفاعلية الاحتياج إلى شبكة البيانات.
يسـتطيع التنصـيب الملائم وصـيانة إدارة الأمن، توفـير أكـثر من بـديل عملي يحقق اهتمامات أمن المستخدمين ويزيد من رضـاهم في فعالية وأمن الشـبكة. إن بنـاء الرضا وأمن المعلومـات الحساسة هما الفوائد الأساسـية من إدارة الأمن. إن الانعكاسـات من عـدم وجـود إدارة أمن للشبكة من الممكن أن نتصوره بسهولة. على سبيل المثال، بفـرض أن شـبكة بيانـات خاصة بأحد المؤسسـات تم توصـيلها بشـبكة البيانـات العامـــة، وأن أحد أجهـــزة الحاسب في شـــبكة المؤسسة يحتـــوي على معلومـــات الـــرواتب، ويـــوفر أيضا طلبـــات تأدية خدمة معلوماتية لأي مستخدم. كما نلاحظ، فإن عاقبة هـذا الاتصـال غـير المحكـوم والمبـاح يمكن أن يضر المؤسسة.

2. تحقيق إدارة الأمن في شبكات البيانات

عزيـزي الـدارس، تتطلب إدارة الأمن الفعالة من مهنـدس الشـبكة أن يـــوازن بين الاحتيـــاج إلى معلومـــات حساسة آمنـــة، وبين احتياجـــات المستخدمين من الوصول إلى المعلومات ذات الصلة لتأدية وظـائفهم. لضمان تحقيق ذلك في إدارة الشبكة ينبغي اتباع أربع خطـوات، 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 وظـائف إدارة الأمن

يوضح شكل5.2 كيفية تحقيق وظائف إدارة الأمن. حيث تمثل قائمة رواتب المـوظفين قاعـدة بيانـات المعلومـات الحساسة المتصـلة بالحاسب الكبير.تعتـبر نقـاط الاتصـال هي: الـدخول عن بعـد، ونقل الملف. يقوم مهندس الشبكة بتأمين نقـاط الاتصـال بواسـطة تهيئة النظـام من خلال وحـدة الإظهـار (وحـدة طرفيـة) للسـماح فقط بتشغيل المستخدمين المفوضين ((Authorized. يقـوم نظـام الرصد بضـمان صـيانة الأمن بواسـطة تسـجيل محـاولات الـدخول غـير المفوضة.

أولا: تنصيب الوسائل الأمنية:

مثال: نفترض جهـاز حاسب يقـوم بتخـزين رواتب المـوظفين لأحد المؤسسات، وهو الـذي يحتفظ بمعلومـات حساسة عن المؤسسـة، وله نقطة اتصال واحدة، من خلال شـبكة البيانـات، وذلك باسـتخدام برنـامج الـدخول عن بعـد. والمطلـوب هو إجـراء عملية التحكم في الدخول لهذا البرنامج.

الحل

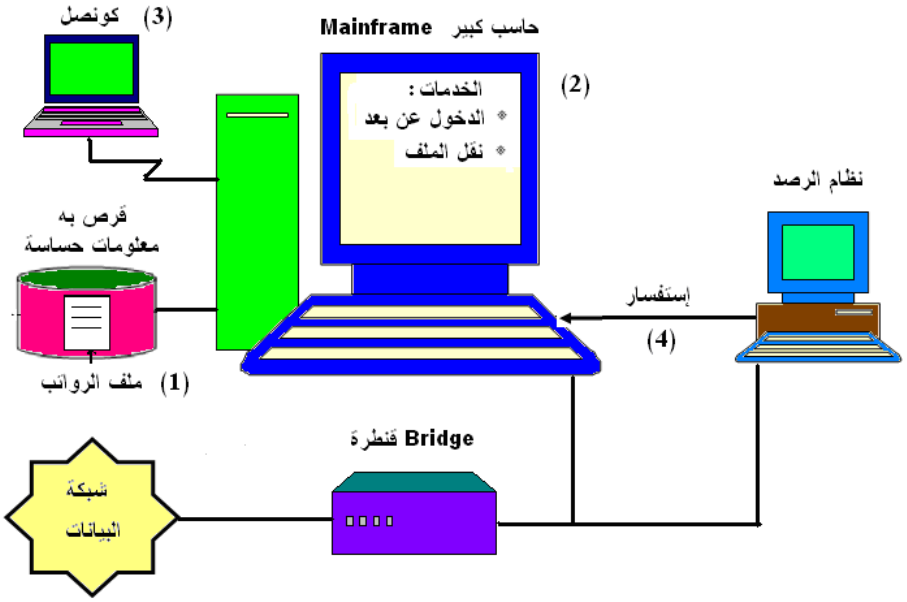
ولإجراء ذلك نتبع الخطوات التالية:

أولا: نستطيع أن نكفل للموظفين الذين لديهم تفويض تام بالاطلاع على المعلومـات، وذلك بـأن يخصص لهم فقط أرقـام حسـابات كمستخدمين.

ثانيـا: ضـمان تخصـيص كلمـات سر (Passwords) يتم طلبها من برنامج الدخول لكل رقم حساب مستخدم.

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

وهكذا، بعد أن يتم تنصـيب هـذه الوسـائل الأمنيـة، يمكن أن نطمئن أننا قد قمنا بتأمين المعلومات الحساسة.



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

ثانيا: استخدام الحاسبات المضيفة المفوضة:

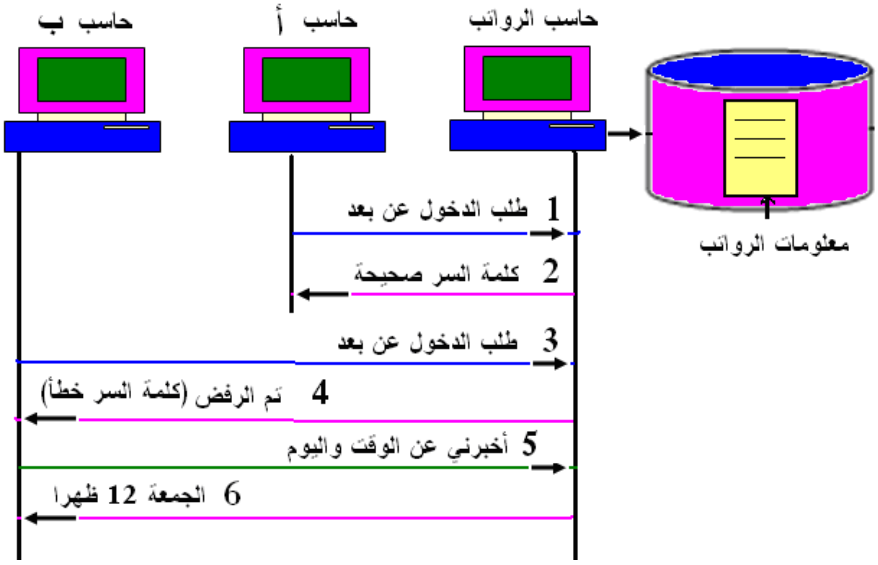
إن مستوى الحماية السـابق شـرحه، ربما لا يكـون كافيـا. بالإضـافة إلى وجود كلمات سر لكل حسـاب. ربما نريد توفـير طلبـات دخـول عن بعد إلى الحاسبات المضيفة الخاصة بقوائم الـرواتب، وأن تـأتي فقط عن بعد من قبل حاســـبات مضـــيفة مفوضة ((Authorized Remote Hosts. ولكي يتمكن المسـتخدم من الوصـول إلى بيانـات الــرواتب، يجب أن يــدخل أولا عن بعد إلى الحاســبات المضــيفة

المفوضة، ويوثق إذن الـدخول بواسـطة كلمة السـر. بعد ذلك يمكن أن يســمح للمســتخدم بــأن يواصل الــدخول إلى جهــاز الحاسب المخـزن عليه الـراتب، مـرة أخـرى من خلال سلسـلة متعاقبة من كلمات السر الموثقة.

لاحظ في هـذا المثـال أننا لم نحـاول تـأمين المعلومـات الحساسة نفسها. على الـرغم من أن المعلومـات الحساسة تكـون آمنة داخل جهاز الحاسب، سوف نجد بعد ذلك أنه من الضـروري، أن يتم تأمينها بين الأمــاكن الآمنــة. أيضا ينبغي أن نكــون على دراية بأنه في بعض الحــالات لا يتطلب الوضع تــأمين نقط الــدخول كلهــا. على ســبيل المثـال، نفـترض أن حاسب الـرواتب، يمكن الوصـول إليه بواسـطة الـدخول عن بعـد، لتوفـير خـدمات لإبلاغ مسـتخدمي الشـبكة عن الوقت، وهذا لا يعتبر معلومات حساسة عادة. في مثل هذه الحالات يمكن أن يسمح بالدخول بحرية إلى خـدمات الـوقت، كما هو موضح في شكل 5.3.

لكي نقنن عملية الــدخول إلى معلومــات الــرواتب، يتم اتباع الخطوات التالية:

- يطلب المسـتخدم الموجـود على جهـاز الحاسـب_"أ"_ طلب الدخول عن بعد إلى حاسب الرواتب.
- إذا كانت كلمة السر صحيحة، يتم السماح له بالدخول.
- يحاول مسـتخدم موجـود على جهـاز الحاسـب_"ب"_ الـدخول عن بعد إلى حاسب الرواتب.
- يتم رفضه لأن كلمة السر غير صحيحة.
- يقوم المسـتخدم الموجـود عند الحاسـب_"ب"_ بالسـؤال عن اليوم والوقت من حاسب الرواتب.
- يقـوم حاسب الـرواتب بإخبـاره عن اليـوم والـوقت، حيث أن معلومات الـرواتب هي معلومـات حساسـة، لكن المعلومـات عن اليوم والوقت ليست معلومات حساسة.



شكل5.3 طريقة الوصول للمعلومات الحساسة.

1.2 تحديد المعلومات الحساسة

إن الخطـوة الأولى لتحقيق إدارة الأمن تتم بواسـطة تحديد الحاسـبات المضيفة المتصلة بالشبكة، والـتي يوجد بها المعلومـات الحساسـة. إن معظم المؤسسات يوجد بها نظام يعـرف جيـدا المعلومـات الحساسـة، وهي غالبا **المعلومات التي تحتوي على: الحسابات، الماليات، العملاء، التسويق، الهندسة، ومعلومات الموظفين**. لـذلك من الوهلة الأولى، فإن هذه العملية تظهر مباشرة، ولكن ما يتم تعريفه بأنه معلومـات حساسة يمكن أن يختلف من مؤسسة لأخـرى، ويعتمد على الوسط المحيـط. إن الجـزء الصـعب في تحديد المعلومـات الحساسة هذه، هو إيجاد مكان على الحاسب المضيف لتخزين هذه المعلومات.

أسئلة تقويم ذاتي

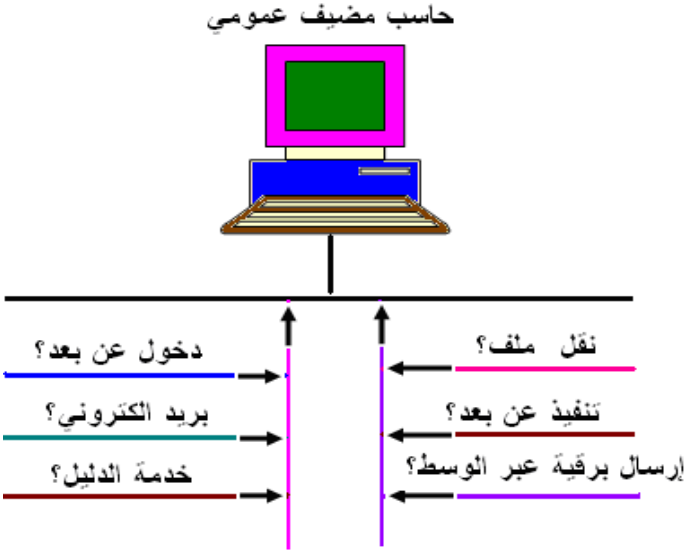
أكمل ما يلي: تختص إدارة أمن شـبكة البيانـات بأربعة خصائص هي:

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

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

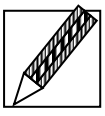
إيجاد نقاط الاتصال

بعد أن يتم معرفة المعلومـــات الحساسة ومكانهـــا، بعد ذلك يتم تحديد كيفية وصـــول مســـتخدمي الشـــبكة من الوصـــول إليهـــا. مع الأخذ في الاعتبار أن نقط الاتصال الأولى لأي شبكة بيانات هي الأسـلاك الفعليـة. إن إيجاد نقط اتصال أخرى في شبكة البيانات يكون غالبا وظيفة صعبة، وهذا سوف يتطلب عادة فحص كل جزء من البرنامج الـذي يقـوم بتأدية خدمة في الشـبكة. ويوجد العديد من الحاسـبات تمتلك الكثـير من مثل هذه البرامج. إن الوصول لهـذه الـبرامج يجـبر شـبكة البيانـات على أن تساهم في الوصـول من خلال نقط الاتصـال إلى المعلومـات الحساسة على الحاسب، كما هو موضح في شكل 5.4ـ لحسن الحظ، فـإن بعض أجهزة الحاسبات تمكننا من تبسيط مهمة إيجاد نقط الاتصال، بواسـطة 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 الجلمة 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:

- **الاتصـــال بالشـــبكة بطريقة غـــير رســـمية (Method Anonymous):**

عزيزي الدارس، تقم معظم أجهزة الحاسبات المتصلة بشبكة البيانـات بتوفير الدخول عن بعد للمستخدمين. وإذا لم تقم وسيلة الـدخول هـذه بتحديد المسـتخدمين المنفـردين (Unique) وتقـنين حـركتهم من خلال النظـام إلى المنـاطق المفوضة لهم، مع إمكانية فحص نقط الاتصـال بقدر الاستطاعة وجعلها آمنة (تستطيع كثير من الحاسبات أيضا، تحقيق عملية نقل الملفات عبر شبكة البيانات. مثل وسيلة الـدخول عن بعـد.) فإن استخدامها سوف يكون محدودا. كمثـال على خدمة نقل الملفـات، الـذي يتطلب تـدقيق إدارة الأمن هو عملية دخـول المسـتخدم كضـيف(Guest)ـ في نظام غير رسـمي (مجهـول المصـدر Anonymous)ـ في بروتوكول نقل الملفات FTP، وهو نظـام يسـمح للمسـتخدم بالـدخول لمواقع محـددة في الشـبكة كزائـر، ويسـمح للمسـتخدم بنقل ملفـات محددة.

يســتخدم بروتوكــول FTP في العديد من الحاســبات المضــيفة الــتي تستخدم بروتوكول TCP/IP. ويوجد العديد من الإصـدارات الـتي تسـمح للمسـتخدمين بالـدخول من خلال نظـام غـير رسـمي، وهـذا النظـام لا يستخدم كلمة سـر، لـذلك فـإن المسـتخدمين يمكنهم كتابة أي حـروف لكلمة السر والدخول إلى حساب خاص في النظام عن بعد. إن التوفير الذي يوفره الدخول من خلال نظام غـير رسـمي هو أن الملفـات الـتي يستطيع المستخدم استرجاعها من هذا الحسـاب عـادة تكـون محـدودة لبعض أجزاء صـغيرة من المجلـدات. وتسـتخدم عملية تهيئة بروتوكـول نقل الملفـــات غالبا في توزيع الوثـــائق والبرمجيـــات العامـــة. يمكن استخدام هـذا التطـبيق أيضـا، عنـدما لا يهتم مـدير جهـاز الحاسب بمن سوف يستطيع الـدخول إلى الملفـات الموجـودة في هياكل المجلـدات المحـددة. وبهـذا، إذا قـام جهـاز حاسب بتوفـير خاصـية الـدخول "غـير رســمية" لخدمة بروتوكــول نقل الملفــات، فإنه ينبغي على مهندسي

الشبكة المتصلة بها الحاسب أن يقومـوا بتنظيم المعلومـات الموجـودة بهذه المجلدات بعناية.

- **طريقة إظهار ومعرفة الملفات المطلوبة:**

ربما تكـون عملية الـدخول عن بعد ونقل الملفـات، هي من أكـثر أنـواع البرامج شيوعا، والتي توفر نقاط اتصال إلى جهاز الحاسـب. لكن يوجد برامج أخرى مثل: البريد الإلكتروني، وتنفيذ العمليات عن بعد، وملفات ومجلـدات أجهـزة الخـادم، وأسـماء أجهـزة الخـادم، يمكن أن تخصص نقاط اتصال إلى جهاز الحاسـب، والـتي تحتـاج أن تكـون آمنة بواسـطة إدارة الأمن. على سبيل المثـال، إن جهـاز الحاسب الـذي يعمل بنظـام التشغيل يونيكس، تكـون الخـدمات الـتي يوفرها الجهـاز، 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 أنــواع مختلفة عديــدة لأجهــزة الحاســب، لأحد أجهــزة الحاسب من الوصول إلى ملفات نظام آخر كما لو أنه موجـود على الحاسب المحلي باســتخدام شــبكة البيانــات. كما أن النظــام أيضا يفيد في مشــاركة المصـادر، حيث يسـتطيع فتح نقـاط توصـيل إلى الملفـات الحساسـة. بالمثــل، يوجد الكثــير من الحاســبات الشخصــية يوجد بها ملفــات أو تطبيقات توضح قائمة الخدمات التي يسـتطيع جهـاز الحاسب تقـديمها. يمكن أن يكـــون هـــذا الملف شـــائعا، مثل ملف تهيئة الشـــبكة NET.CFG ،أو ملف مخبأ مثل الملفــات ذات الامتــداد .INI إن إيجــاد التطبيقـات الموجـودة على الحاسب الشخصـي، الـتي ربما تسـتخدم الشــبكة يمكن أن تكــون عملية صــعبة. وقد نحتــاج اســتخدام محلل بروتوكول الشبكة، للمساعدة في تحديد نـوع بروتوكـول الشـبكة الـذي يجب أن يستخدمه الحاسب الشخصي.

- **استخدام بروتوكول NetBIOS:**

مثــال: إن الحاسب الشخصي الــذي يعمل كمــدير في وسط شــبكة محلية لميكروسـوفت، يسـتخدم بروتوكـول NetBIOS لإجـراء عمليـات الاتصال بين العملاء وأجهزة الخـادم. وهـذا الوسط له خاصـية ميدانية (Domains)، وهي منطقة في الشــبكة يوجد بها جهــاز الخــادم. يقــوم الخادم بإذاعة اسمه والمقاطعة التي يوجد بها على فترات دوريـة. على العملاء أن تصغي إلى التحديثات من خلال اسم ميـداني خـاص، قبل أن تســتطيع رؤية أجهــزة الخــادم في هــذه المقاطعة (وتقــوم 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

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

هـذه المعلومـات، ربما نكتشف أن الاتصـالات المحظـورة ينبغي أن يتم التأكيد عليها. على سبيل المثـال، إن كل بروتوكـول إدارة شـبكة تقريبا يكـون له قـدرة على سـؤال الحاسب عن المعلومـات الأساسـية، مثل عنـاوين الشـبكة، ونـوع إصـدار نظـام التشـغيل، ومـدة التشـغيل، والمعلومـات العامة غـير الضـارة. نفـترض على الـرغم من ذلـك، أن الحاسب الـذي يقـوم بتشـغيل بروتوكـول إدارة الشـبكة، يقـوم بفحص إصدار نظام تشغيل جديد من المورد. عنـدما يقف في طـابور الانتظـار من قبل مورد مضـارب، فـإن إصـدار نظـام التشـغيل العائـد، يكـون هو النظـام غـير المعـروف للعامة بعـد. هـذا النقص من المعلومـات، على الرغم من صغره، ربما يؤثر على سوق منتجات المضاربين.

- **استخدام نظام إدارة الشبكة:**

عامل آخـر، غالبا نغفل عنه هو المكـان الـذي يحتـوى على المعلومـات الحساسة في شبكة البيانات، وهو نظام إدارة الشبكة نفسه. إن نظـام إدارة الشبكة يوفر طرقاً كثيرةً للمسـتخدمين للكشف عن المعلومـات الحساسـة، الموجـودة على الشـبكة، والموجـودة في قاعـدة البيانـات العلائقيـة. عنـدما يتم تحديد نقـاط الاتصـال بشـبكة البيانـات، ينبغي أن نأخذ في الاعتبـار نظـام إدارة الشـبكة كحاسب مضـيف يحتـاج الى اهتمامات أمنية خاصة.

- **توحيد معايير نقاط الأمن:**

تخصص كثير من المؤسسات مصادر ماديـة، لتوحيد نقـاط الأمن لجميع أجهـزة شـبكاتهم والحاسـبات المضـيفة. ويعمل توحيد أمن الشـبكة كقاعدة للتعامل مع الطرق العديدة للوصول إلى المعلومات الحساسة. يمكن تحقيق هذه المعايير من خلال أي عدد من المعاملات. على سبيل المثـال، نسـتطيع تعريف نقـاط الاتصـال بواسـطة مصـنعي الحاسب المضيف، أو نـوع نظـام التشـغيل. في هـذه الحـالات، فـإن المؤسسة تسـتطيع أن تقـرر أن كل الحاسـبات المضـيفة من مصـنع معين به معلومـات حساسة لا يمكن الـدخول إليه بواسـطة بروتوكـول نقل الملفات عن طريق نظام غير رسمي (Anonymous)، أو يستطيع تحديد أن حزم برامج الشبكة للحاسبات الشخصية لا توفر أمناً كافياً، وبـذلك تمنع من اسـتخدامها. المبـدأ الرئيسي هنا يكـون للمسـتخدم في وضع معـايير مصـنع الحاسـبات المضـيفة الـتي تسـتطيع حفظ المعلومـات الحساسة والتطبيقات التي تستطيع تشـغيل هـذه الحاسـبات المضـيفة دون تسوية الأمن.

3.2 تأمين نقاط الاتصال

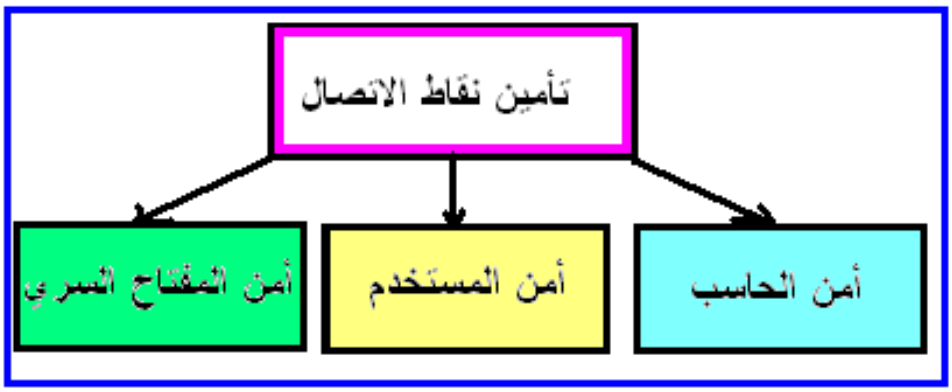
إن الخطوة التالية في إدارة الأمن، هي تطبيق تقنيات الأمن الضـرورية. ويمكن اسـتخدام الأمن في مسـتويات عديـدة في شـبكة البيانـات، كما يلي:

- يمكن استخدام التشفير في مستوى وصلة البيانات.
- يمكن استخدام مرشـحات الحـزم لتـأمين تـدفق حركة البيانـات في أجهزة مستوى الشبكة.

1.3.2 وسائل تأمين نقاط الاتصال في الشبكة

يوجد بكل حاسب مضيف خـدمات مصـاحبة، وهـذه الخـدمات تـوفر الوصول إلى المعلومات الحساسة التي تستطيع توفير واحد أو أكـثر من بين ثلاثة أنواع للأمن، هي موضحة في شكل5.5، وتشـمل على ما يلي:

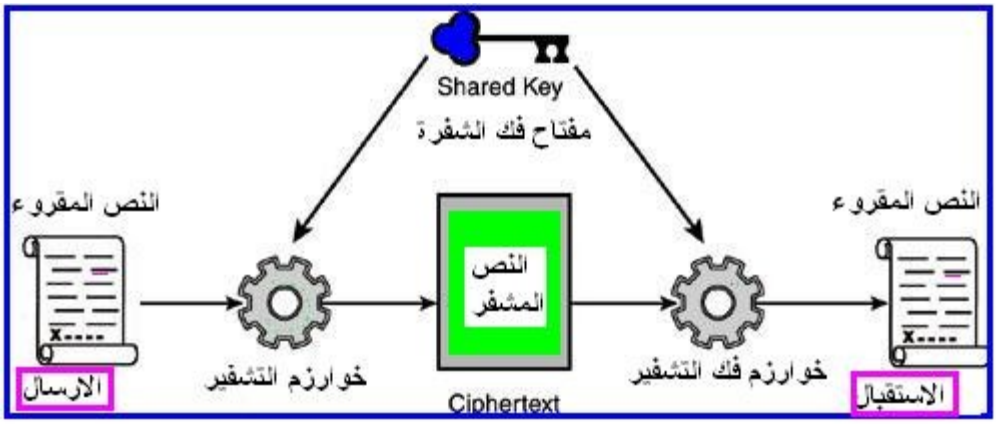
- أمن الحاسب المضيف بواسطة التوثيق.
- أمن المستخدم بواسطة التوثيق.
- أمن المفتاح السري بواسطة التوثيق.



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

نقـاط اتصـال. لكن لسـوء الحظ أن هـذه الطريقة مكلفـة، لأنها تحتـاج وجود عتاد مشفر أو برنامج لكل جهـاز متصل بالشـبكة المحليـة. أيضـا، إن تشفير الشبكة المحلية يجعل عملية فحص أعطال الشـبكة مشـكلة 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 تشـفير معلومات النص. وهذا يجعل خوارزم التشـفير بسـيطاً طالما تم معرفة مفتاح التشفير. وبسبب أن مفتاح التشـفير ربما يتم كسـره (معرفتـه)، لـذلك يمكن تغيـير المفتـاح عند كلا من المصـدر والهـدف على أسـاس منتظم بواسـطة إرسـال فعلي لمفتـاح جديد (إما باسـتخدام العتـاد أو البرامج)، لكل جهـاز يحقق تشـفير. إن الإرسـال الفعلي للمفتـاح يمكن أن يستهلك جزءاً من وقت ومصادر الشبكة، لكنها تكون الطريقة الأكثر أمانا لنقل المفـاتيح. وعلى الـرغم من أن تشـفير الأجهـزة بطريقة المفتـاح الخـاص يمكن أن يكـون الاحتفـاظ به صـعب، لكن كثـير من المؤسسـات تفضل اسـتخدام هـذه الطريقة لتـأمين المعلومـات الحساسة.

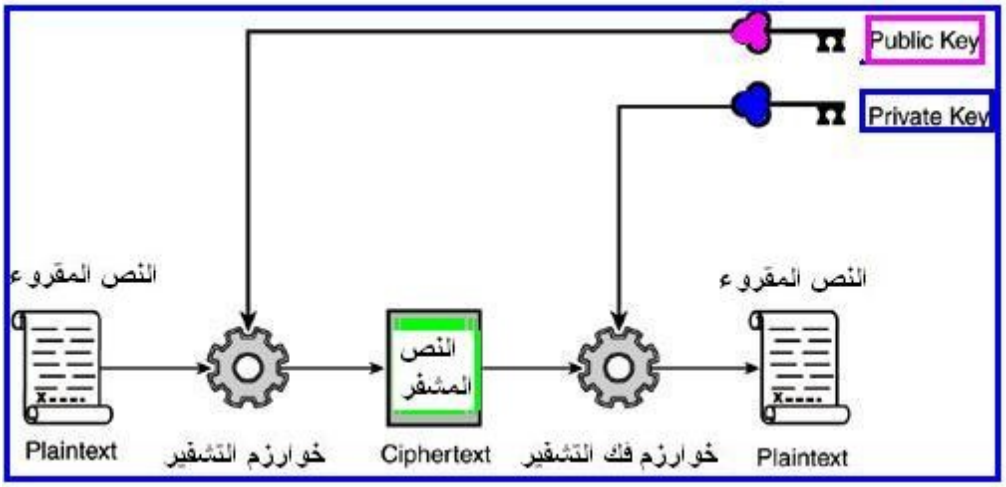
- **نظام التشفير القياسي** DES(Data Encryption Standard)**:**

نظام التشـفير القياسي هو أحد نظم التشـفير الشـائعة الـتي تسـتخدم المفتاح الخاص. وباستخدام DES يتم تشفير النص المقـروء باسـتخدام قطاعـات حزمية طولها 64 بيت. عند نظـام المصـدر، كل قطـاع نصي مقـروء يتم تشـفيره باسـتخدام مفتـاح تشـفير طوله 56 بيت. إن أي انحراف بسـيط مكمل للمفتـاح 56 بيت ينتج عنه تشـفير نصي مختلف تمامـا. يسـتخدم الخـوارزم المـركب دخل نص مقـروء طوله 64 بيت، ويتم تشفيره إلى 64 بيت نص مشـفر. عند نظـام الهـدف، تتم العملية العكسية، ويحول النص المشفر إلى نص مقروء.

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

إن استخدام طريقة المفتاح العـام في التشـفير لا تعتمد على مشـاركة كل من نظام المصدر والهـدف لنفس مفتـاح التشـفير. حيث تمنع هـذه

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 مفتـاح التشـفير في نفس اللحظة إلى كل من مصـدر وهـدف يتم حذفـه. ومن عيـوب نظـام التشـفير باسـتخدام المفتاح العـام، أن كل نظـام يريد أن يرسل نصـاً مشـفراً إلى الهـدف، يجب أولا أن يستفسر عن الجزء العام من مفتاح التشـفير في الهـدف. أيضا، عند إرسـال التشـفير في اتجـاهين، فـإن كل نظـام يحتـاج معرفة الجـزء العـام من مفتـاح التشـفير. يسـتخدم بروتوكـول إدارة الشـبكة البسيط (الإصدار الثاني) طريقة التشفير باستخدام المفتاح العام.

4.3.2 ترشيح الحزم

إن العديد من أجهزة الشـبكة مثـل: الجسـور، والمفـاتيح، والموجهـات، يمكنها تحقيق ترشيح الحزم المبني باستخدام عنـاوين الوصـول لوسط الشبكة MAC (Medium Access Control). إن عملية ترشـيح الحـزم، توقف الحزم من الوصول إلى الحاسبات المضـيفة غـير الآمنـة، قبل أن تصل إلى نقطة اتصال ربما تحتوي معلومات حساسة. لكن على الرغم من ذلـك، فـإن هـذه الطريقـة، ربما تسـاعد في توفـير الأمن، إلا أنها تتعرض لبعض المشاكل.

أولا: إن مرشحات الحزم يجب أن تهيئ من خلال كل أجهـزة الشـبكة. وهكذا لكل عنوان جديد يتم إضافته أو يتم تغيـيره، سـوف نحتـاج تغيـير المرشحات.

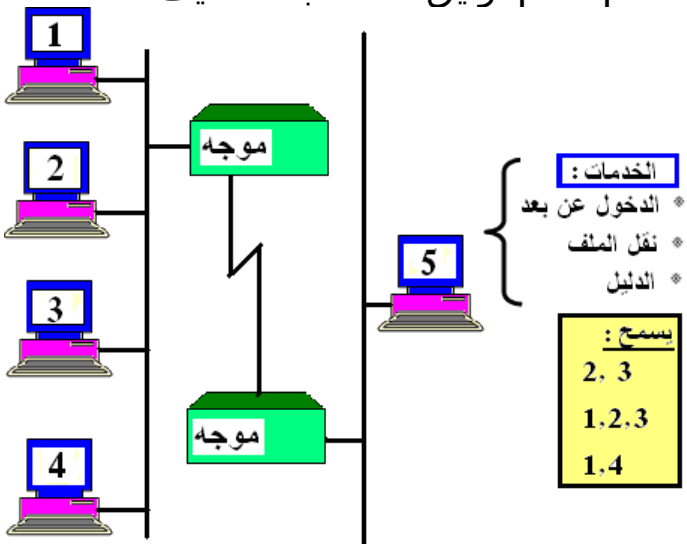
ثانيا: باستخدام مرشح لا يعمل، إذا قـام الحاسب المضـيف غـير الآمن بتغيير العنوان دون أن يخبرنا بذلك.

على سبيل المثال، بفـرض أن جسر إثـرنيت تقـوم بترشـيح الحـزم بين قطاعـات مؤسسة بنـاء عنـوان MAC. بسـبب أن عنـاوين الوصـول الشـبكية تكـون نوعيا مخزنة في شـريحة ذاكـرة قـراءة فقط ROM متواجـدة في وحـدة مواجهة قنطـرة ايـثرنيت، فـإذا كـانت لوحة وحـدة المواجهة موضوعة في حاسب مضيف غـير آمن، لكي يتم تغيـيره، فـإن اللوحة الجديدة سوف لا تحتوي على نفس عنـاوين الوصـول الشـبكية، وأن مرشحات الحزم سوف لا تستطيع على أية حـال وقف المعلومـات من والى الحاسب المضيف غـير الآمن. يمكن أن تنتج هـذه المشـكلة، ليس فقط بواسـطة مسـتخدمين مـاكرين (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 وصـول الشبكية جديـدة. يوجد بعض الحاسـبات المضـيفة تـوفر معـاملات تهيئة برمجية تسمح لمهندس الشبكة بتنصيب عناوين الوصول الشـبكية لهم،

و احتمـال تجنب هـذه المشـكلة أو جعلها أسـهل عنـدما يريد إحبـاط (توقيف) مرشح.

5.3.2 توثيق الحاسب المضيف

تسمح طريقة توثيق الحاسب المضـيف الوصـول إلى الخدمة بنـاء على عنوان محدد موجود بجهاز حاسب مضيف يعمل كمصدر، وهـذا المحـدد هو عبارة عن عنوان شبكة شائع مثل الذي يستخدم بواسطة X.25، IP أو Dec _Net، أو حتى بواسطة عناوين الوصول الشبكية. ويوضح شكل 5.8 مثالاً لتنصـيب شـائع لتوثيق حاسب مضـيف. إن خـدمات 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 الـذي يسـتخدم بروتوكـول X.25 في الاتصـالات من خلال وصلة توالي، ربما لا يقرر قبـول أو رفض المكالمـات بنـاء على عنـاوين منبع X.121 (نظام تخصيص عنـاوين). أو ربما لا يسـمح لكل حاسب من الوصول إلى الخدمة، بل يسمح فقط لجـزء من مجموعة كل احتمـالات عناوين شبكة المصدر.

بسبب أن توثيق الحاسب المضيف مؤسس بنـاء على عنـاوين الشـبكة، فإن العديد من أجهزة الشبكة أيضا تستطيع المساعدة في تحقيق هـذه الوظيفة. إذ تسـتطيع قنطـرة شـبكة حلقة تـوكين (Token Ring) عمل ذلك بواسطة تشغيل ***الوصول المحظور***، للسماح فقط لنظم مصـدر 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: x host <host name>).

- **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

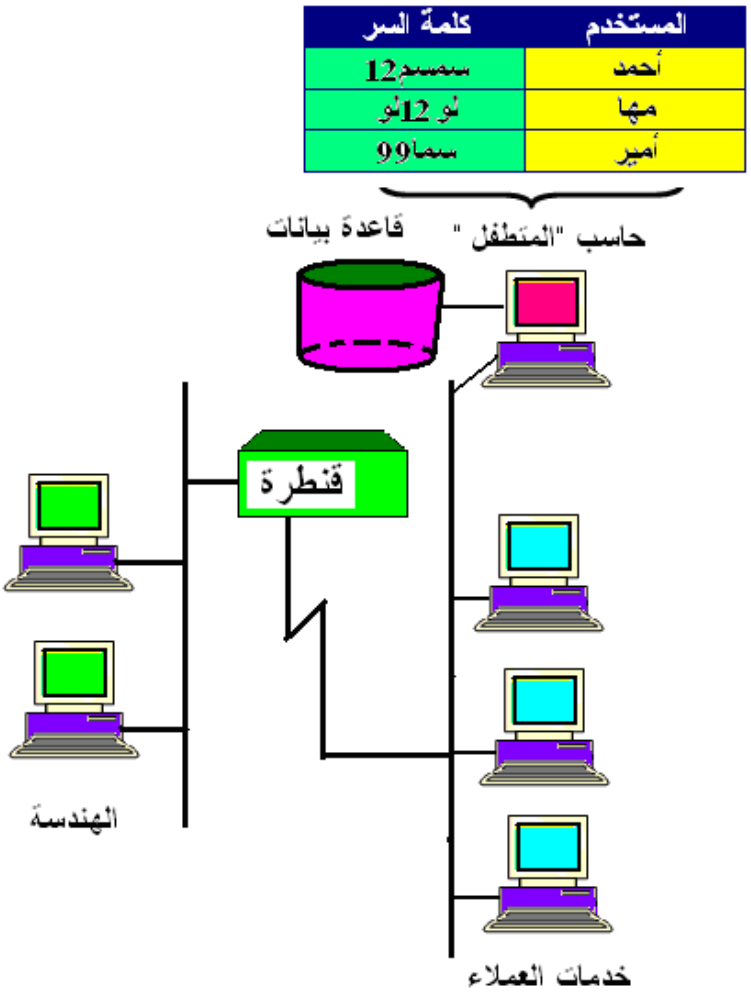
فقط مفيدة لتوثيق واحد فقـط. العيب الواضح لهـذا النظـام، أنه يحتـاج من المستخدم أن يحمل مولد كلمة السر وأن يقوم بإدخال المفتاح إليه في كل مرة يحتاج فيها التوثيق.

- **بروتوكول تاكاكس :TACACS**

عزيزي الـدارس، من أمثلة الـبروتوكولات القياسـية الـتي تحـدد طريقة الاتصـال بين نظـام الهـدف وخـادم كلمة السر الـتي يتم تنفيـذها، هو بروتوكول TACACS (Terminal Access Controller Access Control System)، ومعناه: محكم الاتصال الطرفي لنظـام تحكم الوصـول. وهو ***بروتوكـول مفـوض عن بعد*** يسـتخدم للاتصـال بالخـادم المفـوض لتحديد سـماحية دخـول العميل إلى شـبكة البيانـات. وهو عبـارة عن برنامج، يوجد منه إصدار حـديث يطلق عليه مسـمى TACACS+، وهو يستخدم عادة في شبكات البيانات التي تعمل بنظام التشغيل يونيكس. في المثال الذي تم شرحه سابقا، باسـتخدام حاسب "السـيد" وحاسب "الخـادم"، لتوضـيح كيفية تنصـيب إدارة أمن فعـال. فبـدلا من السـماح لكل مسـتخدم له حسـاب على "الخـادم" بالوصـول إلى الـبرامج الموجـودة على حاسب "السـيد"، يمكننا فقط اسـتخدام الخدمة الـتي تمكن الوصول إلى هذه البرامج مع حساب صحيح على "السـيد". بهـذه الترتيبات، ولتشغيل البرامج من "السـيد"، فـإن المسـتخدم، أولاً ينبغي أن يبدأ بأستخدام حاسب مفوض، وثانيـاً أن يـدخل كلمـة سر فريـدة ((Unique.

مثال: خدمة عميل مفوض من خلال كلمات سرية:

نفـترض حاسـباً يسـمى "المتطفـل"، يقـدم الخدمة الـتي تسـمح للمسـتخدمين الـدخول إلى قاعـدة بيانـات تتكـون من معلومـات عملاء مؤسسـة، كما هو موضح في شـكل5.7. يسـمح فقط للمـوظفين العـاملين في قسم خدمة العملاء للمؤسسة المفوضـين بالـدخول إلى هذه المعلومات الحساسة. وتبعا لذلك، عنـدما يحتـاج بعض وكلاء خدمة العميل بعض المعلومـات عن العملاء، فهي تسـتخدم برنامجـاً موجـوداً على حاسباتهم الشخصية متصل بالحاسب "المتطفل". على الرغم من ذلك، قبل أن يقوم الحاسب "المتطفـل" بإعطـاء المعلومـات للوكيـل، تقـوم قاعـدة البيانـات بسـؤال الوكيل عن كلمة السر الـتي تحـدد أن المستخدم مفوض له اسـتخدام قاعـدة البيانـات. وبـذلك لا يسـمح لكل مسـتخدم جهـاز حاسـب، في مكتب وكالة خدمة عميـل، بـأن يسـتطيع 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 عـام أكـثر فاعلية من طريقة ***توثيق الحاسب المضيف*** الـذي يعمل بمفـرده، إلا أن لها عيباً ممـيزاً. تقريبا فـإن كل طـرق توثيق المسـتخدم تعتمد على التهيئة السليمة لجهاز الحاسب. من الواضح، أنه إذا قام الحاسب بتوفير توثيق المســـتخدم من أجل الخدمـــة، وجعل كلمة السر هي نفســـها لكل مستخدم، فإن الأمن المطلوب لا يتم تحقيقه.

- **دمج عمليـــــتي توثيق المســـــتخدم وتوثيق الحاسب المضيف:**

إن دمج عمليتي توثيق المستخدم، وتوثيق الحاسب المضـيف معا يـوفر وسـيلة أكـثر فاعلية لتـأمين نقط اتصـال أحسن من اسـتخدام طريقة واحدة منهما فقط. لتوضيح ذلك، نعود إلى مثال الحاسب "المتطفـل". تم التخطيط على أن يتم إعطـــــاء كل مســـــتخدم كلمة سر لتوثيق المستخدم. لكن هل ذلك سوف يوفر لنا كل الأمن الذي نحتاجه؟ إن أي مستخدم معه حاسب شخصي وكلمة سر وحساب في قاعـدة البيانـات يســـتطيع الوصـــول إلى المعلومـــات الحساسة من خلال الحاسب "المتطفـــل". لتحســـين الأمن، نريد تطـــبيق كلا من توثيق الحاسب المضيف، وتوثيق المسـتخدم في هـذه الخدمـة. إن هـذه الطريقة ***ذات المسـتويين*** سـوف تكفل أن كلاً من المسـتخدمين الـذين يطلبـون الخدمة يـأتوا فقط من حاسـبات مضـيفة مفوضة وأنهم مسـتخدمون مفوضون.

7.3.2 توثيق المفتاح

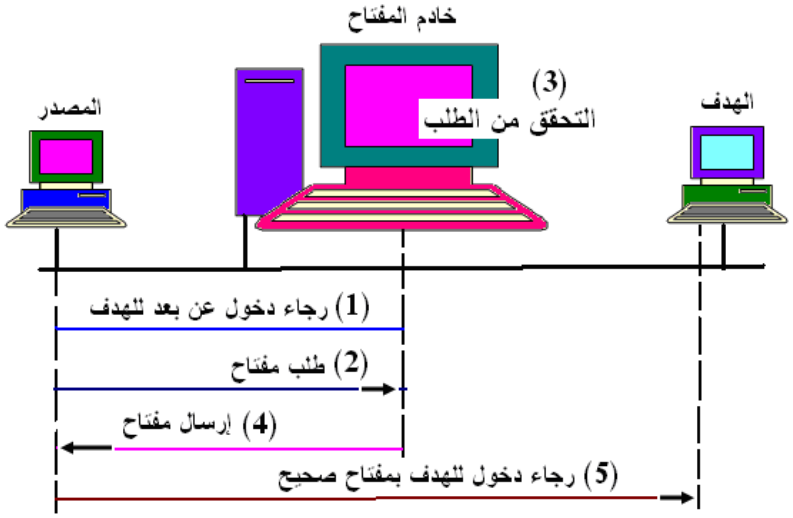
يـــوفر نظام توثيق المفتـــاح وســـيلة لتحقيق كلا من توثيق الحاسب المضيف، وتوثيق المستخدم مع إضافة مـيزة دون الاعتمـاد مطلقا على حاسب الهـــدف المضـــيف. وتعمل طريقة توثيق المفتـــاح بواســـطة تخصيص حاسب مضيف على الشبكة يسـمى ***خادم المفتـاح*** A Key Server .

يكـون خـادم المفتـاح مسـئولا عن إصـدار المفـاتيح إلى المسـتخدمين المفوضين. عندما يتم طلب خدمة، فـإن حاسب المصـدر يسـأل خـادم المفتاح عن المفتاح. بعد ذلك، ربما يمتلك خادم المفتاح نوع المستخدم داخل كلمة السر للتفويض. والآن يستطيع خادم المفتـاح تحديد كلاً من حاسب المصـدر والمسـتخدم طـالب الخدمـة. بنـاء على هـذه البيانـات وعلى قواعد الأمن المخزنة داخل خادم المفتاح، فإن الخادم ربما يصدر مفتاحاً صحيحاً.

إن هذا النظـام يعمل بسـبب أن حاسب الهـدف سـوف يسـمح بالخدمة فقط عندما يكون طلب الدخول مصـحوبا بالمفتـاح الصـحيح. في بعض خادمات تفويض المفتاح تكون المفاتيح الصحيحة غير متاحة في فترات الاستراحة. ويمكن أن يسبب ذلك توقيف جلسة المستخدم، ولكنه أيضا يضمن أن المفتـاح الصـحيح المنفـرد لا يسـمح بـدخول غـير مقنن. كما نرى، بسبب أن خادم المفتاح يقوم بتفويض المسـتخدم، ويمنع الـدخول إلى الخدمات، فإنه يحتاج أن يكون تحت أمن فعلي قوي.

- **مثـال: عملية طلب الـدخول عن بعد باسـتخدام توثيق المفتاح:**

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



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

- يقـــوم حاسب المنبع بطلب رجـــاء خدمة الـــدخول 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 المفتـاح بـالتحقق من حاسب المصـدر، وضـمان أن المسـتخدم مفـوض، لاسـتخدام خدمة الـدخول عن بعد للحاسب الهدف.
- عندما يتم فحص كل شيء، يقـوم خـادم المفتـاح بإصـدار مفتـاح صـحيح للحاسب المصـدر من أجل الـدخول عن بعد إلى حاسب الهدف.
- يتم إرسال المفتاح الصحيح إلى حاسب المصدر.
- يقـوم حاسب المصـدر بطلب رجـاء خدمة الـدخول عن بعد إلى حاسب الهدف بواسطة المفتاح الصحيح.

في **طريقة توثيق المفتـاح،** يكـون خـادم المفتـاح حرجا للاحتفـاظ بتأمين نقاط الاتصال الخاصة بخدمات شبكة البيانـات. من المهم أيضـا، أن تتم إدارة وتهيئة خـادم المفتـاح بشـكل صـحيح. لكي تعمل طريقة

توثيق المفتـاح، فـإن كل خدمة على حاسب المصـدر يجب أن تطلب مفتاحاً من خادم المفتاح، قبل بدء العملية. بالإضـافة إلى أن الخـدمات في حاسب الهدف يجب أن تقبل طلبـات الخدمة فقط عنـدما يصـاحب هذه الطلبات المفتاح الصحيح. ويعني ذلك أننا لا نستطيع تنصيب خـادم المفتاح وأن نبدأ استخدام توثيق المفتاح ببساطة. يجب أن تتغير وتتهيأ كل التطبيقات والخدمات لاستخدام خادم المفتاح. لقد أصـبحت طريقة توثيق المفتـاح أكـثر شـيوعا وخاصة في حاسـبات يـونيكس. كما يوجد العديد من الموردين توفرون أشكالاً من نظم توثيق المفتاح.

2.4 المحافظة على نقاط اتصال آمنة

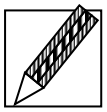
تعتبر عملية الصيانة هي الخطـوة الأخـيرة للحصـول على نقـاط اتصـال شبكة آمنة وفعالة. كما تعلمنا سـابقا، إن الاحتفـاظ بمعـايير أمن حديثة وآمنة في شبكة البيانات مهمة صعبة وتتطلب الـتزام المؤسسة بتوفـير كل من المصـادر والـوقت. من مهـام مهنـدس الشـبكة الحفـاظ على الشبكة، بصرف النظر عن كيفية التخطيط والبناء، فعنـدما تنتهي تكملة مهمة نظام الأمن، فإن الصيانة وتعديل الشبكة سوف يكون مطلبـا. إن المبـدأ الرئيسي للصـيانة هو تحديد مكـان الإجهـاد أو اخـتراق الأمن الفعلي. في بعض الحـالات ربما يتم عمل ذلك بواسـطة المهندسـين المسـئولين عن فحص أمن الشـبكة. فهم قد يسـتخدمون مثلا نقـاط اتصال الشبكة كأساس للفحص، والتي يقـوم مهنـدس الشـبكة بتوثيقها وإجـراء الأمن المطلـوب لهـا. لسـوء الحـظ، فـإن حفظ هـذه الوثـائق وتحديثها باستخدام وفـرة بـرامج الشـبكة المتاحة في الأسـواق يكـون مهمة أخرى كبيرة. لـذلك في مثل هـذه الحـالات، فـإن أحسن ما يأمله فاحصو الشـبكة هو فهم المسـائل المتعلقة بـإدارة الأمن والخطـوط الإرشادية للمؤسسة المتعلقة بذلك.

- **برامج محاولات اختراق أمن الشبكة:**

عزيزي الدارس، في حالات أخري، فإن مهندسي الشـبكة ربما يوظفـوا بـرامج على الحاسـبات المضـيفة لفحص مشـاكل الأمن المعروفة والشـائعة. يمكن للـبرامج البسـيطة محاولة اخـتراق الأمن بواسـطة محاولة كسر كلمـات السر ومفتـاح الشـفرة بطريقة عشـوائية. يمكن للبرامج الأكثر دقة أن تشن هجوما على الشبكة والحاسبات بعدة طرق مختلفة. في كلا الحالتين، فإن كل برنامج سوف يخبر مهنـدس الشـبكة عن نجاحه أو فشـله في اخـتراق الأمن. إن المنطق وراء ذلك أنـه، 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 Network File System))NFS:

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. الـ

عزيزي الـ
بتحقيق إدارة الأمن [illegible] التي تمتلك شبكة بيانات غير متصلة بالشبكة العامة قد تجد أن هذه

الخطوات سوف توفر الأمن اللازم. لكن في المؤسسة الـتي بها شـبكة بيانات متصلة بالشـبكة العامـة، فـإن تحقيق إدارة الأمن يتطلب طريقة مختلفة. ويوجد ثلاثة أنواع ممكنة لتوصيل شبكة البيانات العامة بشـبكة بيانات المؤسسة، وهي:

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

إن شبكة البيانات الخاصة التي تسـمح بعـدم توصـيل الـدخول عن بعـد، من شبكة البيانات العامة ربما تستخدم ببسـاطة توصـيلته إلى الشـبكة 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 العامـة. وتكـون كل العمليـات مع شـبكة البيانـات العامة يتم بـدؤها من خلال شـبكة بيانـات المؤسسة. بهـذه الطريقـة، فـإن المؤسسة لا تحتـاج إلى أن تجد نقـاط اتصال بشبكة البيانات العامة، بسبب أنه لا يوجد مثل هذه النقاط.

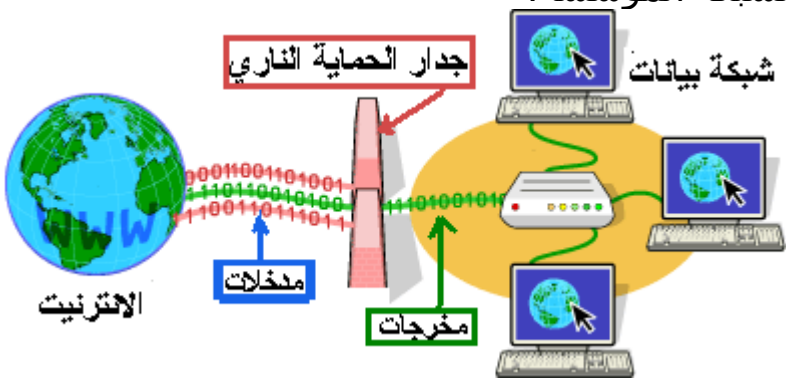
على العكس من ذلـــك، عنـــدما لا تضع المؤسسة أية محـــاذير على العمليات بين حاسباتها وشبكة البيانات العامة، فـإن كل إدارة أمن يجب أن تحفظ في كل حاسب منفـــرد موجـــود داخل المؤسســـة. في هـــذا التركيب، ربما تسمح المؤسسة لأي بيانات أن تدخل شـبكتها وأن تعتمد على الحاسبات في توفير توثيق الحاسب المضيف أو توثيق المسـتخدم قبل إطلاق المعلومات الحساسة.

لكن، بفـــرض أن المؤسسة تريد إدخـــال بعض الخـــدمات من الشـــبكة العامـــة، أو عـــرض بعضـــها إلى الشـــبكة العامـــة، لكن لا يوجد حاسب مضيف، أو مستخدم مفوض على معظم حاسـباتها. من الواضح أن فتح شبكة بيانات المؤسسة وتوصيلها بالشبكة العامـة، في مثل هـذه الحالة سوف يؤدي إلى مخاطر أمنية. إن طريقة التوصيل المحـدودة تسـتطيع مساعدة ونفع الاهتمامات الأمنية في هذه الحالة.

- **الجدار الناري Firewall:**

يتضـمن الوصـول محـدود السـماح فقط لمجموعة صـغيرة مفوضة من الحاسـبات المضـيفة لتوفـير الخدمة بين شـبكة المؤسسة والشـبكة العامـة. يتم وضع مجموعة من نظم الحاسـبات أو أجهـزة الشـبكة بين شـبكة المؤسسة والشـبكة العامة لتـدعيم إدارة الأمن، وهـذه الطريقة تسـمى بنـاء جـدار نـاري ((Firewall، ويـبين شـكل5.11 مثـالاً يوضح استخدام جدار حماية ناري بين شبكة بيانات مؤسسة وشبكة الانـترنت.

وتمكن طريقة استخدام الجدار الناري مهندس الشـبكة من التحكم في كل حاسب يـوفر خدمة إلى شـبكة البيانـات العامـة. وبـذلك يتم تحديد الخـدمات المتاحة للشـبكة العامة ويـوفر نقـاط اتصـال آمنة بطريقة أحسن لشبكة المؤسسة.

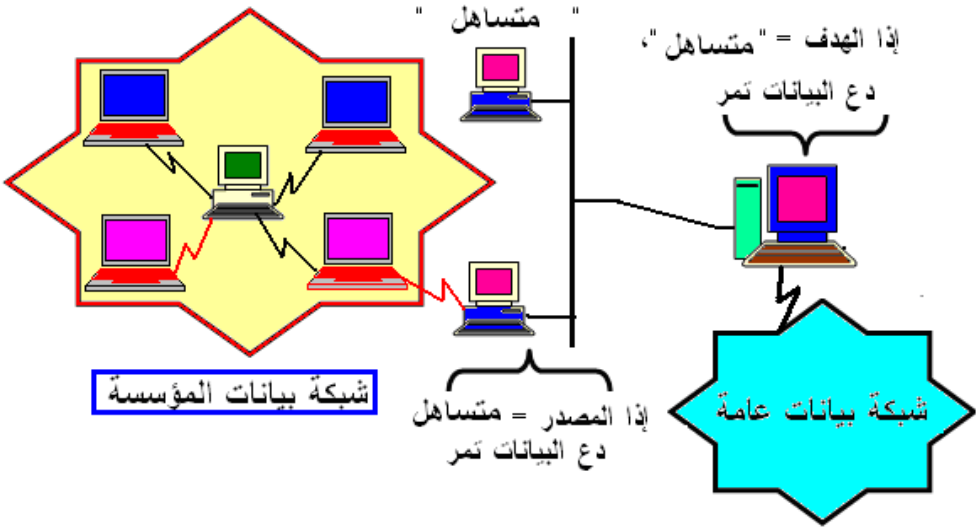


شكل5.11 استخدام جدار الحماية الناري في ترشيح المدخلات لحماية المستخدم والشبكة من القرصنة.

إن جدار الحماية الناري هو عبارة عن طريقة لدمج خصائص إدارة الأمن لسلسة من أجهزة الشبكة تم تصـميمها بحيث تسـمح فقط لمعلومـات معينة بالمرور من مكان لآخر. في هذه الحالة فإن الجدار الناري سوف يسـمح فقط لبيانـات معينة من الشـبكة العامة كي تمر خلال الشـبكة الخاصـة. ويتم بنـاء الجـدار النـاري عـادة بواسـطة اسـتخدام أجهـزة موجهات تقوم بتوفير مستوى شبكي لترشيح الحزم بواسطة اسـتخدام حاسبات تعمل كبوابات سريعة Gateways تتحكم في تدفق البيانات بين التطبيقات.

مثال: ضبط التهيئة للسماح بوصول مقنن:

نفترض أن مؤسسة بها شـبكة بيانـات متصل بها جهـاز حاسب يسـمى "متساهل"، وهو عبـارة عن تطـبيق لبوابة طريق داخل الجـدار النـاري. يعمل النظام الأمني على ضمان أن أي بيانات خاصة بشـبكة المؤسسة يجب أولاً أن ترسل إلى الحاسب "متساهل"، كما هو موضح في شـكل 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

المضـيف، ومصـادر الشـبكة، وكـذلك بواسـطة تبليغ المهنـدس عن محاولات اختراق الأمن. يتم تحقيق إدارة الأمن في نظام إدارة الشـبكة باسـتخدام أدوات برمجيـة. وحسب كيفية دقة الأداة المسـتخدمة والمتاحة لمهندس الشبكة، يتم الحكم على جودة النظام.

1.4 اسـتخدام الأداة البسـيطة لإدارة الأمن

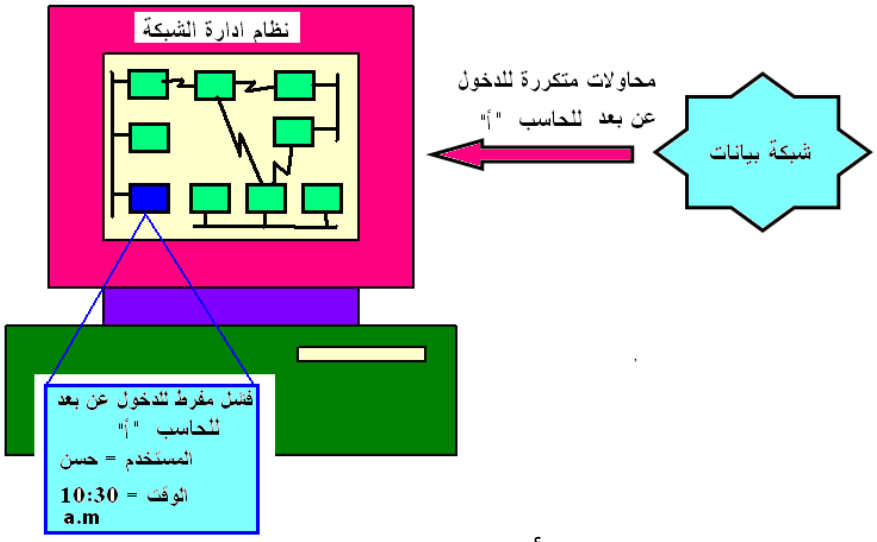
إن الأداة البسـيطة الـتي تسـتخدم لإنجـاز إدارة الأمن في نظـام إدارة الشبكة، تحتـاج أن تظهر الأمـاكن الـتي يتم فيها تنصـيب معـايير الأمن. بالاعتماد على الـدخل من خريطة الشـبكة الرسـومية، فـإن هـذه الأداة تسـتطيع إنشـاء شاشة تظهر كل معـايير الأمن المطبقة في أي جهـاز حاسب مضيف لمستخدم يتم اختياره. بالإضـافة إلى تحديد كل الأمـاكن المحددة لعناوين شبكية أو مستخدم معين في الشـبكة. إن الأداة ينبغي أن تكون قادرة على الاستفسار من قاعدة بيانات التهيئة، وإنشاء نافذة لعـرض المعلومـات الضـرورية. كما تسـتطيع أداة الأمن اسـتخدام معلومـات إدارة التهيئة الموجـودة في نظـام إدارة الشـبكة، في حل مشاكل التوصيل المعقدة الموجودة في الشبكة.

تقوم الأداة البسيطة بالاستفسار من قاعدة البيانات العلاقية في نظـام إدارة الشبكة، عن تهيئة جهاز تم اختيـاره من خلال خريطة الشـبكة. إذا لم تـوفر بـرامج إدارة الأمن في نظـام إدارة الشـبكة، إمكانية تحقيق خصـائص الأمن واسـتخدامها بواسـطة الأداة البسـيطة، فـإن مهنـدس الشبكة يستطيع استخدام الأداة لرؤية أجزاء من تهيئة الأجهـزة، ويقـوم هو بإجراء وتشغيل خصائص الأمن المتاحة يدويا.

2.4 استخدام الأداة المركبة لإدارة أمن الشبكة

يكون للأداة المركبة القـدرة على إجـراء تطبيقـات في الـزمن الفعلي، ورصد اتصال المعلومات الحساسة. بعد تحديد مشكلة الأمن المحتملة، فإن هذا التطبيق يستطيع تغيير ألـوان الحاسـبات المضـيفة المتـأثرة أو أجهزة الشبكة في خريطة الشبكة الرسومية. أو إذا توفر عدد كبـير من الألوان لأحداث مختلفة (ويصبح الأمر مربكا)؛ فإن الأداة تستطيع تدوين ما تم الحصـول عليه بوسـائل أخـرى، مثل قـرع جـرس النظـام (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

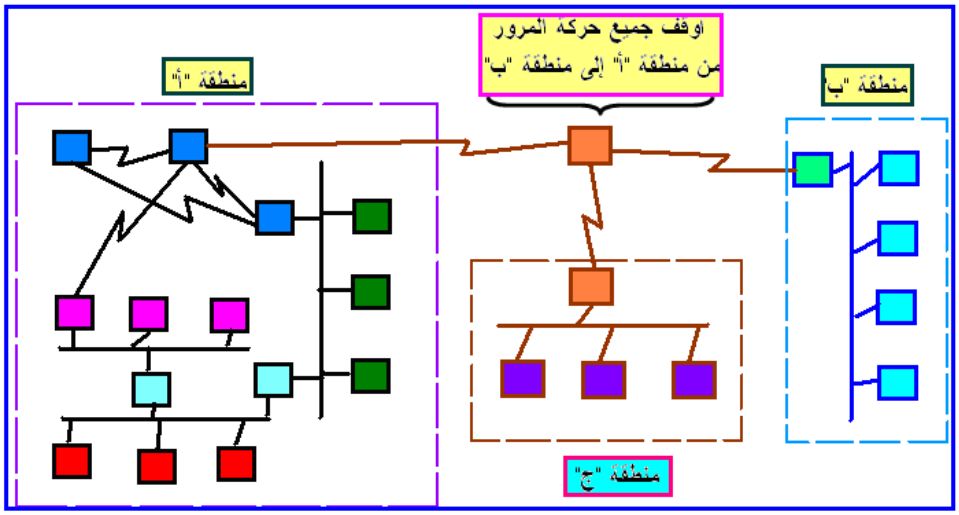
تستفسر عن الحاسب المضيف أو الجهاز في المكان المطلوب تطـبيق الأمن عنـــده، بعد ذلك تستفسر من المســـتخدم عن المعلومـــات المسـتولى عليهـا. على سـبيل المثـال، تكـون عملية تطـبيق الأمن في تحديد مرور عناوين الشبكة، مختلفة تماما عندما يتم تحقيقها على جهاز أو مكــرر (Repeater)، أو جسر أو حاسب مقدمة ومــؤخرة، أو موجــه. بالإضافة إلى أنه لكل جهاز مصنع، يمكن أن يأخذ التطبيق الأمـني شـكلا مختلفا تماما.

3.4 اســـــتخدام الأداة المتقدمة لإدارة أمن الشبكة

تســتطيع الأداة المتقدمة تجميع البيانــات عن نمــاذج حركة المــرور، لإرشادنا حول الأمن المفروض إجراؤه. وتحتـاج إدارة الأمن التـام هـذه الوظيفــة، بالإضــافة إلى الخصــائص الخاصة بكل من الأداة البســيطة والمركبـة. يمكن للأداة المتقدمة فحص نـوع الأمن الـذي ننـوي تنصـيبه على الحاسب أو الجهـــاز، وتنبهنا إلى المحـــاذير الممكنة عن هـــذه التنصـيبات. يمكن للأداة أن تسـتقبل مـدخلاً من طرفنـا، بالإضـافة 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 لتنصـيب نظـام مرشح حـزمي لإيقـاف حركة مـرور البيانـات بين منطقـتين في شـبكة البيانـات هما أ، ب كما هو مـبين في شــكل5.14. ســوف تقــوم الأداة بتحليل نمــاذج حركة المــرور بين المنطقتين أ، ب في الشـبكة. بعد ذلك تخبرنا بـأن الخطة الأمنية يمكنها وقف 85% من حركة المرور بين المنطقتين أ، ب في الشبكة. إن هذه النسبة من المعدل الفعـال ربما تمثل التـأثير الـذي نريـده في النظـام. بغض النظر، عن إن الأداة المتقدمة سوف تقــوم إما بتعزيز جهودنــا، 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".

تحتـــاج الأداة المتقدمة أن تعمل بـــالقرب من معلومـــات إدارة الأداء المخزنة في قاعــدة البيانــات في نظــام إدارة الشــبكة، لإيجــاد حركة المرور الكلية بين المنطقتين أ، ب في الشبكة. وينبغي أن تقيم البيانات بدلالة نمـــــاذج الحركـــــة، بعد ذلك تنفذ التحليلات اللازمة عن الأمن المقترح.

- **رصد الشبكة عن بعد:**

يمكن استخدام بروتوكـول "رصد الشـبكة عن بعـد" RMON (Remote Network Monitoring) كمجس ((Probe يستطيع تجميع المعلومـات حـول مصـفوفة حركة مـرور البيانـات بين المصـدر والهـدف لعنـاوين الوصول الشبكية. عندما نريد وضع أمن عناوين الوصول الشبكية، فـإن هـــذه المعلومـــات يمكن تحليلها بســـهولة كي تـــؤدى وظيفة الأداة المتقدمة. مع ذلك، إذا أردنا تنصيب مرشح حـزمي مـركب في عنـاوين مستوى الشبكة وأنواع التطبيق، فـإن معلومـات RMON ربما لا تـؤدي الوظيفة.

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

توجد بعض التقنيات البرمجية من قبل شركات موردة، تسـتطيع إجـراء حسابات نماذج حركة مرور البيانات عبر الشبكة. تسمح هـذه التقنيـات النوعية لجهاز الشبكة أن يحسب عدد حزم البيانات والحروف المرسلة

بين نظـامين في كل مسـتوى شـبكي للـبروتوكول المسـتخدم (مثل بروتوكـول IP، بروتوكـول IPX). إذا اسـتطاعت الأداة المتقدمة تحديد الجهاز الذي يطبق معايير الأمن، أن به هـذه الخصـائص، فتسـتطيع هي الاستفسار عن هذه المعلومات من قاعدة بيانات نظام إدارة الشبكة.

- **تحليل مرشحات الحزم:**

إن المشكلة الأخـرى المتعلقة بتنفيذ الأداة المتقدمـة، هي عملية تحليل مرشحات الحـزم المقترحة المصـاحبة لأجهـزة الشـبكة. إن كل شـركة موردة لجهاز، يوجد لها طريقة منفـردة لتهيئة مرشـحات الحـزم، وهـذا يجعل أداة تحليل هـذه المرشـحات الحزمية مهمة صـعبة. وتوجد بعض التطبيقـات في إدارة الشـبكة، بها خصـائص لتحليل مرشـحات الحـزم. ولكن هـــذه التحليلات ليست مخصصة عـــادة لفحص حركة نمـــاذج البيانــات، وتكــون هــذه ضــرورية ولو لإنشــاء إصــدار محــدود للأداة المتقدمة.

5. تـــــدوين حـــــوادث الأمن في الشبكة

إن سجلات الفحص التي تلخص تدوين معلومات الأمن تكون حرجة في تحقيق إدارة الأمن. لكن بمعاونة التطبيقــات الــتي تجــري عمليــات الإدخال في سجل الفحص، نستطيع تحديد النماذج ((Patterns التي تبين تهديد نقاط الاتصال، ومن ثم توقيف الاتصالات غير المسـموحة. أيضـا، مثلما يحدث في تطبيقات الوقت الفعلي، فإن مثل هـذه البيانـات يمكن أن تسـاعدنا في إيجـاد الطلبـات الغـير مسـموحة الـتي تنتج عن سـوء التهيئة.

مثال: الاحتياطات الأمنية عندما يغادر مسئول إدارة الشـبكة المؤسسة:

نفترض أن مهندس الشبكة، المسـئول عن إدارة وتهيئة شـبكة البيانـات يخطط لمغادرة المؤسسة من أجل العمل في مؤسسة منافسة أخرى.

الخطوة الأولى: للتعامل مع هذا الوضع، تكـون بإزاحة هـذا الشـخص فورا من الوصول الفعلي إلى مباني المؤسسة، أو أي مكان يمكنه فعليا الوصـول إلى المعلومـات الحساسـة. وهـذه الخطـوة قد تحتـاج تغيـير شفرات المفتاح وتغيير مفاتيح بطاقة الدخول.

الخطــوة الثانية: هي إزاحة حسـابات هـذا الشـخص من جميع نظم الحاسب. وبحسب الاعتماد على اتصالات الموظف السابقة، فـإن هـذه الخطوة يجب أن تتضمن أيضا تغيـير كلمـات السر ذات الامتيـاز (مثـل:

أصل المصدر ((Root، المشـرف (Supervisor)، مـدير النظـام System Manager) في جميع نظم الحاسبات، وأجهزة الشبكة.
الخطوة الثالثة: ينبغي أن يتم تغيير كلمات السر، وشفرات المفـاتيح في كل أجهـزة الشـبكة الـتي توصل المؤسسة إلى الشـبكة العامة (أو تلك الــتي يمكن أن توصل إلى العــالم الخــارجي)، مثل جميع أجهــزة المودم، أجهزة الشبكة، والحاسبات المضيفة في نظام الجدار الناري.
الخطوة الرابعة: يمكن تنصيب أداة إدارة الأمن، لمراقبة كل الأجهزة المتصلة بشبكة البيانات، عن الأمـاكن الـتي يسـتطيع الموظف السـابق الدخول من خلالها.
الخطوة الخامسة: يمكن أن يتم تشغيل برنامج يتم تصـميمه للبحث في الملفـات أو التطبيقـات الـتي ربما قـام بتغييرها الموظف السـابق، لإنشــاء ثغــرة أمنية في المســتقبل. إن البحث عن ملفــات تنفيذية أو ملفات قد تم تغييرها حديثا، هي مهمة يمكن تحقيقهـا، بواسـطة بـرامج عديدة كجـزء من عمل إدارة النظم (على الـرغم 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 سـجلات فحص مكثفـة، وإجـراء عمليـات توضع في أمـاكن لرصد الشـبكة. في هـذا الوضـع، فـإن سـجل فحص الأمن (على ما يبـدو في نظــام إدارة الشــبكة) يكــون مهما أيضــا. إن إنشــاء تطــبيق يمكن أن ينشىء سجل فحص، ليس صعبا، حيث يوفر كل تطبيق إدارة أمن الذي يجد محاولات اختراق تدخل نتائج البحث في قاعـدة بيانـات نظـام إدارة الشبكة.
على سـبيل المثـال، إن التطـبيق الـذي يكتشف محـاولات عديـدة غـير ناجحة للـدخول عن بعـد، يسـتطيع إضـافة مـدخل إلى قاعـدة البيانـات عندما يتم تنبيه مهندس الشبكة عن المشكلة. يمكن بعد ذلك، أن تقـوم قاعــدة البيانــات بتوليد تقــارير ملخصــة. على الــرغم من أن هــذه التطبيقات يمكن إتمامها ببساطة نسبيا، باستخدام بنـاء نظـام معمـاري صحيح لإدارة الشبكة، فإنه لا يجب المبالغة في فوائدها.
مثــال: تقرير عن محــاولات غــير صــحيحة لنقل ملفــات من شبكة مؤسسة:

نفـترض عينة من تقرير يـومي كما هو موضح في جـدول5.1، والـذي يوضح كيف يستطيع تطبيق إدارة الأمن، إحضار بيانات مفيدة لمهنــدس الشبكة. يحدد الجدول اثنين من أغلبية نقاط الاتصال، والمحاولات غـير ال صحيحة لنقل ملفات من أحد شـبكات المؤسسـة، الـتي وجـدت في هذا اليوم، وحاسب المصدر، واسم المستخدم عنـدما فشـلت المحاولة (إذا كان متاحـا)، والـوقت الـذي وقع فيه الحـدث. كما يـبين جـدول5.2 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 إجـراء تطبيقـات مماثلة تنتج بيانـات ذات صـلة لفـترات أطـول (أسبوع أو شـهر)، وهـذه التطبيقات تكـون أيضا حرجـة، بالنسـبة لإدارة الأمن في نظـام إدارة الشـبكة. بـإجراء مراجعة منتظمـة، فـإن هـذه

التقارير يمكن أن تساعد مهندس الشبكة، في الاحتفاظ بـأمن الشـبكة، وأن يكون على وعي ودراية باحتمالات اختراقات أمنية فعلية.

6. برامج تطبيقية لأمن الشبكة

يوجد حـــزم برمجية متعـــددة متـــوفرة على شـــبكة الانـــترنيت يمكن للمؤسسات التي تمتلك شبكات بيانات شراؤها وتنصـيبها لتحقيق إدارة أمن الشبكات في المؤسسة كما تم شرحه سابقا. نقدم، في هذا الجزء من الوحـــدة الدراســـية، بعض الـــبرامج المتاحة مجانا على شـــبكة الانترنيت، الـتي يمكن للـدارس تنصـيبها والتـدرب عليها وذلك لإكسـاب الدارس المهارات اللازمة التي تعينه وتمكنه من استخدام بعض وسـائل أمن الشبكات والحماية من المخاطر.

وأن يتدرب الدارس على كيفية استخدام هذه الـبرامج لحماية ملفـات العملاء على أجهزة الحاسـبات المتصـلة بشـبكة البيانـات. ونعـرض هنا مجموعة من أشهر هذه البرامج التطبيقية التي يمكن للدارس أن يقـوم بتحميلها من عنـاوين مواقع شـبكة الانـترنيت الموضـحة تباعا ومن ثم تنصيبها والتدرب عليها. وهـذه الـبرامج مهمة جـدا للحماية من مخـاطر 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

اســتخدام الحاســبات المضــيفة المفوضــة: ((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 NFS((Network File System:**

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 MAC (Medium Access Control).

توقف الحزم من الوصول إلى الحاسبات المضيفة غير الآمنة، قبل أن تصل إلى نقطة اتصال ربما تحتوي معلومات حساسة.

- **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 .

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

المصطلح بالإنجليزية	معناه بالعربية
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
Private Key	مفتاح الخاص
Probe	مجس
Polling	تصويت
Public Key	المفتاح العام
Process Status: ps	أمر تنفيذ حالة العملية
Unique	فريد
Network File System))NFS	نظام ملفات الشبكة
NetBIOS	نظام الدخل والخرج الأساسي للشبكة
One Time Password	مولد كلمة السر لمرة واحدة

المصطلح بالإنجليزية	معناه بالعربية
Generator	
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
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

rity, McGraw Hill,

lution/kahate

73



محتويات الوحدة

الموضوع	رقم الصفحة
المقدمة	**211**
التمهيد	**211**
أهداف الوحدة	**212**
1. فوائد إدارة الأداء	**213**
2. تحقيق إدارة الأداء	**215**
1.2 تجميع بيانات معدلات الاستخدام	**216**
2.2 تحليل بيانات الأداء	221
3.2 ضبط القيم الحدية	222
4.2 استخدام محاكاة الشبكة لفحص الأداء	223
3. إدارة الأداء في نظام إدارة الشبكة	**262**
4. تدوين معلومات الأداء في نظام إدارة الشبكة	**241**
5. برامج عملية للتدريب على قياس الأداء	**244**
الخلاصة	**246**
لمحة مسبقة عن الوحدة التالية	**247**
مسرد المصطلحات	**248**
المراجع	**252**

المقدمة

تمهيد

عزيزي الدارس مرحبا بك الى هذه الوحدة والتي بعنوان إدارة الأداء. تختص إدارة الأداء بضمان أن الخط السريع للشبكة يظل غـير مـزدحم، ويمكن الوصول إليه. ويتم تحقيق ذلك من خلال:

- رصد أجهــزة الشــبكة والوصــلات المصــاحبة لها لتحديد معــدل 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 هــذه الوحــدة ، ســوف يتم شــرح فوائد إدارة الأداء، ومناقشة الخطـوات الأربعة الخاصة بتحقيق هـذه الفوائـد. بعد ذلـك، يتم وصف ثلاثة أدوات لإدارة الأداء، ويشـــمل ذلك الأداة البســـيطة، 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 الوحدة ينبغي 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.

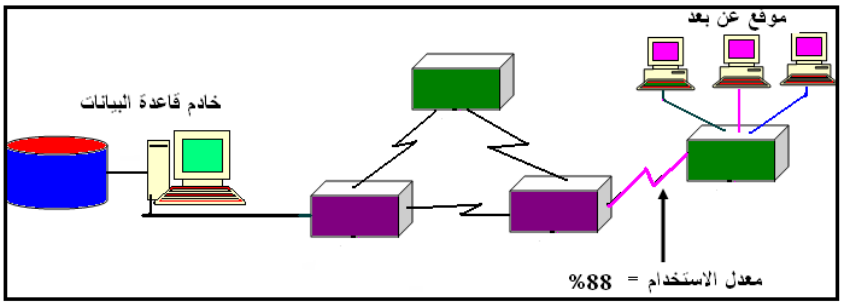
1. فوائد إدارة الأداء

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 غـير ملائمة على أداء الشـبكة. بهـذه الطريقة تستطيع إدارة الأداء أيضا المساعدة في تخطيط سعة الشبكة.

- **رصد معدل الاستخدام:**

تمثل عملية رصد معدل الاستخدام الحالي لأجهـزة الشـبكة والوصـلات نقطة حرجة في إدارة الأداء. تستطيع البيانات الـتي يتم الحصـول عليها معاونتنا في عزل مكونات شـبكة البيانـات الـتي اسـتخدمت بكثافة في الحـال، كما تسـاعدنا أيضا في إيجـاد أجوبة لمشـاكل الإجهـاد الأخـرى، وربما يعتبر ذلك الأكثر أهمية. على سبيل المثال، في الشبكة الموضحة في شكل 6.1، يشتكي المستخدمين من بطيء الاتصـال عن بعد إلى خـادم قاعـدة البيانـات الـذي قد ينتج من أسـباب متعـددة. قد تقع هـذه المشكلة في أي جهاز أو وصلة من المصدر إلى الهدف. تسـتطيع إدارة الأداء مسـاعدتنا بسـرعة في تحديد وصـلة بين الموقع البعيد وخـادم قاعدة البيانـات الـتي يكـون معـدل اسـتخدامها فـوق 80%، وهـذا 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:**

تسـتطيع تقنيـات إدارة الأداء مسـاعدتنا في فحص اتجاهـات الشـبكة. نسـتطيع اسـتخدام اتجـاه البيانـات للتنبؤ بالقيمة العظمي لمعـدل استخدام الشـبكة. وبالتـالي نتجنب الأداء الضـعيف الـذي يمكن أن ينتج عن تشبع الشبكة. على سبيل المثال، إذا علمنا متوسط زمن الاستجابة بين الوحدة الطرفية لمستخدم والحاسب الكبير Mainframe ، نستطيع تنصيب إجـراءات تجعلنا نعـرف مـتى يكـون زمن الاسـتجابة أطـول من اللازم. سوف نتعلم من خلال دراسة هذه الوحدة، أن أجهزة وتطبيقـات إدارة الشبكة، يمكن تنصيبها لإرسال تنبيهـات عنـدما يوجد مشـكلة أداء محتملة، أو عندما يتم اجتياز حد معرف لمستخدم.

يستطيع بروتوكول رصد الشبكة عن بعد RMON، تجميع معلومات عن قطاع الشبكة في الـزمن الفعلي، ويختـبر البيانـات عند جـدول فـترات زمنية (ربما كل خمسة دقــائق)، ويخـــزن البيانـــات التاريخية من أجل استرجاعها فيما بعد بواسطة نظام إدارة الشبكة. وهذه الإمكانية لجهاز رصد الشبكة عن بعد RMON ، هي أحد الأمثلة علي استخدام بيانـات الشبكة في الزمن الفعلي من أجل اتجاه تحليلي طويل الأجل.

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

نسـتطيع أيضـا، رسم معـدل الاسـتخدام للشـبكة مقابل الـزمن، وذلك لتحديد أوقــات ذروة الاســتخدام. وبمعرفة ذلــك، نســتطيع جدولة نقل البيانـات الضـخمة إلى أوقـات عـدم الازدحـام. في كثـير من شـبكات البيانـات، يقـوم المسـتخدمين بجدولة انتقـالات البيانـات الضـخمة إلى أوقات يكون عندها؛ على ما يبـدو؛ اسـتخدام الشـبكة منخفض، مثلا عند منتصف الليل أو وقت تناول الغـذاء. على الـرغم من أن عـدد قليل من المستخدمين ربما تلاحظ وجود مشكلة في هذا التوقيت، فإن استعمال الشبكة يمكن أن يصل في الحقيقة إلى معـدل اسـتخدام عـالي وعـادل بعد ذلك.

- **تخطيط السعة Capacity Planning**:

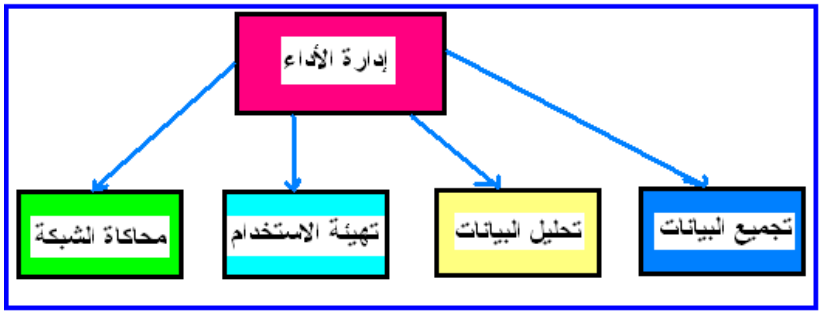
يفيد تخطيط السعة كل من المستخدمين ومهندس الشبكة. باســتخدام معلومات إدارة الأداء، يسـتطيع مهنـدس الشـبكة تحديد السـعة الحالية للشبكة بواسطة اسـتخدام بروتوكـول إدارة الشـبكة لتجميع معلومـات عن كل الحــروف المرسـلة والمسـتقبلة في الوحـدة البينية للشـبكة. ويعطي إجمالي عدد هذه الحـروف حجم الشـبكة Network Volume . وعند إجراء هذه العمليـة، ينبغي تجنب عـدم عد نفس البيانـات مـرتين. في مثل هذه الحالة، يمكن إجراء عملية عد الحـروف عند أمـاكن يكـون فيها حركة مرور البيانـات متزنة عند نقـاط وصـول منفـردة للهـدف (أو الأهـداف Destinations). وبعد معرفة السـعة الحالية للشـبكة، نسـتطيع 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 الحـالي لأجهـزة ووصـلات الشبكة.
2- تحليل البيانات ذات الصلة.
3- تهيئة حدود الاستخدام.

4- محاكاة الشبكة.



شكل6.2 الوظائف الواجب تحقيقها بواسطة إدارة الأداء.

1.2 تجميع بيانـــــات معـــــدلات الاستخدام

إن تحديد معدل استخدام جهـاز الشـبكة ليس عـادة مهمة مباشـرة، إن كل نـوع جهـاز ربما يكـون له خصـائص مختلفة تحـدد الاسـتخدام. على الرغم من أننا نوفر بعض معايير الاستخدام الشـائعة، ينبغي علينا العمل مع مـورد الأجهـزة. على سـبيل المثـال، إن **معدل اسـتخدام خـادم الملفـات** ربما من المفضل أن يتم قياسه بواسـطة تحميل المعـالج، ومعـدل الوصـول للقـرص، ومعـدل اسـتخدام كـارت الوحـدة البينية للشبكة. إن المعالج المشـغول ربما يحقق مهـام بطيئة للمسـتخدم، إن القرص الذي يتم الاتصال به باستمرار ربما يقـرأ ويكتب ملفـات جديـدة أكثر بطأ من المطلـوب، وأن كـارت وحـدة بينية مشـغول للشـبكة ربما يبطئ الوصول إلى الشبكة.

يمكن قياس **معدل الاستخدام لجهـاز موجه أو قنطـرة** بواسـطة معدل تدفق الحزم، حمل المعالج Processor Load، نسبة الأطر Frames المرسلة لكل وحدة بينية، وعدد الحـزم المخزنة في الانتظـار. إن هـذه الأجهـزة من الأفضل أن يتم قياسـها بواسـطة فحص معـدلات الإرسـال مقابل مقدرتها علي الإرسال في حوار شـبكي معطى، بسـبب أن هـذه الأجهزة يمكنها معالجة الأطر بسـرعة أعلى من الـتي تسـتطيع توفيرها الوصلات المصاحبة.

إن **معالج الشبكة** عـالي التحميـل، يـبين لمهنـدس الشـبكة أن الجهاز يكـون له زمن توقف Idle Time ضـئيل. إن الاحتفـاظ بمعـالج الجهـاز مشغولا لا يسبب عادة مشكلة، إلي أن يصـبح الجهـاز مشـغولا 100% من الوقت ولا يستطيع الاستمرار في معالجة حركة مرور الشـبكة. في

هذه الحالة، فإن معدل الاستخدام المرتفع لهـذا الجهـاز ينتج عنه حـذف حـزم البيانـات، وهـذا يجـبر نظـام المصـدر على إعـادة إرسـالها (ومن المحتمل أن يجعل مشكلة الأداء أسوأ). إذا كان الجهاز يستطيع معالجة الحزم ولكنه يحتاج تخزينها في طابور انتظار، فـإن هـذا أيضا يـؤثر على الأداء الكلي للشـبكة. إن الجهـاز الـذي ينتظر عند وصـلة شـبكة ذات استخدام مكثف، أو وصـلة بها عديد من الأخطـاء، أو جهـاز شـبكة آخـر، يعاني مشاكل في الأداء.

ويمكن **تحديد معدل استخدام الوصلة** في الشـبكة بطريق أسـهل ، على الرغم من أن الوصلة ربما لا تستخدم بنسـبة 100%، فـإن نسـبة أقل من معدل اسـتخدام الوصـلة ربما يسـبب مشـاكل في الأداء. على سـبيل المثـال، تسـتطيع شـبكة إثـيرنيت احتـواء حركة مـرور بيانـات بمعدلات اسـتخدام عالية جـدا، لكن إذا زاد حمل حركة البيانـات العادية 40%، فإن القطاع ربما يسبب أداء رديء وسيء.

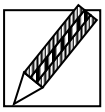
إن معـدل اسـتخدام الوصـلة هو عبـارة عن مجمـوع كمية المعلومـات المرسلة في الثانية والمستقبلة في الثانية مقسومة علي سعة النطـاق الكلية المتاحة (التي تكون أيضا بوحدة معلومات في الثانية).

$$\text{نسبة معدل الاستخدام} = \frac{(\text{إجمالى عدد المعلومات المرسله} + \text{إجمالى عدد المعلومات المستقبله})}{\text{سعة النطاق}}$$

إن هـــذه المعادلة لا تســـتخدم لوصـــلات التـــوالي ذات الإرســـال في الاتجاهين Full Duplex ، التي تستطيع إرسال واستقبال معدل نطـاق الإرسـال الكامل في كلا الاتجـاهين في نفس الـوقت. وهـذا يعـني أن معـدل الاسـتخدام يسـتطيع حسـاب 200%. لهـذا ينبغي أن نسـتخدم المعادلة التالية بدلا من المعادلة السابقة، والـتي تحـدد القيمة العظمي للمعلومات المرسلة في الثانية والمعلومـات المسـتقبلة في الثانية كما يلي:-

$$\text{نسبة معدل الاستخدام} = \frac{\text{القيمه العظمى}(\text{إجمالى عدد المعلومات المرسله} ، \text{إجمالى عدد المعلومات المستقبله})}{\text{سعة النطاق}}$$

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.

- **ق**

لقيــاس ت
التالية:
أولا:-
ثانيا:-
ثالث:- الإتاحة Availability.

أولا: إجمالي زمن الاستجابة:

يعرف إجمالي زمن الاستجابة بأنه الفترة الزمنية الـتي تأخـذها 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 حـرف من وحــدة المفــاتيح إلي لحظة انتقــال المعلومة إلي حاسب الهــدف بالشــبكة وعــودة الاســتجابة إلى الوحــدة الطرفية المحلية للحاسب المصدر.

إن العديد من بروتوكــولات طبقة النقــل، مثل بروتوكــول التحكم في الإرســال القياسي بين الشــبكات TCP، يمكن أن تقيس زمن دورة الرحلة Round-Trip Time بـالملي ثانية لكل معلومة اسـتدلالية ترسل من المصدر إلي الهدف لأغراض التحكم في التدفق. يمكن أن تستخدم هذه القيمة للحصول علي قيمة تقريبية جيدة لإجمـالي زمن الاسـتجابة. إن الفترة الزمنية لـدورة الرحلة سـوف لا تطـابق تماما الفـترة الزمنية الإجمالية لــزمن الاســتجابة، بســبب أن مســتوي النقل في الشــبكة يسـتقبل المعلومة الاسـتدلالية قبل أن يقـوم التطـبيق بمعالجتهـا، وأن

عملية معالجة التطـبيق سـوف تضـيف وقتا إضـافيا. بغض النظـر، فـإن زمن الرحلة يمثل جزء مهم من إجمالي زمن الاستجابة.

ثانيا: معدل الرفض:

يعرف معدل الـرفض بأنه النسـبة المئوية للـزمن الـذي لا تسـتطيع فيه الشبكة نقل المعلومات، بسبب نقص في المصـادر وفي الأداء. لقيـاس معدل الرفض، يوجد العديد من الأجهزة تسجل عدد المحـاولات لإجـراء اتصـال ، وإجمـالي عـدد الاتصـالات الـتي تمت ، ونحصل علي النسـبة المئوية لمعدل الرفض بواسطة قسمة عدد الاتصـالات الـتي تمت على إجمالي عدد محاولات الاتصـال. في حـالات كثـيرة، عنـدما تكـون 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 الإخفـاق MTBF(Mean Time Between Failure) . وكـذلك متوسط زمن اللازم للإصلاح MTTR، و تبين المعادلة التالية طريقة حساب الإتاحة (A):

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

و يمكن قيــاس الإتاحة من الناحية النظريــة، حيث أن معظم مــوردين الأجهـزة تقـوم بتوفـير قيم لهـذه القياسـات. من الناحية العمليـة، فـإن معظم موردين الأجهزة تستطيع أن تخبرنا عن المدة التي تسـتطيع فيها هــذه الأجهــزة أن تظل في العمل (العمر الافتراضي للجهــاز). بمقارنة هذه القيمة، بالمدة الزمنية الكلية المنقضية منذ كان الجهـاز أو الوصـلة في الخدمــة، يعطينا قيمة الإتاحــة. ويوضح الجــدول 6.1، أمثلة عددية لحساب قيمة الإتاحة بمعلومية كلا من MTBF، وقيمة MTTR.

الجدول 6.1: أمثلة عددية لحساب قيمة الإتاحة.

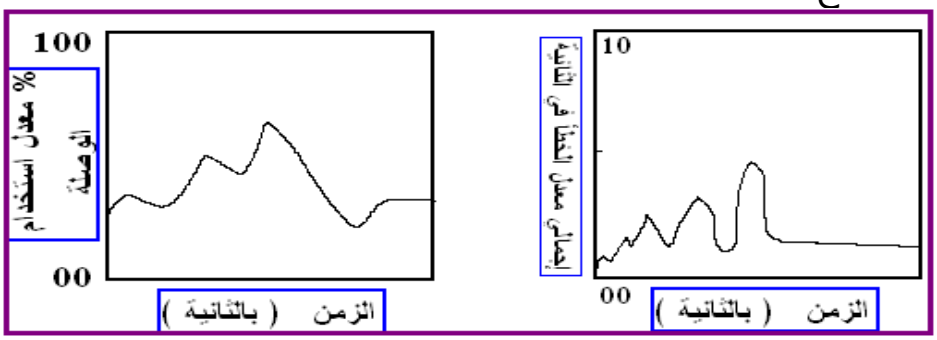
Availab'ty	MTTR	MTBF
0.985	3.5	229.83
0.985	3.5	229.83
0.985	3.5	229.83
0.985	3.5	229.83
0.985	4	262.67
0.985	4	262.67
0.985	4	262.67
0.985	4	262.67
0.985	4.5	295.50
0.985	4.5	295.50
0.985	4.5	295.50

ونستطيع استخدام بروتوكـول إدارة الشـبكة لتجميع هـذه البيانـات من الشبكة. وهذه المعلومات ذات أهمية كبيرة من أجل تشخيص الأعطـال Troubleshooting وتحليلات تحديد الاتجاهات Trend Analysis.

2.2 تحليل بيانات الأداء

يمكن أن نحصل من نتائج تحليلات بيانات الشـبكة على رسـومات بيانية (خطية – قضبان) تعبر عن معدل استخدام جهاز الشبكة أو الوصـلة في الزمن الفعلي، أو من منظور تاريخي. وهـذه الرسـومات تكـون مفيـدة جدا في تحليلات الأداء. يمكن أن توضح الرسومات التحليلية في الزمن الفعلي حالات الاستخدام الحالية للشبكة، وكذلك الأخطاء الـتي تحـدث في الشبكة مقابل الزمن، كما هو موضح في الشكلين6.3 a,b . علي سبيل المثال، يمكن أن يظهر الرسم الوقت الفعلي الـذي يـبين العلاقة بين الحزم المرسلة مقابل معدل الأخطـاء، ويمكن الاسـتفادة من هـذه الرسومات في تحديد مشاكل الأداء في الشبكة. يمكن أيضا أن تسـاعد رسومات الوقت الفعلي في تشـخيص مشـاكل إدارة الشـبكة المتعلقة بمصادر الأجهزة والوصلات المصـاحبة لهـا: وقد يشـمل ذلك معلومـات عن الأجهزة مثل: استخدام الذاكرة – معدل استخدام المعـالج – معـدل الوصــول إلى قــرص التخــزين – عــدد الجلســات – الخ. وقد تشــمل

معلومات الوصلة: معدل الاستخدام – معـدلات الخطأ – النسب المئوية للخطأ – الخ.



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

إن الرسـومات الـتي تمثل معلومـات تاريخية عن الشـبكة لا تظهر حالة الشبكة الحاليـة، لكنها مفيـدة في توضـيح الاتجاهـات. إن بيانـات تحديد الاتجاه Trend Data ، تساعدنا في التنبؤ عندما تزيد طلبات مسـتخدم الشبكة عن سعة الوصلة أو الجهاز. وهذا يساعدنا في التخطيط لزيـادة سـعة الشـبكة أو إعـادة تصـميمها لتفي باحتياجـات المسـتخدمين. وتسـتخدم رسـومات المراحل التاريخية للشـبكة غالبا لفحص حالة الشبكة إما أسبوعيا، شهريا، ربع سنويا، أو سنويا، بحسب الاحتياجات.

توضح الرسـومات ليس فقط عمليـات الزيـادة أو النقصـان في معـدل الاسـتخدام لوصـلة الشـبكة، ولكن أيضا يمكن أن تسـتخدم لإجـراء إحصائيات مفيـدة، مثل معـدلات الخطأ في الوصـلة، ومعـدل اسـتخدام المعـالج لجهـاز معين، عند فـترات زمنية محـددة. عنـدما نلاحظ اتجـاه كمية الأخطـاء الـتي يعـاني منها أحد الأجهـزة، فـإن هـذا قد يمكنا من تشخيص المشكلة قبل أن تؤثر على الأداء. علي سـبيل المثـال، عنـدما نلاحظ أن أحد أجهزة الشـبكة، يقـوم ببطء بزيـادة قـدرة المعـالج الـتي يستخدمها مع الوقت، ربما نقـرر تقليل حركة التـدفق على الجهـاز قبل أن تصل قدرته على المعالجة إلى المستوي الحرج. أو كحل بديل آخـر، ربما نقوم بتحديث المعالج ونسـتخدم جهـاز ذو معـالج له قـدرة 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 الـتي تـؤثر على أداء الشـبكة. بخصـوص معـالج أو جهـاز الشـبكة، فـإن هـذه 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 الاستخدامUtilization – 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.

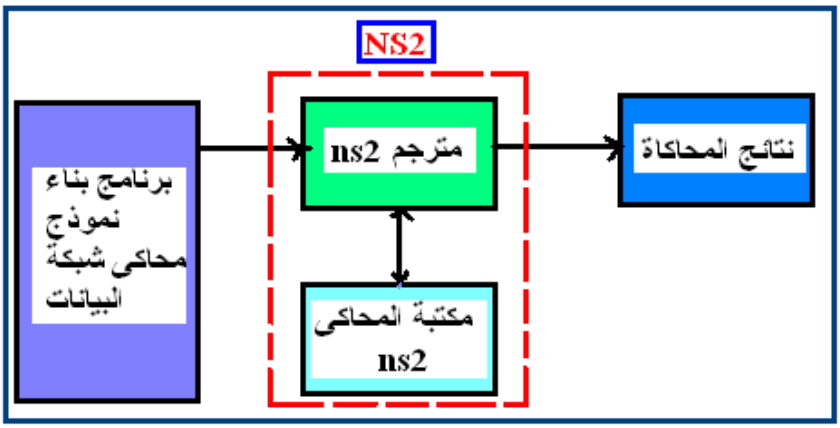
4.2 استخدام محاكاة الشبكة لفحص الأداء

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.

بـــالبحث أكـــثر، نجد أن بروتوكول طبقة النقل المســـتخدم بواســـطة التطبيق الجديد، يستخدم بروتوكول توقف-ثم-انتظر (Stop-and-Wait)، وهو بروتوكول ذو سعة نافذة تساوي حزمة واحدة (Window Size = 1 Packet). ويسـتخدم بروتوكـول طبقة النقـل، طريقة تحكم في التـدفق الــتي ترسل حزمة واحــدة لكل جلسة Session ، ثم ينتظر حــتى يتم وصول الرد Acknowledge ، قبل أن يتم إرسال حزمة البيانات التالية. إن وجود سعة نطاق أكبر لوصـلة الموقع البعيد للشـبكة سـوف يسـمح بإرسال أكثر من حزمة بيانات في نفس الوقت، لكن ذلك لن يـؤثر على زمن التأخير الإجمالي الذي يراه مستخدمين الشبكة.
لذلك فـإن تحـديث الوصـلة لن يحل مشـكلة زمن الاسـتجابة الضـعيف. باستخدام تطبيق محاكاة دقيق للشـبكة، وبروتوكـول طبقة النقـل، قبل أن يتم تحـديث الوصـلة، قد يسـاعد مهنـدس الشـبكة في الكشف عن الإخفـاق المصـاحب لـبروتوكول طبقة النقـل. إن الحل المناسب لهـذه المشكلة هو أن يستخدم التطبيق مخـزن مكـدس بروتوكـولي Protocol Stack مصاحب لبروتوكول طبقة النقل الذي يستخدم طريقة تحكم في التدفق ذات حجم نافذة أكبر من واحد في شبكة البيانات الإقليمية.

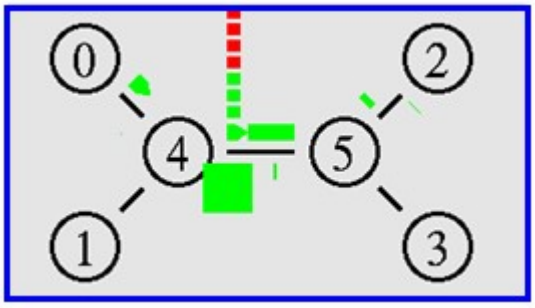
- **برنامج محاكي الشبكة:**

يمكن استخدام برنامج محاكي الشبكة Network Simulator المعروف باسم ns ، والذي تم تطويره بواسـطة مؤسسة بـركلي، وهو يسـتخدم لمحاكاة برتوكولات الشبكات UDP ، TCP ، IP ، وكذلك الشبكات التي تعمل معهـا. ويوجد منه متـوفرا في الأسـواق إصـدارين ، أحـدثهم هو الإصـدار الثـاني ns2. يتم كتابة برنـامج بنـاء نمـوذج محاكـاة الشـبكة باستخدام لغة C++ ، أو لغة OTcl وهي لغات مبنية باستخدام تقنيات الكائنات Object Oriented. يوضح شكل6.4 المكونات الأساسـية لهـذا 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 نظـام إدارة الشبكة

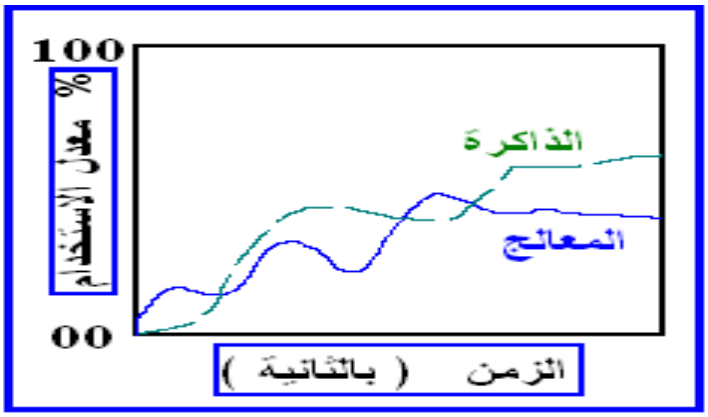
يختص إدارة الأداء في نظـــام إدارة الشـــبكة، باســـتخدام أدوات ذكية تسـتطيع فحص حالة الشـبكة من منظـور تـاريخي، وكـذلك من منظـور الـزمن الفعلي. وتعتمد فاعلية إدارة الأداء علي مسـتوى الأداة المتاحة لمهندس الشبكة.

3.1 الأداة البسيطة لفحص الأداء

ينبغي أن توفر أداة إدارة الأداء البسيطة معلومات الزمن الفعلي حـــول أجهزة الشبكة والوصلات، ويفضل أن تكون هذه المعلومـات في شـكل رسـومات بيانية كـالخطوط والقضـبان. تسـتطيع هـذه الأداة مسـاعدة مهنـــدس الشـــبكة في إيجـــاد الاختناقـــات في الشـــبكة Network Bottlenecks، ومن ثم عزل مشاكل الأداء.

نستطيع رسم الإحصـائيات المتاحة من الشـبكة، باسـتخدام بروتوكـول إدارة الشـــبكة، وهـــذا يعطينا مرونة كبـــيرة عنـــدما نحـــاول تحليل أداء الشـبكة. سـوف تـوفر أيضا الأداة البسـيطة وسـيلة لإيجـاد المعلومـات الأساســية عن الجهــاز أو الوصــلة، دون أن نضــطر لمعرفة تفاصــيل معلومات إدارة الشبكة. في حالات كثـيرة لا نحتـاج معرفة كل تفاصـيل عن معلومات أجهزة الشبكة (حيث أنها تكـون معلومـات ضـخمة)، نريد فقط أن نعرف كيفية أداء الجهاز.

وتوفر الأداة البسيطة وسيلة سهلة لأجهـزة الشـبكة، مثل الضـغط علي زر مفتاح أو بند في قائمة، لتجميع بيانات عن معـدل اسـتخدام المعـالج والـذاكرة. إن معـدل الاسـتخدام المرتفع للمعـالج يعـني أن الجهـاز لا يستطيع معالجة حركة مرور البيانات في الشبكة. بينما معدل استخدام الذاكرة (المكثف) قد يعـني أن الجهـاز يقـوم بتخـزين كمية ضـخمة من المعلومات في الذاكرة. يوضح لنا الـزمن الفعلي لهـذه القيم مشـاكل الأداء المحتملة للجهاز، كما هو مبين في شكل 6.6 .



شكل 6.6 مقارنة بين أداء معدل استخدام الذاكرة، والمعالج.
في وصـــلات الشـــبكة، يمكن أن توضح لنا الأداة البســـيطة، معـــدل الاسـتخدام الحـالي، ومعـدلات الخطـأ. على سـبيل المثـال، إن الرسم الذي يبين علاقة الحزم في الثانية والمعلومات في الثانية للوصلة يكون مفيدا في توضيح إجمالي أداء الوصلة. يعتبر معدل الاسـتخدام الحـالي لوصلة الشبكة الذي يتم توضيح قيمته على الرسم مفيـدا، ويتم حسـابه بواسـطة قسـمة معـدل المعلومـات في الثانية للوصـلة، على القيمة العظمي للمعلومات في الثانية. في حالة تشـخيص الأعطـال قد نحتـاج فحص عـــدد الأخطـــاء في الوصـــلة، مقابل كمية البيانـــات الصـــحيحة المرسلة. تسـتطيع الأداة البسـيطة تمثيل هـاتين القيمـتين على الرسم وإنشاء النتائج الضرورية.

ويوجد العديد من الأدوات المتـوفرة في الأسـواق تـؤدي وظـائف الأداة البسـيطة. معظم بـرامج إدارة الشـبكة تسـمح بإنشـاء رسـومات في الزمن الفعلي للمعلومات المتاحة من جهـاز الشـبكة. بالإضـافة إلى أن تطبيقـــات إدارة الشـــبكة، يتم تصـــميمها بواســـطة المـــوردين لتعطينا رسومات تعبر عن الحالة الصحية للجهاز.

2.3 الأداة المركبة لفحص الأداء

تستطيع الأداة المركبة أن تسمح لمهندس الشـبكة، بتهيئة القيم الحدية لمعدل الاسـتخدام ومعـدلات الأخطـاء. إذا زادت المعـدلات الحدية عن المسموح في الشبكة، فإن الأداة المركبة تسـتطيع تحقيق اتخـاذ فعـل. تستطيع هذه الأداة أيضـا، تجميع معلومـات الـزمن الفعلي وتخزينها في نظام إدارة قاعدة البيانات، كي نستطيع استخدامها في إجراء دراسـات تاريخية، وإنشاء رسومات لرؤية أداء الشبكة عند فترات سابقة.

- **القيم الحدية:**

إن ضـبط القيم الحدية الـتي تسـتطيع تشـغيل أعمـال لاحقـة، تعطي مهندس الشبكة وظائف اعتباريـة. سـوف تمكنا الأداة من تحديد حـدث بسيط، مثل حدوث إنذار ،أو وميض ضوئي، أو حدث متقدم مثل تشغيل الدوائر الاحتياطية، أو إرسال بريد الكتروني. علي سـبيل المثـال، يـوفر مفتـــاح الخدمة المتكاملة ISDN دوائر ذات ســـعة نطـــاق مرتفع عند

الطلب، باستخدام مودم خاص. وكلفة هذه الـدوائر تعتمد على الـوقت، وهذا يجعل هذه الدوائر اقتصادية. تستطيع الأداة اسـتخدام هـذه التقنية لطلب الدوائر، بنـاء على معـدل الاسـتخدام، ومعـدلات الخطـأ، أو تهيئة القيم الحدية بواسطة مهندس الشبكة.
تمثل القيم الحدية وظيفة حيوية للأداة المركبـــة، ويمكن لمهنـــدس الشـبكة أن يقـوم بتحديد القيم المثلى لهـذه الوظيفـة. تسـتطيع الأداة المركبة أن تحظرنا من وجود حالات تخطي لهذه القيم الحديـة، وكـذلك الأوضـاع الـتي تقـترب من القيم الحديـة. على سـبيل المثـال، يمكن تشغيل الأداة كي ترصد معدل استخدام معالج جهاز الشبكة. بفرض أنه في مكـان معين في الشـبكة أن أحد الأجهـزة يـؤثر على أداء الشـبكة، وكـان معـدل اسـتخدام المعـالج 90% من السـعة الإجماليـة. إن الأداة يمكن أن يتم تهيئتها، كي تنبهنا عندما يصل معدل استخدام المعـالج إلي 80% من القيمة الحدية، وبـذلك تسـمح لنا بفحص حـدوث مشـكلة في أداء الشبكة.

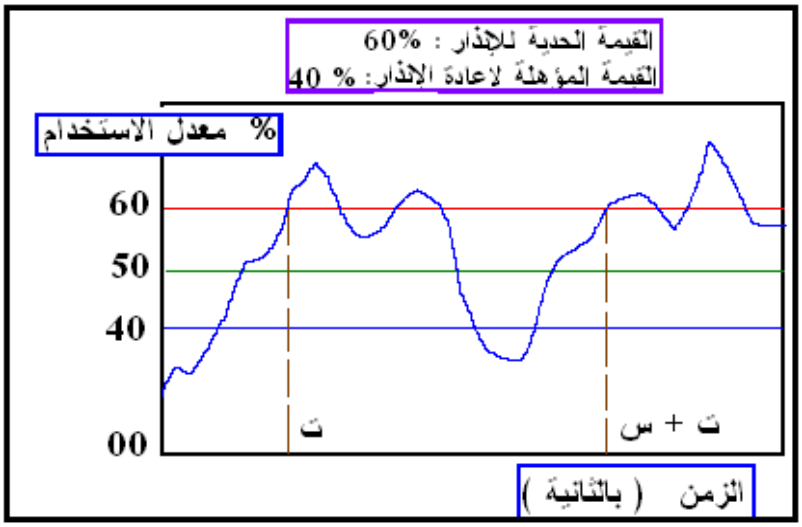
ينبغي للقيم الحدية أيضـا، أن تحتـوي على أولويـات للملاحظات. يوجد على الأقل ثلاثة مســتويات من الملاحظـــات هي(عـــالي – متوسط – منخفض). إن الأولوية العالية تبـــــدي عن الأولوية المتوســـــطة، وأن الأولوية المتوسـطة بـدورها تبـدي عن الأولوية المنخفضـة. تعطي لكل أولوية لون ممـيز في خطة الشـبكة، أو سـجل الحـدث في نظـام إدارة الشـبكة. في بعض الأحيـان، يمكن أن تنتج نفس الأولوية للقيم الحديـة، عند مواقع مختلفة داخل الشـبكة. على سـبيل المثـال، بفـرض انه تم تهيئة القيم الحدية لرصد معـــدل اســـتخدام الوصـــلة. إذا زادمعـــدل اسـتخدام الوصـلة عن 40%ـ ، فـإن الأداة تجتـاز الأولوية المنخفضة للقيمة الحديـة. وأن معـدل اسـتخدام 65% يجتـاز الأولوية المتوسـطة للقيم الحدية، وأن معـدل اسـتخدام 75% يجتـاز الأولوية العالية للقيمة الحدية.

نفترض بعد ذلـك، في مرحلة لاحقـة، أنه قد تم تهيئة قيمة حدية أخـري، لمراقبة معدل استخدام الـذاكرة لجهـاز. إذا قلت الـذاكرة المتبقية في الجهاز عن 100 كيلوبايت، تقوم الأداة المركبة بإعلان أن القيمة الحدية وصلة للأولوية العالية. خلال دقائق من اختيار معـدل اسـتخدام الوصـلة للقيمة الحدية للأولوية المتوسـطة، فـإن القيمة الحدية للأولوية العالية للـذاكرة يتم اجتيازهـا. تحتـاج الأداة المركبة الآن أن تحتفظ بقائمة لكل القيم الحدية الزائدة للجهاز، وأن تعرضهم على مهندس الشـبكة حسب الأولويـة. إذا اسـتخدمت الأداة المركبـة، خريطة الشـبكة لعـرض القيم

الحدية الزائدة الحالية للجهاز بلون واحد، فإن هذا لا يصلح. لذلك يفضل تخصيص لون مختلف لكل أولوية.

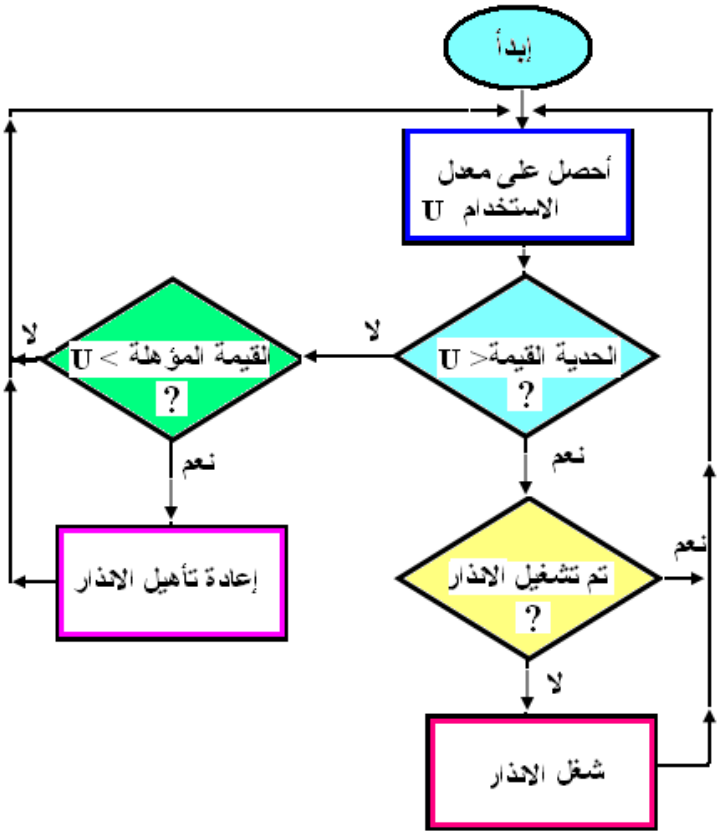
- **القيم التأهيلية Re-arm Values**:

ينبغي علي الأداة أيضـــا، أن تكـــون قـــادرة على تأهيل Re-arm القيمة الحدية بالسلوك المعقـول، ويتم عمل ذلك بواسـطة إعـادة تأهيل القيم الحدية بقيم تسمي "القيم التأهيلية". علي سبيل المثال، نفترض أنه تم حدوث إنذار عندما وصل معـدل الاسـتخدام إلي القيمة الحدية 60%ـ ، بعد لحظة متأخرة، توقف الإنذار عندما قل معدل الاستخدام إلي 58%، بعد مـرور ثـواني قليلة لاحقـا، عنـدما وصل معـدل الاسـتخدام 61%، حـدث الإنـذار مـرة أخـرى. لمنع هـذا الفـائض المـزعج المتتـالي من الإنذارات المتعددة، ينبغي ضبط الأداة بحيث عنـدما تصل القيمة الحدية في المرة الأولي، فإن الأداة تحدث الإنذار. لاحقـا، فـإن الأداة ينبغي أن تؤهل القيمة الحدية فقط عنـــدما يقل معـــدل الاســـتخدام عن القيمة المعرفة، مثلا 40%، كما هو موضح في شـكل 6.7 . بهـذه الترتيبـات، تقوم الأداة بإعطاء صوت إنذار عندما يتم اجتياز القيمة الحدية، وسـوف يتم إصدار إنذار آخر فقـط، عنـدما يقل معـدل الاسـتخدام عن 40%ـ ، وزاد بعد ذلك مرة أخرى فوق 60%. توضح خريطة التـدفق شـكل 6.8 هـذا المثـال. يمكن أيضـا، ضـبط الأداة كي تسـتخدم نفس الأسـلوب 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

؟

قـــــارن بين كلا مما يلي، موضـــــحا تأثيرهما على أداء الشبكة:

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

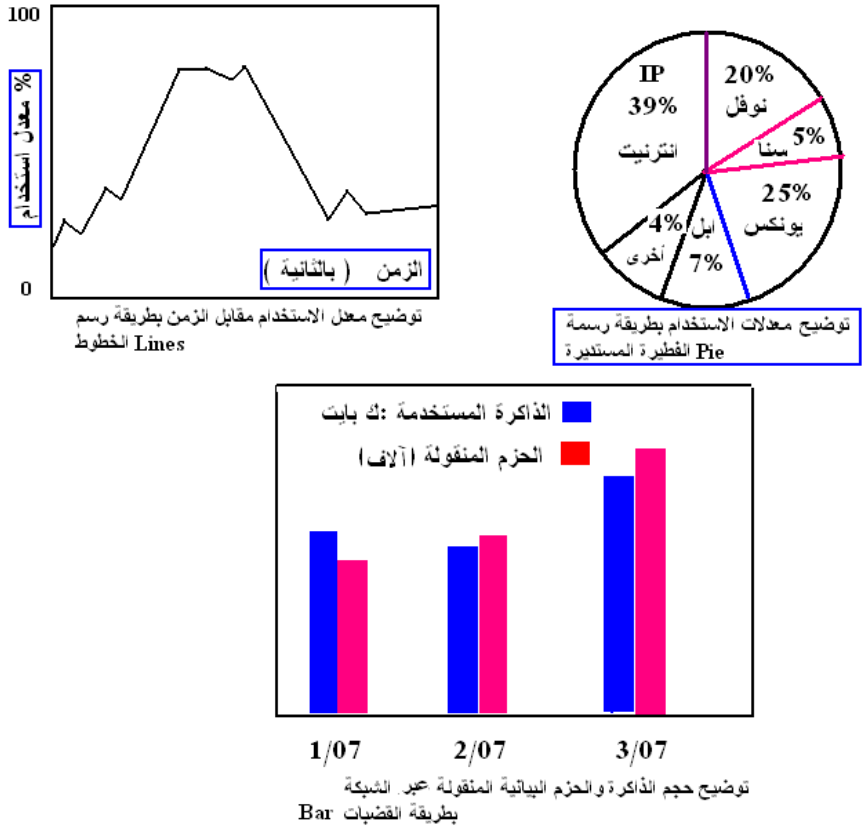
2- القيم الحدية Threshold Values، والقيم التأهيلية Re-arm Values.

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

ينبغي أيضـــا، أن تســـتطيع الأداة المركبة رسم البيانـــات التاريخية الموجودة في نظام إدارة قاعدة البيانات والخاصة بإدارة الأداء. عنــدما تعــاني شــبكة البيانــات من مشــاكل في الأداء، فإنه غالبا لا يســتطيع 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 الأوضـاع، فـإن الرسـومات الـتي توفرها الأداة البســيطة في الــزمن الفعلي لا تســاعدنا كثــيرا. لكن بواســطة القـدرة على اسـترجاع المعلومـات الضـرورية ، وبعد ذلك فحصـها في شــكل رســومات بيانيــة، تســتطيع مســاعدتنا في حل هــذا النــوع من المشاكل بشكل صـحيح. ينبغي على الأداة إنشـاء رسـومات بيانية علي شكل خطوط Lines – قضبان Bars – شكل مستدير

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

تفيد الرســومات الخطية عند فحص اتجاهــات البيانــات، مثل معــدل الاستخدام. تكون الرسومات القضـبانية أكـثر فاعلية عند إجـراء مقارنة القيم مثل حجم الذاكرة المستهلكة في جهاز الشبكة مقابل عـدد حـزم البيانــات الــتي يتم معالجتهــا. تكــون الرســومات البيانية علي شــكل مستديرفائدة كبيرة خاصة عند توضيح النسب المئوية للقيم، مثل أنـواع 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

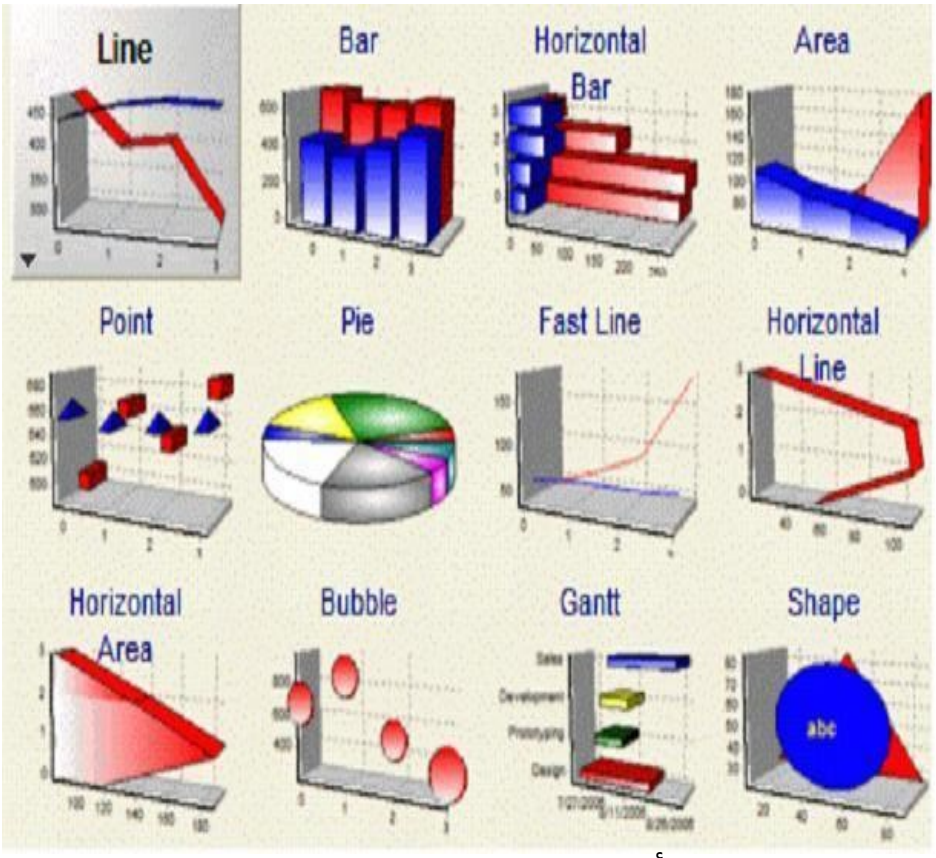
توضيح معدلات الاستخدام بطريقة رسمة الفطيرة المستديرة Pie

توضيح حجم الذاكرة والحزم البيانية المنقولة عبر الشبكة بطريقة القضبان Bar

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

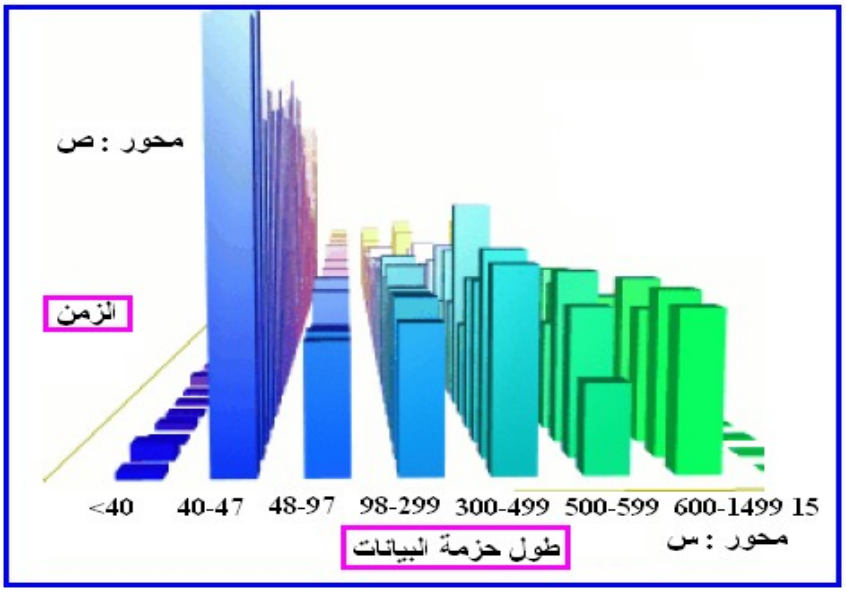
- **الرسومات المجسمة (ثلاثية الأبعاد):**

لقد تطـورت طـرق عـرض الرسـومات البيانية الخاصة بقيـاس الأداء، بواسـطة أدوات إدارة الأداء المتطـورة، وهـذا يمكن أدوات إدارة الأداء من إنشـاء رسـومات مجسـمة ترسم في الأبعـاد الثلاثية 3Dimension Graphics ، ويوضح شـكل 6.10 نمـاذج من هـذه الأنـواع المجسـمة 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 نطـاق أطـوال حـزم بيانية Packet Sizes . ويمثل محـور ص ، انتشـار عينـات البيانـات Data Samples. يـبين كل قضيب منها عدد حـزم البيانـات الـتي تقع في جيب حـزمي محـدد 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 الـرفض، والإتاحة.

- **فحص البيانات التاريخية للشبكة:**

ينبغي على الأداة المتقدمة أن تكون قـادرة على اسـتخدام المعلومـات الموجـودة في قاعـدة البيانـات العلائقية لفحص حالة الشـبكة، عند أي فترة زمنية ماضـية، للبحث عن مشـاكل محتملة في الأداء وتسـاعد في تخطيط سعة الشبكة. لتحقيق ذلك فإن الأداة المتقدمة تحتاج أن تكون قادرة على الأتي:

1- تستقبل دخل المستخدم الـذي يعـبر عن حالة الشـبكة ومشـاكل الأداء.
2- تستقبل المعلومات من قاعدة البيانات.
3- تحلل حالة الشبكة.

تتطلب الخطوة الأولي لهذه العمليـة، أن يتم إخبـار الأداة عن المـدة الزمنية الماضـية المطلـوب أن يتم عنـدها فحص بيانـات الشـبكة. وكــذلك أن يتم إخبــار الأداة عن الحاســبات المضــيفة والأجهــزة

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
```

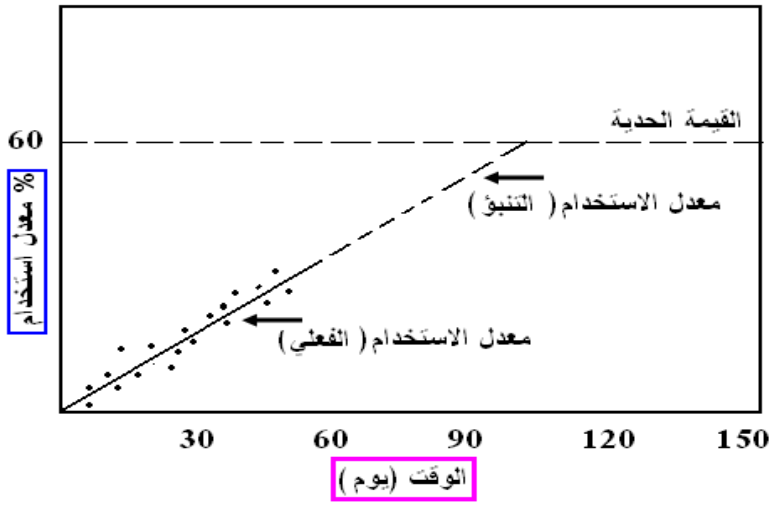
- **تخطيط سعة وصلات الشبكة:**

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.

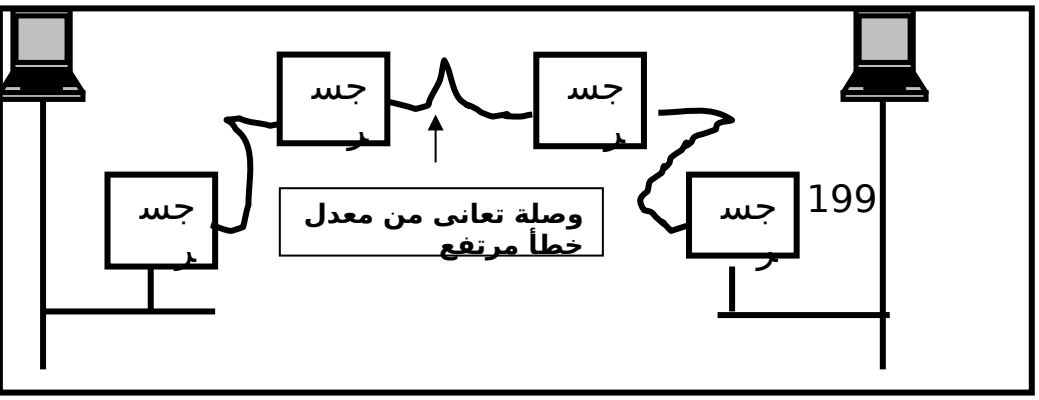


شكل6.12 يوضح اتجاه معدل استخدام الوصلة

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

يمكن للأداة المتقدمة أن تـوفر وقت مهنـدس الشـبكة، وإجـراء المساعدة في رسم النتـائج عن منـاطق الشـبكة الـتي تعـاني أداء غـير مقبول. (لاحظ أن هذه الأداة من المحتمل أن تستهلك كمية ضخمة من الـــذاكرة). لـــذلك ينبغي أن يتم تحـــدد كمية المعلومـــات التاريخية المطلوبة، لتوفير المساحة اللازمة لتخزينها.

مثال، نفترض إننا نستقبل دخل البيانات الذي يقوم المســتخدمين بنقله من الحاسـب"أ" إلى الحاسـب"ب"، وأن الأداء كـان يعـاني بطئا خلال أسبوع مضي. يوضح شكل6.13 تهيئة الشبكة لهـذا التطـبيق. يمكن أن تسـتخدم الأداة لتحليل جـزء من الشـبكة الـذي يوصل الحاسـبين "أ" ، "ب" . دعنا نفـترض أن التحليل يـبين تزايد تـدريجي لمعـدل الخطأ في الوصلة التي تربط القنطرتين على المسارين بين الحاسبين "أ" ، "ب". وأن معـدل الخطأ هـذا قد ازداد بدرجة كافيـة، لكن ليس بالدرجة الـتي تؤدي إلى تشغيل إنذار تخطي القيمة الحديـة. تسـتطيع الأداة المتقدمة إنشاء رسم بياني خطي يوضح تقدم معدل الخطأ، وهذا يمكن مهنـدس الشبكة من مخاطبة مورد الجهاز وتدوين المشـكلة في التقريـر. بـذلك نلاحظ أن استخدام الأداة المتقدمة توفر الـوقت المسـتغرق 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

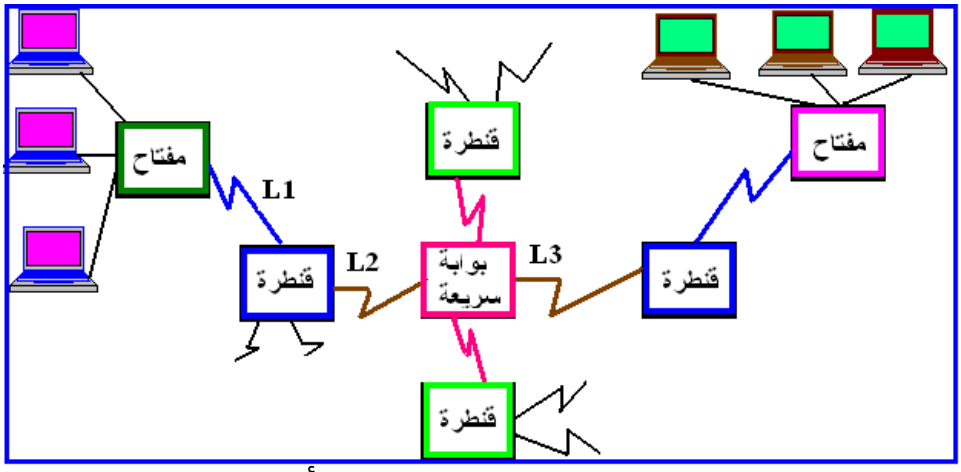
مختلفـة، بعد ذلك نجهز النمـوذج بعـدد الحاسـبات المضـيفة وأجهـزة الشبكة المناسبة.

إن هـذا الجـزء من الأداة المتقدمة تسـتخدم محاكـاة الشـبكة. بتوفـير نمــوذج محاكــاة جيــد، يمكن تحقيق التنبؤ بكل من الإتاحــة، معــدلات الرفض، وزمن الاسـتجابة. بـالطبع، إن هـذه الوظيفة يخصص لها نفس عدد الإنذارات مثل مكونات محاكاة الشـبكة. يمكن لمهنـدس الشـبكة، اسـتخدام الأدوات المتقدمة المتاحة في الأسـواق لإجـراء التطبيقـات السـابقة. كـذلك يمكن أن يقـوم هو بنفسه ببنـاء الأداة المتقدمة الـتي يمكنها تحقيق المحاكاة.

4. تــدوين معلومــات الأداء في نظام إدارة الشبكة

يوجد عـدة طـرق متاحة لتـدوين بيانـات الأداء. تعتـبر طريقة التـدوين النصي أشــهر هــذه الوســائل، حيث يمكن عرضــها على جميع أجهــزة الحاسـبات ويمكن طبعها بسـهولة. وهى تسـتخدم في إظهـار معـدل الاستخدام ومعدلات الأخطاء لأجهزة الشبكة. كمثال: يـبين جـدول 6.2 معدلات الاستخدام والخطأ للشبكة الموضحة في شـكل 6.14. ويكـون هــذا النــوع من التقــارير مفيــدا للحصــول على معلومــات إدارة الأداء لأجهزة الشبكة، كما يمكن توليد تقرير مماثل لوصـلات الشـبكة كما هو مبين في جدول 6.3 .

ويمكن أن يحتوي التقرير النصي على معلومـات قيمـة. لكن بسـبب أنه أيضا من المفيد التعبير عن معلومـات الأداء بواسـطة الرسـومات، فإنه من الناحية المثالية ينبغي أن تقوم البرامج بتحويل التقـارير النصـية إلى رسومات بيانية. إن معظم نظم إدارة الشبكة تـوفر طريقة للتعبـير عن البيانات بواسطة الرسـومات، وذلك باسـتخدام فورمـات رسـومية 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 تجــاوز القيمة الحدية. إن الصورة التي تعبر عن وجود أخطاء ناتجة عن مشكلة في وصلة الشبكة، التي تعاني معـدل خطأ ضـخم، يمكن أن يتم التعبـير 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. بـــرامج عملية للتـــدريب على قياس الأداء

يوجد العديد من الـبرامج المتاحة للتـدريب على قيـاس أداء الشـبكات، ويبين جدول6.6 بعض هذه البرامج المشهورة، الــتي يمكن تحميلها من شــبكة الانــترنيت والتــدريب عليهــا. وفيه يتضح مســمى البرنــامج واســتخدامه والموقع الــذي يمكن منه تحميل البرنــامج. معظم هــذه 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 الشبكة	/http://www.pathrate.org
pathrate	قياس سعة مسار capacity	/http://www.pathrate.org

	الشبكة	
Pchar	قياس سعة مسار capacity الشبكة	http://www.employees.org/~bmah/Software/pchar
sprobe	قياس اختناق سعة bottleneck 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 التـالي يوضح مسـمى الأداة العملية الـتي يمكن استخدامها لفحص
أداء الشـبكة.أكمل المعلومـات الـتي توضح استخدامات كل منهم؟

رقم الأداة	مسمى الأداة العملية (البرنامج)	استخدامه
1	iperf	.....
2	netperf	.....
3	nettimer	.....
4	pathload	.....

الخلاصة

عزيزي الدارس , تعرفنا في هذه الوحدة على إختصاصات إدارة الأداء بضمان أن الخط السريع للشبكة يظل غير مزدحم، وكـذلك تم تم تناول أمكانية الوصول إليه. و كيفية تحقيق ذلك من خلال:

- رصد أجهـزة الشـبكة والوصـلات المصـاحبة لها لتحديد معـدل 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 UDP ، TCP ، IP ، 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

المصطلح بالإنجليزية	معناه بالعربية
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
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

المصطلح بالإنجليزية	معناه بالعربية
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

محتويات الوحدة

الموضوع	الصفحة
مقدمة	**255**
تمهيد	**255**
أهداف الوحدة	**256**
1. فوائد إدارة الحسابات	**257**
1.1 استخدام إدارة الحسابات في تخصيص مصادر الشبكة	258
2.1 فهم سلوك المستخدمين في شبكة البيانات	258

3.1 تحديد المكان الذي يتم فيه تخصيص مصادر الشبكة	**259**
4.1 استخدام التقنيات ذات الجدوى الاقتصادية	**260**
2. تحقيق إدارة الحسابات	260
1.2 تكوين إدارة الحسابات	260
2.2 تحديد قيمة فواتير الاستخدام	264
3.2 رسوم فترة زمنية واحدة نظير التركيب شهرياً	264
4.2 تحديد الرسوم بناء على كمية مصادر الشبكة المستهلكة	245
5.2 طريقة العد الاجمالي لعدد الحزم	266
3. إدارة الحسابات	271
4. إدارة الحسابات في نظام إدارة الشبكة	272
5. تدوين إدارة الشبكة	281
الخلاصة	**284**
مسرد المصطلحات	**285**
المراجع	**289**

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

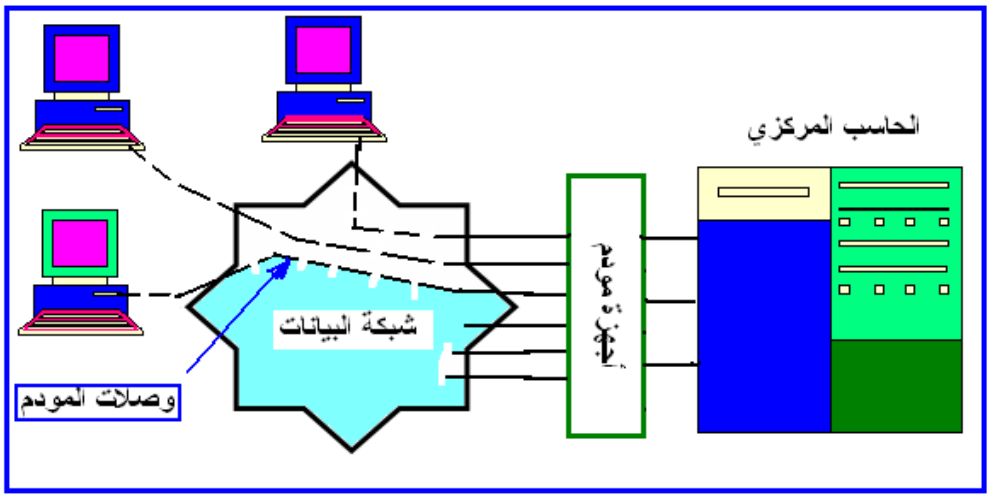
عزيزي الدارس، تساعد إدارة الحسابات مهندس الشبكة في **قياس وتدوين معلومات الحسابات بناء على إرسال بيانات المستخدمين عبر الشبكة**. واستخدام هذه البيانات في تحديد قيمة دفع المستخدمين لفواتيرهم، وتوزيع المصادر، وحساب التكاليف. كما تعزز إدارة الحسابات من فهم مهندس الشبكة لمعدل استخدام مصادر الشبكة، وإنشاء 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.

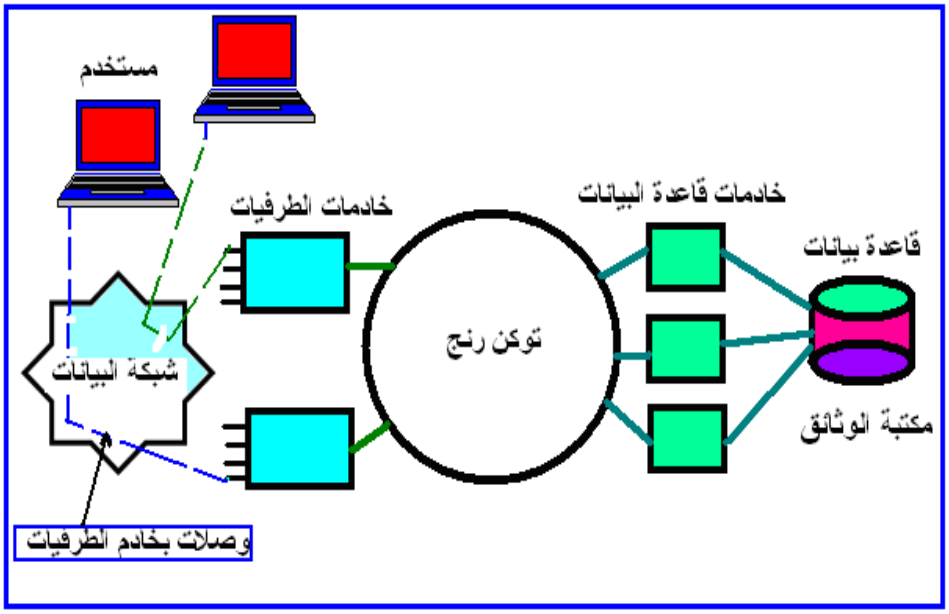
2.1.2 استخدام المعايير وضبط الحصص

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 For Request

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، وبحسب 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

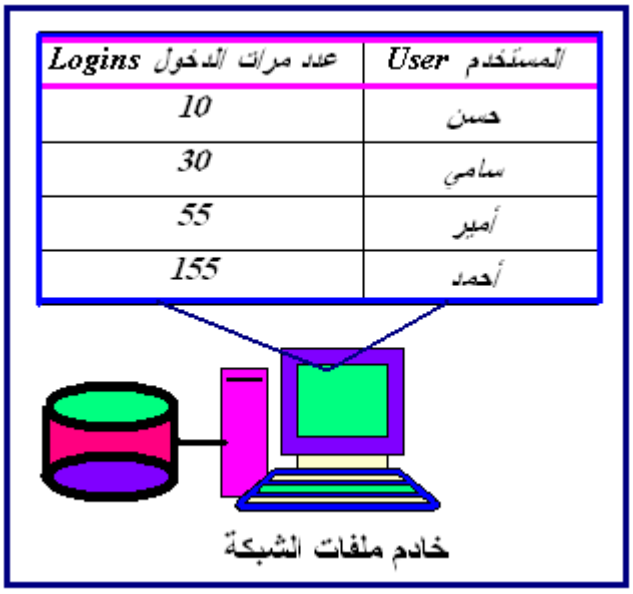
في هذه الطريقة، يتم تحديد فاتورة المستخدم بناء على تركيب وصلة الشبكة، بالإضافة إلى رسوم قياسية نظير الاستخدام عن كل شهر. إن إدارة الحسابات ليس من الضروري أن تكون من أجل الفواتير، لأنها لا تتطلب معلومات من الشبكة. على الرغم من ذلك، فإن هذا النظام من السهل جدا تنفيذه، لكنه قد يصبح صعبا للحكم عل مستخدم 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 مداخلInputs 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 الإجمـــالي لعـــدد الحزم

في هـذه الطريقة يتم عد إجمـالي لعـدد الحـزم، وهـذا يـبين اسـتخدام الشبكة. ثم تزداد الفاتورة، عند كل مرة يرسل المسـتخدم، أو يسـتقبل حزمه. من عيوب هذه الطريقـة، أن الفـاتورة لعـدد معلـوم من الحـزم تكون واحدة، بغض النظر عن كمية المعلومات المرسلة أو المسـتقبلة. على سبيل المثال، ربما يقوم أحد المسـتخدمين بإرسـال حـزم قصـيرة لحركة مرور تفاعلية الـتي لا تمثل عبأ على وصـلات أو أجهـزة الشـبكة. لكن مستخدم آخر، ربما يقوم بإرسال ملف يعتمد على حزم ضخمة. إذا كان كل من حركة المـرور التفاعليـة، وملف النقل تحتـاج 1000 حزمة لإتمامهما، فإن الفاتورتين سوف تتوافقان. لكن ، لا يتم الإجراء كـذلك ، إن ملف النقل ذو الحـزم الضـخمة، سـوف يسـتخدم مصـادر أكـثر من الشـبكة، على الـرغم من أنه يـدفع نفس الفـاتورة، مثل حركة المـرور التفاعلية، التي تستخدم مصادر أقل.

دفع الفاتورة الإجمالية حسب الحروف المستخدمة:

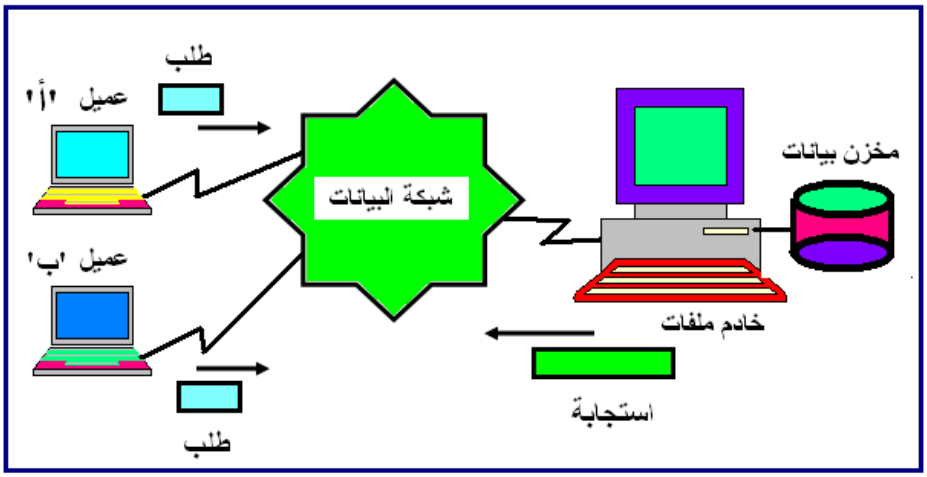
يمكن **تجنب عيوب الطريقتين السابقتين** بواسـطة دفع الفـاتورة الإجمالية للحـروف المسـتخدمة، يقـوم المسـتهلك بالـدفع حسب كمية مصـادر المسـتخدم للشـبكة. تشـمل هـذه المصـادر: سـعة النطـاق، والحروف المستهلكة (حرف-حرف أو بيت-بيت)، وليس من الضـروري على أساس الحزم. القرار التـالي الـذي يجب اتخـاذه هو هل يتم تحديد الفـاتورة بنـاء على إجمـالي عـدد الحـروف المرسـلة أم الحـروف المستقبلة؟

إن تطبيقـات الشـبكة الـتي تسـتخدم **بروتوكـول طبقة النقل الاعتمادي**، مثل TCP أو بروتوكول شبكة نوفيل SPX ، يتم تأكيد حزم البيانـات المسـتقبلة من الهـدف بواسـطة **حـزم إعلام** Acknowledgement Packets. في هـذه التطبيقـات، يتم فقط عد الحروف في حزم البيانات، وهـذا منطقي ومعقـول، لأنها الحـزم الأكـبر التي تستهلك مصادر شبكية أكثر. أما التطبيقات التي لا تسـتخدم طبقة النقل الاعتمادي، تحتاج منا أن نقوم فقط بعد الحـروف في اتجـاه واحد عبر الشبكة.

كثير من الوسائط المحيطة، تقوم بدمج التطبيقات التي تستخدم طبقة النقل الاعتمادي والتطبيقـات الـتي لا تسـتخدمها. معظم المؤسسـات تختار طريقة تحديد فاتورة الدفع على أسـاس الحـروف المسـتقبلة من الشــبكة، والحــروف المرســلة إلى الشــبكة، أو الــدمج بينهمــا. يوجد ممــيزات واضــحة لكل من هــذين الأســلوبين، بالتماشي مع الخــروق المصاحبة.

طريقة تحديد فاتورة الدفع بناء على الحروف المرسلة:

إن طريقة تحديد فاتورة الدفع بنـاء على الحـروف المرسـلة إلى شـبكة البيانات بديهي ومعقول. عنـدما يقـوم المسـتخدم بإرسـال أشـياء عـبر الشبكة، فإن الفاتورة ينبغي أن تزداد. لسوء الحـظ، في نمـوذج شـبكة الخـادم/ العميـل، الشـائعة، فـإن هيكلية تحديد فـاتورة الـدفع يوجد بها بعض الخـروق الخطـيرة. إن تحديد فـاتورة الـدفع على أسـاس الخـرج يـؤدي إلى عـدم تشـجيع المسـتخدم من عـرض الخـدمات من أجهـزة الخادم التي يملكونها. لتوضيح ذلك، نفترض أن أحد المســتخدمين على الشبكة يمتلك خادم ملفات يحتـوي بيانـات مهمة لمشـروع بحـثي. وأن العديد من المستخدمين تم توصيلهم بخادم الملفات، ويقومـون بتحميل كمية ضخمة من المعلومات يوميا. وهؤلاء الذين يجمعـون المعلومـات، يرسلون حزماً صغيرة إلى أجهـزة الخادمـات، لطلب معلومـات. يقـوم خـادم الملفـات بعد ذلك بنقل كمية ضـخمة من البيانـات وترجيعها إلى المسـتخدم، كما هو موضح في شـكل7.4. إذا تم تحديد فـاتورة الـدفع بناء على الحـروف الخارجـة، فـإن المسـتخدم الـذي يـوفر المعلومـات سوف يستلم فاتورة ضخمة، التي بـدورها تسـبب أن المسـتخدم الـذي 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 المجلـدات Folders. في شبكات خادم ملفات شبكة نوفيل، يمكن ترك الدليل متاح للعملاء من أجل وضع أو اسـتقبال بيانـات. معظم هـذه الخـدمات، يتم تصـميمها لتحقيق مكـان مخصص للعملاء لأخذ الوثـائق والتطبيقـات. بواسـطة دفع فواتـير المؤسسـة على أسـاس اسـتقبال الحـروف من الشبكة. تستطيع الشبكة المساعدة في تـأمين المسـتخدم الـذي يـوفر الخدمة، بحيث لا يستقبل فاتورة ضخمة آليا.

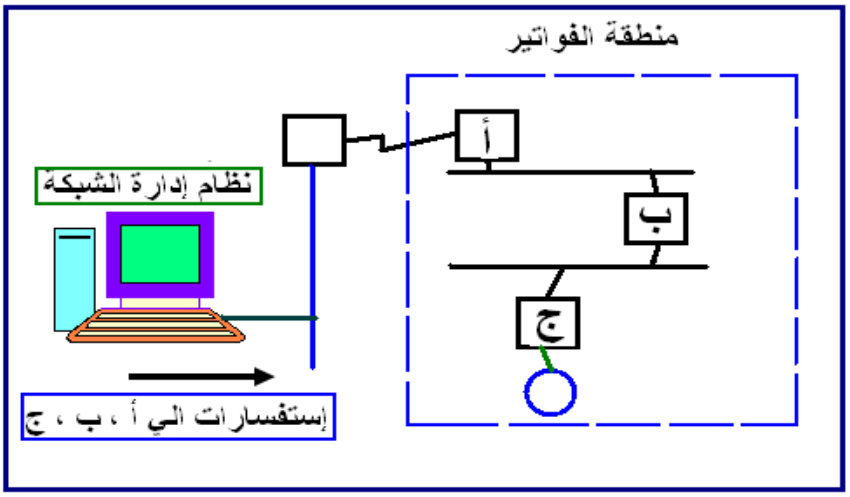
عيوب طريقة الدفع على أساس الحروف المستقبلة:

إن طريقة الدفع المبنية على أساس الحروف المستقبلة يوجد بها بعض الخروق.

أولا: يوجد العديد من بروتوكولات الشـبكة ترسل **رسـائل إعلام** من الهدف إلى المصدر. ينتج عن ذلك أن المستخدمين الذين يـوفرون هذه الخـدمات للشـبكة تسـتقبل حـروف بيانـات غـير مطلوبة من الشبكة. لحسن الحظ، أن حـزم الشـكر تكـون عـادة ذات أطـوال صـغيرة للغايـة. يمكن إهمـال هـذه الحـروف، لكن باسـتخدام الإحصـائيات عن أجهـزة الشـبكة، نسـتطيع حسـاب إجمـالي عـدد الرسائل المرئية. أيضا، أن المؤسسة الـتي تحسب فواتـير الـدفع، 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 طـول الحروف المستقبلة من الشبكة، هي **حدوث البيانـات الـتي لم تطلب** Unsolicited Data، مثل البريد الإلكـتروني. حيث تضـاف إلى فاتورة دفع المسـتخدم. ربما يمكن للمؤسسة أن تتغاضى عن هـذه الخروقـات، بسـبب أن العديد من المسـتخدمين ويرسـلون ويسـتقبلون البريد بنفس المعـدل. لكن ليست هـذه هي الحالـة، عنـدما يكـون المسـتخدم على قائمة البريد ويسـتقبل العديد من الرسـائل البريديـة. بسـبب أن المسـتخدم يكـون على القائمة البريدية لأحد الأسباب، فإن فاتورة الدفع ينبغي أن تعكس استقبال هذه البيانات نتيجة خدمة هذه الشبكة. لسوء الحظ، إن نمو شـبكة الانترنيت قد أدى إلى نمو طردي في حدوث نفايات بريدية Junk e-Mail غير مطلوبة، يمكنها أن تغرم المستخدمين بسبب نظـام دفع الفواتير حسب طريقة الحروف المستقبلة.

ثالثـا: أحد العيـوب الأخـرى الممكنة لهـذه الطريقة في تحديد قيمة فواتير الدفع طبقا للحروف المستقبلة، تنتج عن أن **كل مستخدم يستلم بيانات من الشبكة، عنـدما تقـوم المؤسسة برصد الشـبكة لأسـباب إدارية**، كما هو مـبين في شـكل 7.5. على الـرغم من أن معظم هـذه البيانـات سـوف يتم إرسـالها إلى المستخدم بطريقة منتظمـة، ولفـترة زمنية محـددة. يمكن إجـراء الاستفسارات Queries مرة في اليـوم، أو في السـاعة، أو كل بضع دقائق. من الممكن حسـاب عـدد الاستفسـارات النوعية الـتي يتم إرسالها خلال فترة دفع الفواتير، وكم عدد الحروف الـتي تحتويهـا. إذا كـانت المؤسسـة تحـدد دفع الفواتـير شـهريا، يمكن بسـهولة حسـاب متوسط عـدد الاستفسـارات خلال الشـهر(على سـبيل المثال، فإن الاستفسار الواحد الذي طوله 500 حرف يتم إرسـاله كل خمسة دقائق). عندما يقـوم مهنـدس الشـبكة بفحص مشـاكل الشبكة، يتم طرح هذه الحـروف من قيمة كل فـاتورة، وكـذلك كل الحروف الأخرى التي ينبغي حدوثها ويتم إرسـالها لأسـباب إداريـة، 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

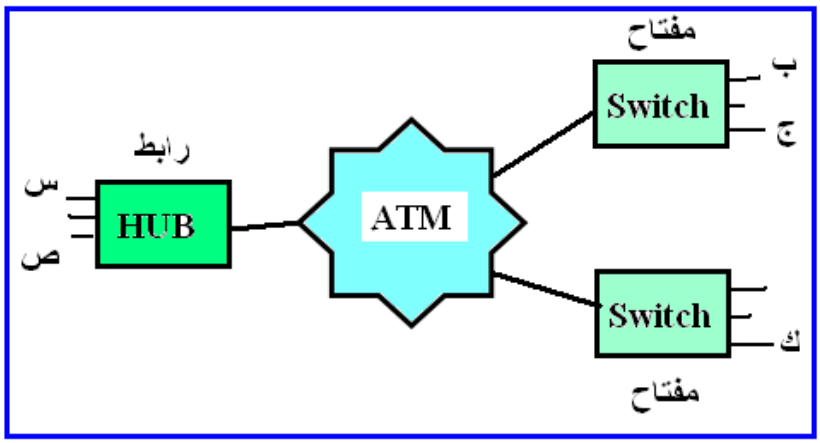
؟

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 الشـبكة المحلية التخيلية

عزيزي الدارس، كما شرحنا، إن تنفيذ نظام دفع الفواتير المبـني على أساس المصادر، يتطلب استخدام إدارة الحسابات لتجميع الإحصـائيات المطلوبـــة. بعد ذلك ينبغي على المؤسسة أن تحصل على مصـــادر المعلومـات، ومعالجتهـا، وتنشئ فواتـير الـدفع بنـاء على المصـادر المستهلكة. على الرغم من أن هذه العملية ربما تبدو صـعبة، فإنها ربما تكون أكثر صعوبة في الشبكات المحلية التخيلية Virtual LANs.

إن تقنيات الشـبكة المحلية التخيلية تقـوم بالتوصـيل المنطقي لأجهـزة الشـبكة المحلية عند المواقع الفعلية المختلفـة، لتكـوين شـبكة محلية منطقية واحدة، كما هو مبين في شكل 7.6. في الواقـع، فـإن الأجهـزة الفعلية ربما يتم ربطها عـبر شـبكة ذات سـرعة عالية باسـتخدام نظـام نمط الاتصال غير المتزامن ATM أو نظام وحدة مواجهة بصرية لتوزيع البياناتFDDI ، أو ربطها إلى نفس أجهزة الشبكة. يوجد بالأسواق العديد من المـوردين تمتلك بـرامج تشـغيل الشـبكة 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 للاداة 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.

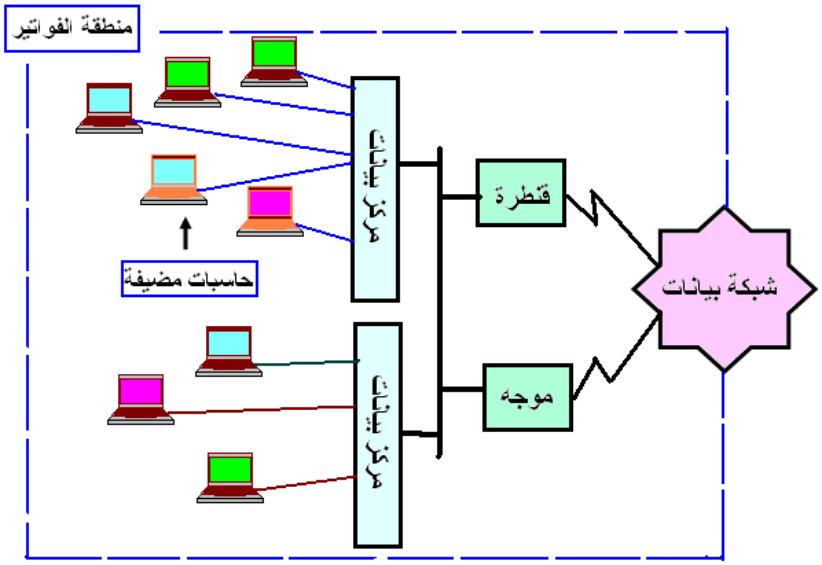
2.4 الأداة المركبة لإدارة الحسابات

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.

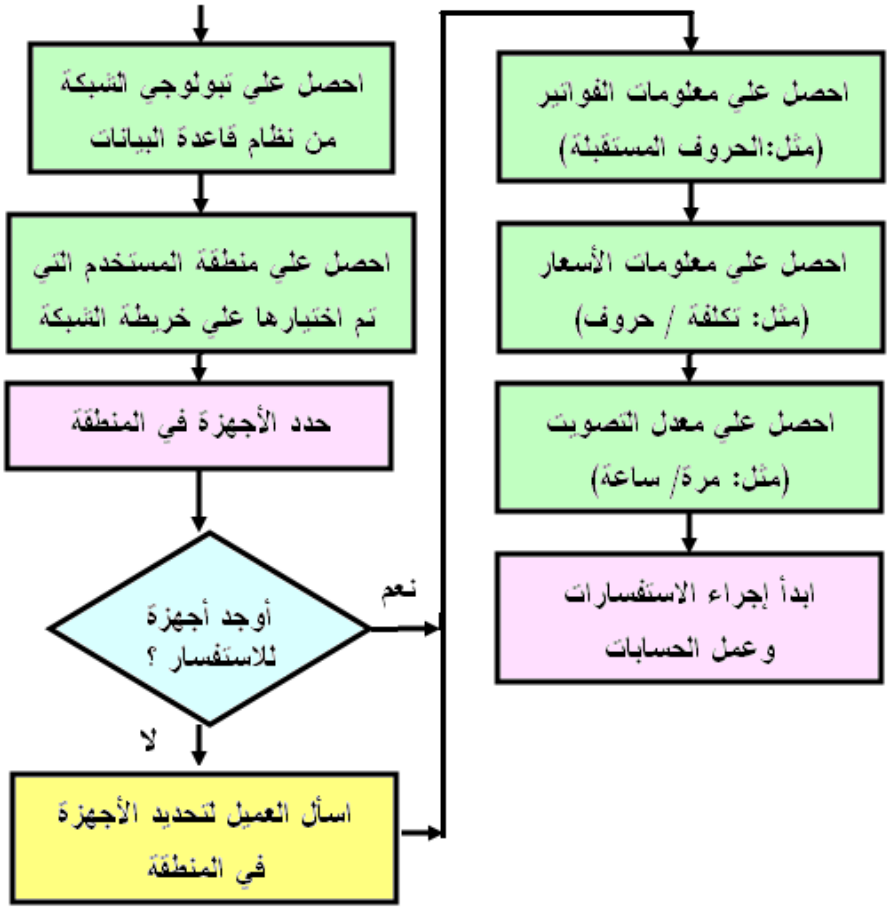
عند هذه النقطة تبدأ عملية حساب فواتير الدفع للمنطقة، بواسطة تجميع بيانات فواتير الدفع ووضعها في قاعدة البيانات العلاقية، كما هو مبين في شكل 7.8.

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 تكـون الأداة المتقدمة قـادرة على التنبؤ بقيمة فـاتورة الـدفع لمستخدم الشبكة. لإجـراء ذلـك، يمكن للأداة أن تقـوم بعمل خطـوتين هما:

1- فحص قاعدة البيانـات العلائقية لتحديد أي اتجـاه في فواتـير الـدفع، 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 مـدير مجموعة المسـتخدمين من مهنـدس الشبكة أن يقوم بحساب فاتورة الدفع القادمة، يمكن لمهندس الشـبكة أن يقوم بإدخال بيانات المجموعة إلى الأداة الـتي تبحث عن معلومـات الفواتير في قاعدة بيانات إدارة الشبكة للحصـول على جميع السـجلات السابقة لهذه المجموعة. بفرض أن هذه السجلات أظهـرت زيـادة 5% عن كل عشـــرة فـــترات فواتـــير دفـــع. تقـــوم الأداة بعد ذلك بفحص المعلومـات في قاعـدة البيانـات عن فـترة الـدفع للفواتـير الحاليـة. وترحيلها إلى نهاية المـدة، وتجد الأداة أن 6% زيـادة محتملة منذ فـترة دفع الفـاتورة السـابقة. عند الخـرج، تقـوم الأداة بإنشـاء الفـاتورة عن المدة المطلوبة التي تمثل 6% زيادة عن فاتورة المدة السابقة.

نفترض أن المعلومات التي تم اسـتخراجها لا ترتبط عن قـرب برسـوم الفـاتورة السـابقة. يمكن أن يحـدث هـذا، عنـدما تكـون مـدة الفـاتورة الحالية بدأت في التو، وأن عينة البيانات لا تمثل مدة الفاتورة بالكامـل، أو أن المجموعة قد زادت أو نقصت من أنشطتها في استعمال الشبكة. في مثل هـــذه الحـــالات، تحتـــاج الأداة المتقدمة إخـــراج التنبـــؤات (الحسابات) على أساس البيانات التاريخية، وبعد ذلك تشـتق منها مـدة الفاتورة الحالية.

إن التقنيـــات الـــتي تســـتخدمها الأداة المتقدمة متاحة في الأســـواق، وتستطيع الأداة استخدام قاعدة البيانات، واسـتخراج المعلومـات الـتي تساعد على حساب حصص وفواتير الدفع لمستخدمي الشبكة.

أسئلة تقويم ذاتي

؟

اشـرح كيف يتم إدارة الحسـابات في الشـبكة المحلية التخيلية.

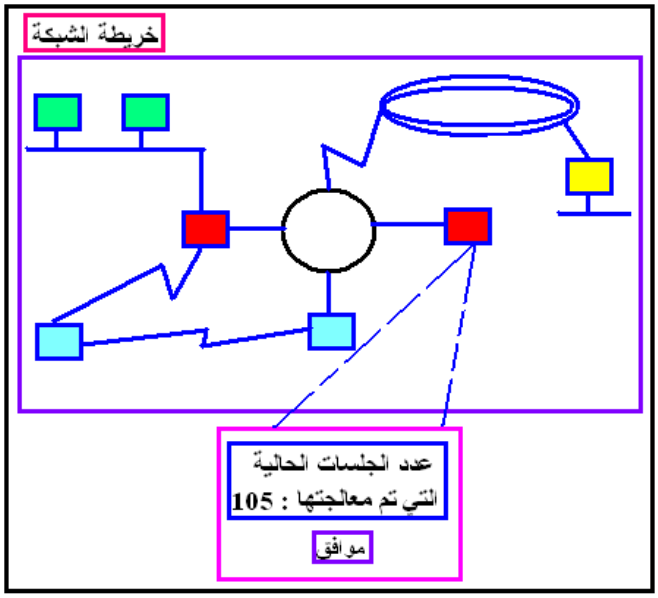
قارن بين استخدام الأداة البسيطة والأداة المركبة في إدارة الحساب لشبكة البيانات.

قارن بين استخدام الأداة المركبة والأداة المتقدمة في إدارة الحسابات لشبكة البيانات .

5. [illegible]

عزيزي الـدارس، يمكن تـدوين معلومـات إدارة الحسـابات على شـكل رسـائل وتقـارير في الـزمن الفعلي. يمكن لرسـائل الـزمن الفعلي أن تخبر مهندس الشـبكة بقيمة معيارية معينـة، كما تـوفر التقـارير النصـية 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 هـذه الوحـدة تعرفنا على إدارة الحسـابات والـتي تختص بقيـاس اسـتعمالات مصـادر الشـبكة بواسـطة المسـتخدمين 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 عنـوان المصـدر الـذي يرسل الحـزم، ومن الممكن إضـافة معلومـات عن بيانـات التطبيقـات في المسـتوى الأعلى خلال الحزمـة. يمكن أن يكـــون متاحا في الأســـواق مكدســـات بروتوكولية Protocol Stacks خاصة تقوم بتنفيذ البروتوكول

المصطلح بالإنجليزية	معناه بالعربية
ManagementAccount	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

المصطلح بالإنجليزية	معناه بالعربية
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
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

المصطلح بالإنجليزية	معناه بالعربية
Queries	استفسارات
Quotas	حصص
Time-Sharing	مشاركة الوقت
Triggers	مقادح
Recurring Cost	التكاليف المرجعية
RFC(Request For Comments)	برجاء التعليق
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.