الفصل الخامس

تأمين وإدارة الشبكة

إدارة أو تنظـــيم شـــبكة قـــد يكون أمرا مرهقا بمسئوليات إدارة وتنظيم الشبكة والمحافظة على انسيابيتها وإصلاح أعطالها وحل مشاكلها .

عند إدارة شبكة تقع على عاتق المسئول عنها مسئوليات تنظيمية منها :

- إعداد وتنظيم سجلات المستخدمين .
- إعداد وتنظيم سجلات المجموعات .
- إعداد توجيهات النظام .
- مراقبة أداء الشبكة .
- تطبيق وسائل حماية الشبكة .
- التخطيط لحل المشاكل وتحديد وحل مشاكل أداء وإدارة الشبكة .

من المفيد تقسيم إدارة الشبكة إلى :

- **تنظـــيم المســـتخدمين** : بإعداد وإلغاء وصيانة سجلات المستخدمين وإعداد أذونـــات الوصول المناسبة للمستخدمين للاستفادة من موارد الشبكة ، واكتشاف وحل مشاكل سجلات وأذونات المستخدم .
- **تنظـــيم وصيانة موارد الشبكة** : مثل الطابعات والتطبيقات وقواعد البيانات والاتصالات .
- **مراقبة الأداء** للكشف عن مشاكل الشبكة ومشاكل المستخدمين قبل حدوثها .
- **تنظـــيم الحمايـــة** لحمايـــة الشبكة من التخريب المتعمد والأعطال وأخطاء المستخدمين .
- **إدارة الأحداث** : بوضع مخطط تصحيح يتم تنفيذه عند عطل الشبكة أو جزء منها وبناء مخطط للتغلب على أعطال الشبكة أو مكون من مكوناتها .

سجل المستخدم

لكـــل مستخدم على الشبكة سجل خاص يتكون من جزء من قاعدة بيانات توفر للمستخدم حقوق استخدام موارد شبكة ، ويتضمن سجل المستخدم معلومات اسم المستخدم وكلمة مرور الدخول وحقوقه والأذونات الممنوحة له على الشبكة .

تحـــتوى جمـــيع نظم تشغيل الشبكات على وسائل إنشاء سجل مستخدم وتحديد الحقـــوق الممـــنوحة لـــه وتوقيتات استخدام هذه الحقوق والقيود التى تحد من اســـتخداماته فمـــثلا فـــى نظـــام تشـــغيل ويندوز Windows NT تنشأ حقوق المســـتخدمين ضمن خدمة إدارة مجال المستخدم حيث يتم تحديد معلومات سجل مستخدم جديد مثل :

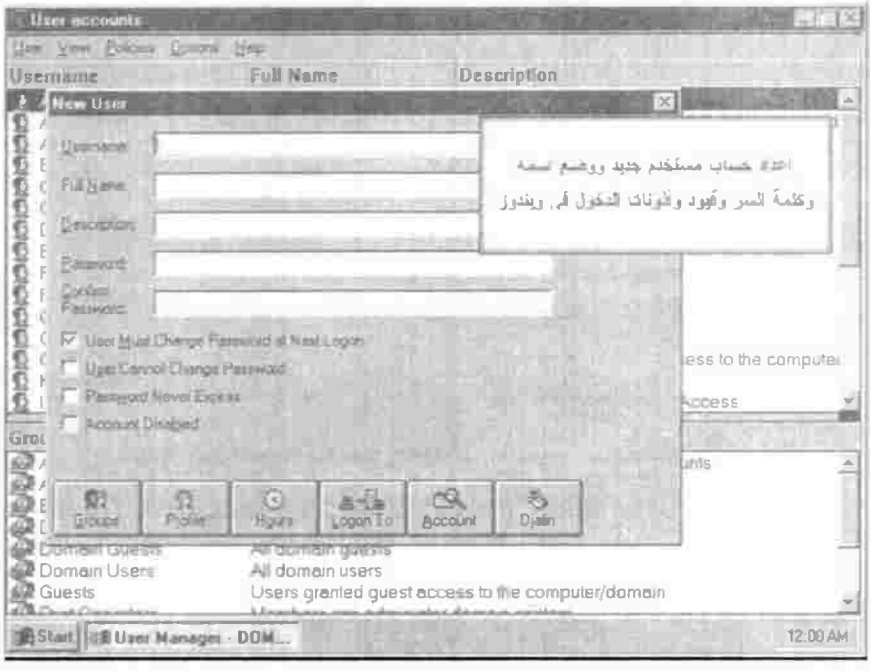
البيان	التعريف
اسم المستخدم	اسم فريد قائم على اصطلاح تسمية وهو حقل ضرورى
الاسم الكامل	اسم شخص لإنشاء سجل مستخدم وهو حقل اختيارى
الوصف	نص تعريف مستخدم مثل القسم وهو حقل اختيارى
كلمة المرور	تســـتطيع إدخال كلمة مرور مبدئية اختياريا ، وفى حالة عـــدم تعريف كلمة مرور تأكد من تعريف كلمة مرور عند تسجيل دخول المستخدم للمرة الأولى .
الـــتأكد من كلمة المرور	حقـــل لإعادة كتابة كلمة المرور للمرة الثانية للتأكد من سلامة حروفها (ضرورى فى حال تحديد كلمة مرور)
علـــى المستخدم التعديل	تســـمح بإجـــبار المستخدم على تعديل كلمة المرور عند أول تسجيل دخول على الشبكة .
لا يجب التعديل	لعـــدم تعديـــل كلمـــة المـــرور بواسطة المستخدم بمنع المستخدم من تغيير كلمة المرور فيما بعد
تعلـــيق ســـجل المستخدم	تسمح بتعليق سجل مستخدم مؤقتا .

سجل مستخدم مقفل	حقل يظهر خافتا وغير قابل للاختيار لسبب ما قد يقفل النظام سجل مستخدم ما فيظهر هذا الحقل معلما وظاهرا غير خافت ويمكن إعادة اختياره ، ويحدث إقفال سجل ما بسبب محاولة إدخال عدة كلمات مرور غير صحيحة

هناك قيم أخرى يجب تحديدها عند إعداد سجل مستخدم جديد :

- تستطيع تحديد أيام وساعات (توقيتات) سماح دخول مستخدم على الشبكة .
- تستطيع تحديد محطات العمل التى يسمح للمستخدم بالعمل عليها .
- تستطيع أيضا تحديد السماح للمستخدم بالدخول إلى الشبكة من موقع بعيد .
- تستطيع أيضا تحديد ملف للمستخدم يستخدمه عند كل دخول على الشبكة ،

ويحدد ملف المستخدم ظهور رمز لجهاز المستخدم عند تسجيل الدخول والبرامج المسموح باستخدامها والشبكات والطابعات المسموح بالوصول إليها .



كلمة المرور Password هى أضعف نقطة حماية الشبكة لذلك يجب تنفيذ سياسة خاصة لها بانتقائها بدقة دون أن تتضمن اختيارات معروفة مثل أسماء الأبناء أو

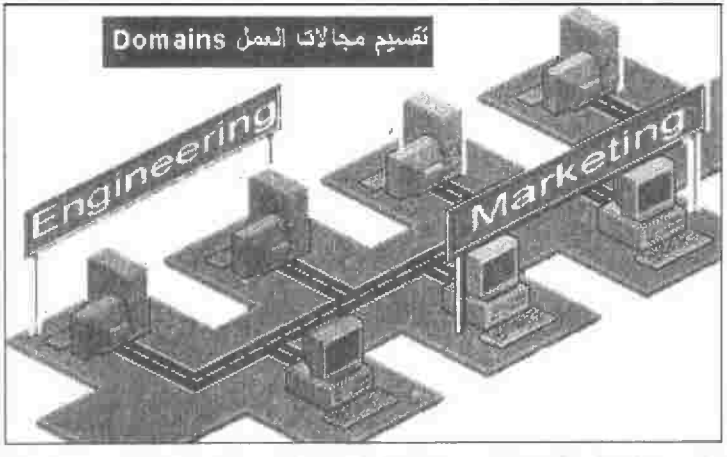
تواريـــخ الميلاد أو كلمات شائعة ويجب عدم تدوينها على الأوراق ، كما يجب تعديلها على فترات منتظمة ، ويمكن استخدام برمجيات تقوم بتوليد أسماء مرور عشوائيا لتوفير جهد الانتقاء .

عند السماح للمستخدمين بتغيير كلمات المرور بأنفسهم عليك استخدام تقنية سهلة لاختيار كلمات مرور من ٨ إلى ١٠ حروف .

عـــند انـــتهاء عمل مستخدم من المؤسسة قد يميل البعض إلى إلغاء سجله نهائيا لكن يمكن تعليق السجل مؤقتا فإلغاء السجل يمحو كل المعلومات المتعلقة بحقوق المســـتخدم وأذونـــات السماح وعضوية المجموعات التى ينتسب إليها ولا يمكن استرجاع هذه المعلومات بعد إلغائها لكن تعليق العضوية يمكن من إعادتها مرة أخرى عن طريق مشرف الشبكة .

سجل المجموعات وصيانته

تـــتألف المجموعـــة مـــن عدة مستخدمين ويتكون سجل المجموعة من سجلات مجموعـــة مســـتخدمين فعـــند إضـــافة سجل مستخدم إلى مجموعة ما يحصل المســـتخدم تلقائـــيا على جميع حقوق وأذونات هذه المجموعة مما يوفر طريقة سهلة لإعطاء حقوق لمجموعة من المستخدمين .



تدعـــم نظـــم تشغيل الشبكات ومنها نظام تشغيل ويندوز Windows NT أنواعا مخـــتلفة مـــن المجموعات ففى نظام تشغيل ويندوز Windows NT تجده يدعم

نوعين من المجموعات المحلية والشاملة :

- توفر المجموعة المحلية لعدد من المستخدمين حق الوصول إلى موارد موجودة على الشبكة وتمنحهم حق تنفيذ مهام معينة كالنسخ الاحتياطى واسترجاع الملفات .
- تنظم المجموعة الشاملة سجلات مستخدمى الشبكة .

تشبه خطوات إعداد سجل مجموعة خطوات إعداد سجل مستخدم .

توفر بعض نظم التشغيل مثل نظام تشغيل ويندوز Windows NT مجموعات مسبقة الأعداد مثل :

المجموعة	نوع	ملاحظات
سجل العاملين	محلية	بحقوق إضافة وتعديل وإلغاء سجلات مستخدمين ومجموعات
الإداريون	محلية	يقوم بكل المهام الإدارية على الحاسب المحلى
عمال النسخ	محلية	حقوق النسخ الاحتياطى والاسترجاع على الجهاز المحلى
إداريو المجال	شاملة	حقوق مهام إدارية ويضاف تلقائيا للمجموعات الإدارية المحلية على أجهزة الحاسب
ضيوف المجال	شاملة	يضاف السجل الضيف تلقائيا لهذه المجموعة وتضاف هذه المجموعة تلقائيا لمجموعة الضيوف المحليين
مستخدمو المجال	شاملة	عند إنشاء سجل مستخدم فى مجال يضاف تلقائيا ضمن المجموعة وتضاف المجموعة إلى مجموعة المستخدمين المحليين

ضيوف	محلية	يقـوم بمهام المجموعة ، والأعضاء فيها لا يقـدرون علـى القيام بتغيرات دائمة على سطح المكتب
عمال الطباعة	محلية	له حقوق إعداد وإدارة طابعات الشبكة
عمال الخادم	محلية	له حقوق المشاركة بموارد أقراص التخزين وحفظ واسترجاع معلومات الخادم
مستخدمون	محلية	يقوم بالمهام التى منح حقوقها والوصول إلى الموارد المسموح له بها

مراقبة أداء شبكة

بعـد إعداد الشبكة تصبح عملية مراقبتها والإشراف عليها من المهام الأساسية للإداريين حيث تساعد هذه المراقبة فى اكتشاف المشاكل قبل حدوثها .

لمراقبة شبكة عدة فوائد فهى توفر :

- طريقة قياس حجم احتمال الشبكة ومخطط توسيعها قبل حدوث مشاكل .
- القدرة على تحسين أداء الشبكة للحصول على زيادة السرعة .
- إمكانية تحديد مواقع الاختناق مما يساعد على حل مشاكل الأداء .

تعمـل المكونات المادية والبرامج فى الحاسب لأداء الوظائف المطلوبة ، وينتج الأداء العـام السيئ عندما لا تعمل إحدى أو بعض المكونات الأداء الملائم مما يؤثـر علـى الأداء العام للنظام ومن أمثلة ذلك احتواء الخادم على معالج قوى وقـرص صـلب عالى السرعة لكن بحجم ذاكرة محدود مما يبطئ عمل النظام ككـل فعلى كل مكونات الجهاز الأخرى انتظار الذاكرة لتنتهى من مهامها مما يسبب مشكلة اختناق (عنق الزجاجة) .

الأجهزة التالية قد تكون سبب الاختناق (عنق الزجاجة) المحتمل على الحاسب :

- الذاكرة عند عدم وجود ذاكرة كافية .
- سرعة المعالج عندما لا تكون سرعة كافية .

- سرعة قرص التخزين غير الملائمة أو عدم وجود سعة فارغة كافية عليه .
- استخدام بطاقات شبكة غير قادرة على مجاراة سرعة الشبكة .

حـــل هذه المشاكل يتطلب وجود ذاكرة كافية ، وسرعة معالج عالية ، وسرعة قـــرص تخزيـــن كبيرة ووجود سعة فارغة كافية عليه ، واستبدال بطاقة الشبكة بأخـــرى مزودة بموصل أكثر سرعة مثل PCI أو بطاقة مزودة بمساحة تخزين مؤقت Buffer أكبر للبيانات .

تـــأتى مـــع أنظمة تشغيل الشبكات بصفة عامة أدوات تساعد على مراقبة أداء النظام كما تتوفر برامج المنافع المستقلة التى تقوم بمراقبة أداء النظام ففى نظام تشغيل مثل نتوير ونظام تشغيل مثل ويندوز Windows NT تتوفر خدمة مراقبة الأداء التى تساعد على القيام بمهمة مراقبة أداء النظام وسوف نتعرض لها عند تناول أدوات الكشف عن أعطال الشبكة .

حماية الشبكة

مـــن مهـــام إدارة شـــبكة وصـــيانتها توفير حماية لها والمحافظة على بياناتها ومواردهـــا مـــن تخريب متعمد أو غير مقصود والحيلولة دون حدوث أضرار للشبكة وبياناتها ومعداتها والاكتشاف السريع لأعطال مكوناتها المادية والبرمجية ويـــتم ذلـــك بوضع الخطط الملائمة للتصرف حيال المواقف بإعداد سياسة حق

وصـــول المســـتخدمين للموارد والتدريب الملائم للمستخدمين وصيانة المعدات وترميز البيانات .

يعـــتمد مستوى الحماية على مدى الحماية المطلوبة فإذا كانت المعلومات سرية مـــثل المعلومـــات الطبية أو القانونية أو المالية فيجب وضع مستوى أعلى من الحماية .

أهـــم خطـــوات حمايـــة الشبكة هى وضع سياسة حماية تغطى حماية المكونات المادية والموارد وحماية البيانات كالآتى :

١- خطة وصول المستخدمين

وضع خطة سليمة واضحة مسجلة تتعلق بحق وصول المستخدمين إلى البيانات والموارد وتوقيتات الوصول وحق تعديل مستوى الوصول وأذون الوصول إلى الموارد للمستخدمين .

٢- إعداد خطة شاملة لتأمين المعدات والمكونات المادية

بـــتحديد المعـــدات الـــتى يجـــب أن تكون خلف أبواب موصدة إذ يجب وضع الخادمات فى غرف مغلقة حماية لها ولمنع أى شخص من أخذ نسخة احتياطية أو أحـــد أقراص التخزين أو العبث بالبيانات أو تعطيل الجهاز أو تخريبه ، كما يجـــب الاهتمام فى الخطة بضمان سلامة محطات عمل كل المستخدمين عندما يغيب أى منهم عنها ووضع أسلوب تأمين تمديدات الشبكة .

٣- وضع خطة شروط سجلات المستخدمين

بتحديد مستويات السماح والحقوق الممنوحة وطرق اختيار كلمات المرور وفترة استخدامها وتوقيتات تعديلها .

٤- وضع خطة التدريب وتنفيذها

فعـــندما يكـــون المستخدمون على دراية بطريقة تشغيل الشبكة وأسلوب عملها يصـــبح تلـــف المـــوارد قلـــيل الحدوث ، وعندما يتم تدريب المستخدمين على خطـــوات تأميـــن وحماية الشبكة تصبح الشبكة أكثر أمانا من عمليات التخريب

المتعمد أو الغير مقصود .

٥- استخدام البرمجيات المساعدة لحماية الخادم

التى تسمح بالدخول على الشبكة عبر الهاتف باتخاذ جانب الحيطة لمنع غير المصرح لهم من الدخول عبر الهاتف وهناك برمجيات وصول عن بعد تسمح بهذه الوسائل منها :

- خدمة برمجيات الوصول عن بعد Remote Access Service من مايكروسوفت التى توفر أصالة دخول مستخدمين عن بعد مع أمان وترميز .
- خدمة التخابر فيما بعد التى تسمح للخادم الموصول عن بعد بإقفال الخط مع المستخدمين عن بعد ومعاودة الاتصال بناء على رقم متفق عليه .
- خدمة التدقيق التى توفر متابعة للمستخدمين الذين يسجلون دخولهم عن بعد وتدوين الملفات والمجلدات والميزات التى يتمتعون بها على النظام .

٦- وضع خطة حماية تمديدات الشبكة

تنقسم هذه الخطة إلى قسمين بحماية التمديدات من التصنت وحماية التمديدات من التلف : فتمديدات الشبكة يسهل التصنت على معظمها كما يصعب اكتشاف التصنت لذلك يجب عدم السماح بالوصول قريبا من التمديدات خارج أو داخل المبنى كما لا يجب ترك التمديدات ظاهرة للعيان بل يجب مدها عبر الحوائط وفوق السقف وتحت الأرض كما يجب حماية التمديدات بمنع الضرر الناتج من نقل المعدات والأثاث فوق التمديدات مما قد يسبب قطعها أو ثنيها .

٧- تخطيط سياسة تدقيق

تسمح بمتابعة نشاط أى مستخدم على الشبكة فبيانات التدقيق تبين المهام التى قام بها المستخدم وتوقيتات قيامه بها ، ويمكنك استخدام التدقيق للمتابعة وللتنبيه عند أى محاولة تسجيل دخول صحيحة أو خاطئة أو محاولة تعديل سياسة الحماية على الشبكة ، وتستطيع نظم تشغيل الشبكات توفير التدقيق مثل نظام ويندوز Windows NT .

٨- استخدام الترميز

الترميز يخلط رسالة ليصعب فهمها باستخدام المفاتيح فعن طريق التشفير العام بمفاتـــيح مثل تلك التى تنتجها شركة RSA يتم الترميز وفك الترميز بمفتاح عام ومفـــتاح خـــاص فالمفتاح العام يعرفه الجميع ويتم حفظه على الدليل ليستطيع الجميع الوصول إليه أما المفتاح الخاص فلا يعرفه إلا المرسل والمستلم .

٩- استخدام حماية الفيروس

الفـــيروس برنامج صغير صمم ليلحق نفسه بالبرامج والملفات وينتشر من ملف إلـــى أخر بنسخ تلقائى دون علم صاحب الجهاز ويقوم بوظيفته التى قد تتضمن محو معلومات قرص أو تتلف البرامج ، ويجب الحماية من الفيروسات باستخدام عـــدة بـــرامج مضادة للفيروسات عند بدء تشغيل الجهاز بالبحث فى الذاكرة أو اختبار أقراص النظام على فترات ، وعند اكتشاف فيروس تقوم البرامج بفصلها وإزالـــتها أو إلغاء الملفات المصابة بها كما يجب فحص الملفات عند نسخ ملف عبر الشبكة أو من قرص مرن .

مخططات الحماية من الفيروسات الحديثة تراقب النظام بحثا وتنبيها عن وجود فيروسات أو أى نشاط مشابه لها .

إلـــى جانـــب اســـتخدام برمجيات مضادة للفيروسات يجب فرض سياسة جيدة وتدريب المستخدمين على القيام بالخطوات المناسبة الوقائية التى تتضمن تحديد نـــوع البرمجـــيات المسموح بتحميلها عبر الشبكة كما أن تطبيق نظام أذونات الوصول إلى الموارد يحمى موارد الشبكة المهمة .

١٠- تجنب فقد البيانات

البيانات هى سبب وجود الشبكة وقد تكون البيانات هامة جدا ومن المهم الحفاظ علـــيها لذلك يجب تطبيق خطة جيدة لمنع ضياع أو تلف البيانات على الشبكة ، وتتضـــمن طرق تفادى ضياع البيانات استخدام مصادر الطاقة البديلة والفورية ونســـخ البيانات احتياطيا وطرق حل المشاكل سريعا عند توقف الشبكة بالتغلب

على الأعطال .

أ- **استخدام مصادر الطاقة الفورية** : وحدة التغذية الفورية UPS مصدر طاقة خارجي يمد الشبكة ومكوناتها بالطاقة كمصدر طاقة احتياطى (مثل بطارية) عند توقف مصدر الطاقة الرئيسى ، وتتم عملية تحويل التغذية الكهربية سريعا دون توقف عمل الأجهزة ، وتوفر وحدات التغذية الفورية وظائف مهمة ببقاء الأجهزة عاملة بدون توقف لوقت محدد وقد تقوم أيضا بالتنسيق مع الخادم لتنفيذ الخروج الآمن والتوقف عن العمل كما تقوم بتنبيه الإدارة عند وقوع عطل وتمنع المزيد من المستخدمين من الدخول إلى الشبكة .

هناك نوعان من أجهزة UPS هما المباشر والبديل فمصدر الطاقة الدائم المباشر يوضع بين مصدر الطاقة الاعتيادية وجهاز الحاسب بحيث يغذى الحاسب بالطاقة بشكل مستمر وهكذا تبقى البطارية مشحونة وتوفر ظروفا مثالية تمنع مشاكل التغذية الكهربية والضوضاء المتسرب مع الطاقة .

مصدر الطاقة البديل يمرر الطاقة الاعتيادية ويوفر طاقة احتياطية عند الحاجة فعند توفر الطاقة الاعتيادية يقوم المصدر البديل بوصلها مباشرة إلى الحاسب ويراقب تقلبات مستوى الطاقة ، أما عند توقف الطاقة الاعتيادية أو حصول خلل بمستوى الطاقة يحول إلى مصدر الطاقة البديلة ، وهذا الأسلوب أقل اعتمادا من الطاقة المباشرة لكنه أقل تكلفة أيضا .

ب- **النسخ الاحتياطى** : أفضل وأكثر طرق حماية البيانات استخداما هى النسخ الاحتياطى الدورى للبيانات على وسائط خارجية مثل الأشرطة أو الأقراص المضغوطة كطريقة سهلة ورخيصة .

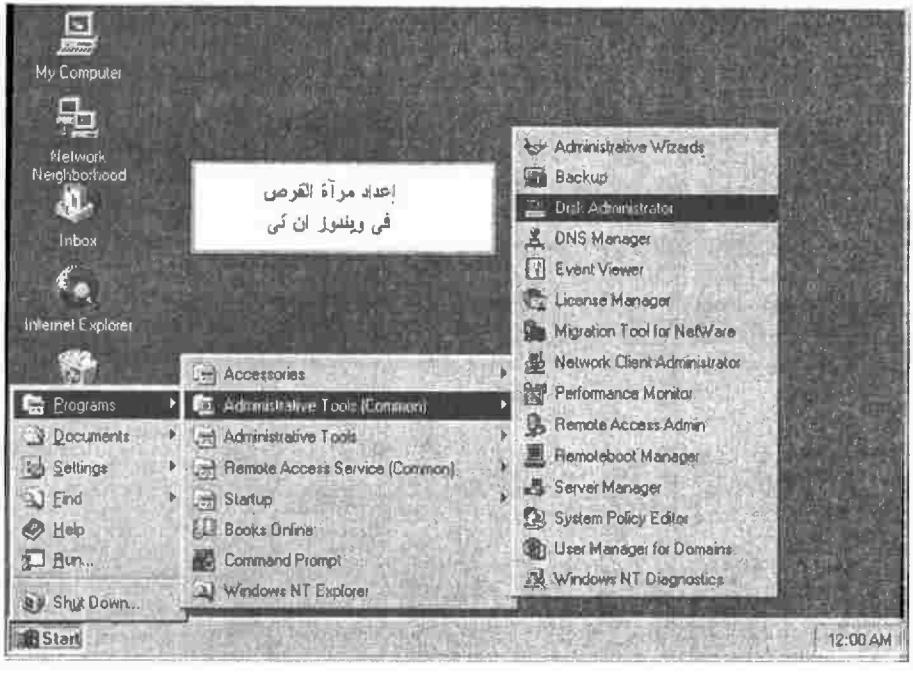
١- الخطوة الأولى لوضع مخطط نسخ فعال هى تحديد البيانات الواجب نسخها فأى شئ لا تستطيع استرجاعه بسهولة يجب نسخه احتياطيا مثل وثائق المستخدمين وقواعد البيانات والبريد الإلكترونى ومعلومات الخادم والملف الخاص بكل مستخدم .

٢- الخطـــوة الثانـــية هى تحديد جدول توقيتات النسخ الاحتياطى ، وهناك عدة توجهـــات لتحديد التوقيت الملائم لكن بشكل عام عليك جدولة خطة على أساس يومى وأسبوعى وشهرى حسب أهمية البيانات .

لفحـــص نظـــام النسخ عليك استرجاع البيانات ومقارنتها بالبيانات الأصلية كما يجـــب وضـــع ســـجل مفصل لعملية النسخ يوفر معلومات تاريخ النسخ ونوعه والقـــائم به ووسط نسخ البيانات وبرمجيات النسخ وهناك برمجيات وأدوات فى كل نظم تشغيل الشبكات توفر خدمات القيام بهذه المهمة .

ج- أنظمـــة قوية للتغلب على الأعطال Fault-Tolerant System : تمثل هذه التســـمية مقدرة نظام على التماثل من الكوارث مثل التغلب على أحداث تتضمن انقطاع الطاقة أو تعطل المكونات المادية أو البرمجية .

يـــتم التغلـــب على أعطال أجهزة التخزين مثل القرص الصلب بعمل نسخة من البيانات فى مكان أخر مثل ازدواج القرص Disk Dupplexing أو مرآة القرص Disk mirroring فإذا تعطل قرص يقوم الآخر بالمهمة .



نظـــام التغلـــب على الأعطال والتماثل من الكوارث بدون ضياع البيانات تقنية تحمـــل اســـم مجموعـــة الأقـــراص المستقلة RAID (Redundant Array of Independent Disk) ، ويـــتم تقسيم الـــتغلب على العطل إلى مجموعة درجات RAID كمجموعة أقراص صلبة لا تعتمد على بعضها ويحل أحدها محل الآخر عـــند عطله كطريقة نسخ المعلومات على مجموعة من الأقراص بطرق مختلفة تحددها مستويات تقنية RAID من المستوى صفر إلى المستوى رقم ٥ .

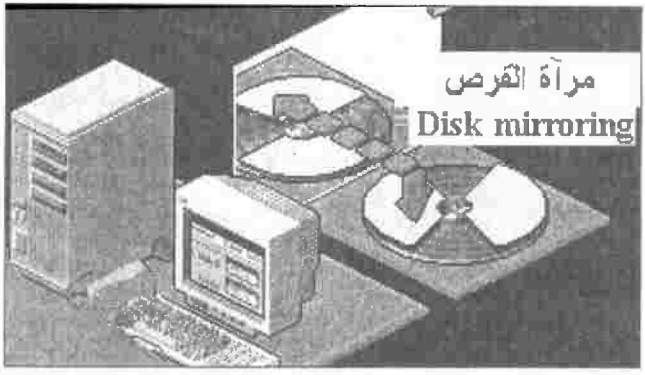
Redundant Arrays of Inexpensive Disks (RAID)		
Level 0	NT Server	Disk striping
Level 1	NT Server	Disk mirroring
Level 2	Disk striping with error correction code (ECC)	
Level 3	Disk striping with ECC stored as parity	
Level 4	Disk striping large blocks with one drive parity	
Level 5	NT Server	Disk striping with parity

مستويات التغلب على الخطأ

يمكن تطبيق نظام مستويات RAID عبر المكونات المادية أو البرمجية فى نظم تشغيل الشبكات .

المســـتوى الأول (صـــفر) يسمى بتقسيم القرص الصلب Disk Striping يمكن تجمـــيع أقراص صلبة بحد أدنى ٢ وأقصى ٣٢ قرص تخزين لتأليف مجموعة تكتب البيانات عبر كل الأقراص صفا بعد صف .

مرآة القرص Disk Mirroring RAID1 بقرصين لنسخ مزدوج للبيانات .



(يطلق على القرصين اسم مجموعة الصورة المعكوسة) وعند تعطل أحد القرصين تبقى البيانات محفوظة على القرص الثانى .

المستوى الخامس (تشريح القرص مع تأكيد التماثل RAID5) أكثر الأنظمة شيوعا وأفضلها فهى تحسن الأداء وتوفر مساحة الأقراص الصلبة حيث يجمع بين ٢ إلى ٣٢ قرص تخزين لتأليف مجموعة شرائح واحدة فى كل مجموعة شرائح ، وتكتب البيانات عبر الأقراص صفا فصفا .

تدعم نظم تشغيل الشبكات مثل ويندوز ونتوير أنظمة احتمال الخطأ أخرى مثل القطاعات البديلة حيث يقوم النظام بمراقبة القراءة والكتابة على القرص وعند اكتشاف قطاع سيئ يمنع استخدامه فيما بعد .

كمدير إدارى من واجبك التخطيط لما يجب فعله عند وقوع كارثة بوضع مخطط واضح ومفصل لمواجهة الكوارث يتناول المواضيع التالية :

- تحديد البيانات الواجب نسخها احتياطيا وتوقيتات نسخها .
- معلومات تشكيل الحاسب والمكونات المادية الأخرى يجب حفظها بالنسخ الاحتياطى .
- تحديد البيانات التى تحفظ فى موقع العمل والبيانات التى تحفظ خارج موقع العمل وكيفية حفظ كل منها .
- معرفة المهارات التدريبية المطلوبة لعامل الخادم والإداريين ليمكنهم التجاوب السريع والمناسب عند الطوارئ .

التغلب على الأعطال

تعرفنا على المكونات المادية وطرق تحقيق توصيلات شبكة وكيفية جمع عناصرها لتناسب الاحتياجات والاحتياطات اللازمة لعملها وتأمين هذه الأعمال وتوفير أكبر قدر من الحماية لمكوناتها لكن أحيانا قد يحدث عطل فى الشبكة أو فى جزء منها ، وتصبح هناك حاجة لاكتشاف مسببات الأعطال أو صيانة الشبكة من احتمالات الأعطال .

إن الشبكات بطبيعتها تختلف عن صيانة الأجهزة المنفردة فصيانة وإصلاح الأجهزة المنفردة أكثر سهولة من صيانة الشبكات ففى الشبكات قد تجد النوعيات المختلفة من الأجهزة مثل أجهزة الحاسب الشخصى IBM وأجهزة ماكنتوش ومنصات يونكس كما قد تجد أجهزة كبيرة Mainframe أو شبكات الأثير Ethernet أو حلقة Token Ring أو شبكة FDDI أو إطارات تحويلة Frame Relay أو شبكة غير متزامنة ATM أو مع وصلات ISDN أو خطوط هاتف Dial Up أو تعمل كشبكات لاسلكية مختلفة النوعية مستخدمة نوعيات مختلفة الإنتاج من أجهزة الوصل المركزية Hubs والموجهات Routers والجسور Bridges والبوابات Gateway عن طريق توصيلها ببطاقات NIC من إنتاج شركات مختلفة ووصلات وحدات خدمة رقمية – ووحدات خدمة قنوات DSU/CSU والمودم Modems .

قد تبدو الصورة مزعجة بوجود هذا الكم من المنتجات للشركات المختلفة لكن مما يزيد الأمر صعوبة وجود برمجيات مختلفة أيضا تعمل على الغالبية العظمى من المكونات المادية إضافة إلى الموارد المختلفة فى الشبكة من طابعات وأجهزة مسح وغيرها .

عندما كانت أجهزة الحاسب منفردة كان من السهولة تحديد التطبيقات التى تحتاج إليها وصيانتها لكن فى حالة الشبكة هناك العديد من الأمور التى يجب أخذها فى الاعتبار فليست التطبيقات فى حد ذاتها هى الأمر الوحيد الذى يتم

تحديـــده فهـــناك تحميل الملفات فى جهاز الخدمة وتركيب التطبيقات ومشاركة الملفـــات وتحديد القيود على استخدامها والوصول إليها وتحديد أذونات تشغيلها والـــتعامل معها كما أن اتساع مسافة الشبكة وعبء التمديدات فيها يضيف عبئا آخر على صيانتها .

إذا وضعت فى الاعتبار أن التكاليف الرئيسية للشبكة ليست هى تكلفة المكونات الماديـــة أو المكونات البرمجية فقد تكون قد وصلت إلى فهم أن التكلفة الرئيسية فى الشبكة هى الصيانة وإدارة الشبكة .

إن فهـــم وظـــائف الشبكة بنموذجها المرجعى OSI يفيد إلى حد كبير فى وضع اســـتراتيجية لإدارة وصيانة الشبكة فمن هذا الفهم يمكن التغلب على الكثير من مشاكل الصيانة فيها .

إن وحدات الشبكة فى وظائفها تقع تحت التقسيم البسيط التالى :

١- الطبقة الأولى (الطبيعية Physical) وفيها تجد بطاقات الشبكة NIC والمودم Modem ووحدات الخدمة DSU/CST والمضاعفات وأى جهاز آخر ينتمى إلى هذه الطبقة .

٢- الطـــبقة الثانـــية طبقة ربط البيانات Data Link وفيها تجد قناطر Bridges ووصـــلات مركـــزية Hub والمعيد Repeater والمبدلات Switch أو أى جهاز آخر يقوم بتعريف البيانات للطبقة الطبيعية .

٣- الطـــبقة الثالـــثة طبقة الشبكة Network Layer وفيها الموجهات Routers وبوابـــات الـــترجمة Translation Gateways والمبدلات التى تنفذ التوجيه وأى أجهـــزة أخرى تحدد المكان الذى يتم توجيه البيانات إليه بناء على نظام العنونة فى الشبكة .

٤- الطـــبقة الرابعة طبقة النقل وهى طبقة اختيارية فى الصيانة باحتوائها على بـــروتوكولات تحقـــق التوصـــيل الموجه Connected Oriented مثل TCP أو بـــــروتوكول UDP أو بـــــروتوكول IPX/NCP أو بـــــروتوكول SPX أو أى

بـــروتوكول يوفـــر خدمات الاتصال الموجه أو خدمات عدم الاتصال بين العقد Nodes .

سوف نلاحظ أن الطبقة الأولى تحدد أجهزة مادية بينما تتكون الطبقة الرابعة من مكونات برمجية خالصة لاعتمادها على بروتوكولات .

إن وظـــائف بروتوكول إدارة الشبكة البسيط Simple Network Management Protocol المعـــروف اختصـــارا برموز SNMP يوفر دعما جيدا لمعرفة كيفية وسبل تأدية المكونات لوظائفها .

بـــروتوكول إدارة الشبكة البسيط SNMP هو البروتوكول الشائع الاستخدام فى صـــيانة ومراقـــبة الشبكات وقد تم تصميمه أساس لبروتوكول TCP/IP إلا أنه اعتمد لكل من Novel IPX/SPX , Digital DECNet and AppleTalk مدعوما لمعظم الشبكات .

لقـــد وضعت مؤسسة المعايير القياسية ISO نموذجا لتقدير الاحتياجات المطلوبة من بروتوكول إدارة الشبكة فى النقاط التالية :

استشعار الأعطال Fault Detection على الشبكة والقدرة على التعامل مع بعض هذه الأعطال .

- القدرة على إدارة التجهيز Configuration Management .
- تحليل الأداء Performance Analysis وتوفير الإحصائيات .
- التحكم فى تأمين الشبكة Security Control بالتحكم فى الوصول .
- المحاسبة Accounting بتجميع البيانات لمن يستخدمها على الشبكة .
- الظهور بواجهة رسومية .
- القدرة على دعم أى إضافات برمجية .
- عدم الاعتماد على نظام تشغيل الشبكة .
- دعم البروتوكولات القياسية .

إن البرامج قد توضع على منصة كما قد توضع كعملاء فى أجهزة لتقوم برامج

العمـــيل بالاتصـــال مع كل جهاز برنامج التحكم الرئيسى وتزويده بالمعلومات اللازمة لإدارة الشبكة والأجهزة .

قد تختلف برامج العميل من شركة إلى أخرى لكنها توفر الوظائف التالية :

- معلومات حالة الجهاز .
- إحصائيات بطاقة الشبكة .
- واجهة لإدارة تجهيز المعدة أو الجهاز الذى تعمل عليه .
- القـــدرة علـــى استشعار المشاكل فى الجهاز وإمداد نظام إدارة الشبكة بهذه المعلومات .
- القدرة على توفير وثوقية وتأمين الجهاز كما يحدده جهاز التحكم .

وسوف نجد أن هذه الوظائف لا تختلف كثيرا عن وظائف التحكم الرئيسى .

إن الـــتحكم فى الشبكة لن يكون بعيدا عن تحكم النظام System Management فـــبرغم أن الصيانة قد ظهرت بمفهوم تحكم فى الشبكة لكن هناك حالات صيانة تعتمد على النظام مثل إضافة مستخدمين جدد أو تغيير أذونات مستخدم أو إتاحة القدرة على الوصول إلى شبكة الإنترنت لمستخدمين فى الشبكة .

إدارة الـــنظام لـــيس لها معنى منفرد هنا لكننا سوف نعتبر أن إدارة الشبكة هى إدارة الجـــزء الخـــاص بالطبقات الأربع الأولى من نموذج الطبقات السبع بينما تعتمد إدارة النظام على :

- إدارة الدعـــم كقاعدة بيانات لكل الأجهزة فى الشبكة مع معلومات كاملة عن المكونـــات الماديـــة فـــيها وتجهـــيز كل منها والملفات التى تحتويها لتجهيزها والبرامج المثبتة فيها .
- نظم التشغيل وتجهيزها وضبطها والخدمات التى تدعمها .
- توزيـــع الـــبرامج بمـــا يعنيه النسخ وتكوين مجموعات وتركيب وتوزيع البرامج الجديدة .
- الإشراف والتحكم عن بعد ودعم المستخدمين .

اكتشاف أعطال الشبكة

إن جعل الشبكة تعمل فى انسيابية يعد تحديا حتى لذوى الخبرة فالشبكة قد تكون معقدة وتتطلب إشرافا دائما يتعلق بكشف وتصحيح الأعطال حتى وإن لم تحدث بها أعطال .

العناصر الأساسية لإدارة ناجحة للشبكة وصيانتها تتحدد بالآتى :

- وضع مخطط عمل لنسخ البيانات المهمة وتأمين الحماية وتوثيق الشبكة ومعايرة المكونات المادية والبرمجية للشبكة والتحسين والتوسيع .
- مراقبة نشاط الشبكة وأداءها دائما لمعرفة وتوقع الأعطال قبل حدوثها .
- استخدام وسائل جيدة لكشف الأعطال وحل المشاكل بطريقة منهجية دون دخول عشوائى حتى لا تتسبب فى أعطال ومشاكل أكبر من الأعطال نفسها .
- فهم الأدوات المستخدمة فى الكشف عن الأعطال .
- التعرف على الخبراء ومراكز الدعم الفنى للمساعدة .
- حل تضارب (تنازع) المكونات المادية للشبكة أو عند توسيع شبكة .
- اختيار المكونات المادية والبرمجية المناسبة لمراقبة الشبكة .
- التعرف على الأخطاء والأعطال الشائعة فى الشبكة خاصة مكونات وبرمجيات الاتصال فلكل شبكة نظامها الخاص ومواطن الأعطال الشائعة فيها .
- تشخيص وتصحيح مشاكل التوصيل الشائعة للبطاقات والكبلات والمكونات المادية الفردية .
- تحديد وتصحيح مشاكل أداء الشبكة ومكوناتها .
- فهم طرق صيانة وإصلاح المكونات الفردية مثل الشاشة والطابعة وجهاز الحاسب المستقل كمحطة عمل وجهاز الخادم كجهاز مستقل .

هناك ٦ خطوات هامة جدا يجب اتباعها :

١- تجنب المشاكل قبل حدوثها .

٢- متابعة نشاط الشبكة باستمرار .

٣- الالتزام بقواعد وتوقيتات وأساسيات الصيانة .

٤- خطوات اكتشاف العطل عند حدوثه .

٥- الأدوات اللازمة لاكتشاف الأعطال .

٦- معرفة أين تجد المعلومات الكافية لحل المشكلة .

خطوات اكتشاف أعطال الشبكة عند حدوثها

لا مفر من وقوع مشاكل ومواجهتها ومن مهام صيانة الشبكة :

- تحديد المشكلة بدقة .
- معرفة القدرة على حلها .
- الأدوات المناسبة للحل .
- المكان الذى تتجه إليه لطلب المساعدة عندما تحتاج إليها .

كشف أعطال الشبكة مهمة لا تخضع للعشوائية أو الجهود الضائعة فالبعض قد يغوص داخل المشكلة مباشرة فى محاولة لحلها بطريقة أو بأخرى فإذا أمكن حلها كان بها أو قد تصبح مشكلة عويصة لا يمكن حلها وبالتالى تتجه الجهود إلى البحث عن الأدوات المناسبة أو على جهات أخرى تساهم فى الحل .

قد تعمل هذه الطريقة على جهاز مستقل لكنها ليست الطريقة المناسبة لمنهجية كشف مشاكل الشبكة حتى لا يضيع الوقت والجهد والمال .

من المهم التوجه الصحيح المنهجى لكشف أعطال ومشاكل الشبكة ووضع خطط تحليل ومعالجة المشاكل قبل تصحيحها حتى لا تتفاقم المشكلة وتزيد وتظهر مشاكل أخرى قد تكون أكبر ، وهناك خطوات أساسية للكشف عن الأعطال المحتملة فى الشبكة :

١- جمع المعلومات .

٢- حصر السبب .

٣- وضع تقييم .

٤- علاج المشكلة .

٥- توثيق النتائج .

إصلاح الأعطال

يجب على القائم بأعمال الصيانة القيام بالمهام الأساسية فى الصيانة وهى :

١- تنمية العادات التى تمنع وقوع الأعطال والمشاكل .

٢- عزل العطل .

٣- التعرف على الاحتمالات المختلفة لمعالجة عطل معين .

٤- الاستفادة من الأدوات المتاحة فى النظام .

مراقبة الشبكة تعتبر من الأساليب الأولى المستخدمة فى تحديد الأعطال التى تحدث .

يعتبر تجزئ المشكلة لتحديد مكان العطل فى الشبكة هو أحد الأساليب السهلة التى تساعد على التشخيص السريع .

الأجزاء الرئيسية فى نظام الشبكة هى جهاز الخدمة الرئيسى ونظام التشبيك والمحطات الفرعية ونظام التشغيل وعطل كل واحد من هذه الأجزاء يكون له مظهر مختلف إلى حد كبير عن عطل الجزء الآخر .

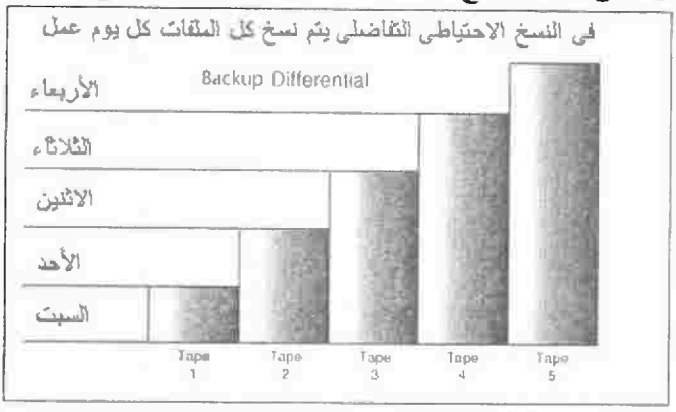
نسخ مهم البيانات يعتبر أكثر الطرق اعتمادا ورخصا للتغلب على أعطال شبكة عند حدوثها وهناك عدة عناصر يجب اعتبارها عند تصميم نظام نسخ هى :

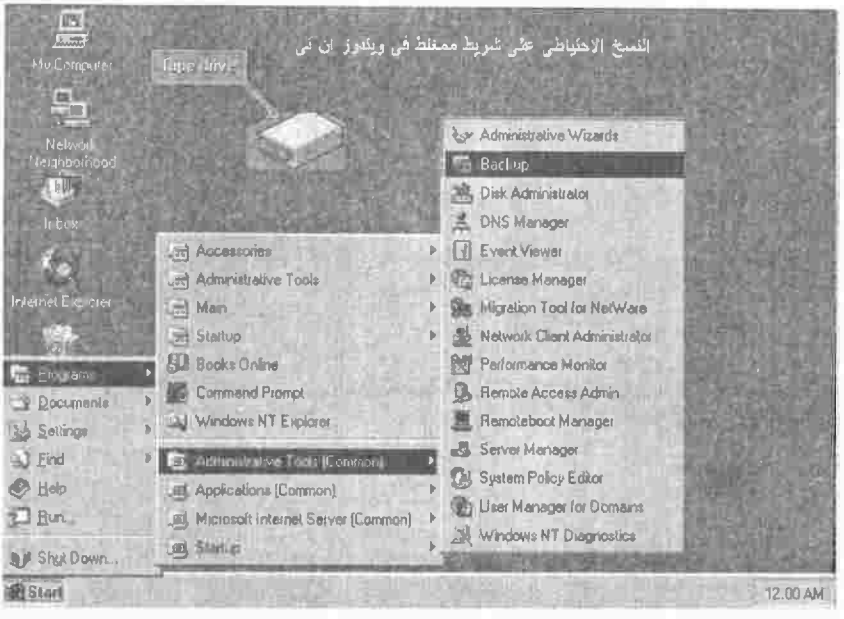
- تحديد ما يجب نسخه .
- كيفية النسخ .
- توقيتات النسخ .
- كيفية الفحص والاسترجاع .
- تحديد أسلوب النسخ .

فى أسلوب النسخ العادى التزايدى نقوم بنسخ عادى كامل كل أول يوم عمل فى الأسبوع ونقوم بنسخ تفاضلى بقية أيام الأسبوع .

فى طريقة النسخ التفاصلى العادى نقوم بنسخ عادى كامل أول يوم عمل فى

الأسـبوع ونقـوم بنسـخ تـزايدى لبقية أيام العمل فى الأسبوع ، ومع أن هذه الطريقة أطول فى الاسترجاع ألا أنها تأخذ وقتا أقل عند النسخ يوميا .





حماية الشبكة يعنى توفير حماية المعلومات والموارد من أى تلاعب مقصود أو عرضـــى ، ويعتمد مستوى الحماية المفروض على مستوى الحماية المطلوب ، ومن هنا فالخطوة الأولى والأهم هى وضع مخطط وسياسة حماية تشمل :

- تطبيق سياسة حماية جيدة تتعلق بأذونات وحقوق الوصول .
- الحماية المادية للشبكة .

توثيق الشبكة

توثيق الشبكة مهمة تتطلب تدوين سياسات العمل وخريطة توزيع المكونات ومعظم المهام اليومية والصيانة الدورية للمكونات ، ومع أن ذلك يستغرق الوقت والجهد لكنه يصبح غاية فى الأهمية فمع وجود طريقة نظامية لمراجعة المعلومات يمكن تفادى الأعطال والمشاكل وإعادة تشغيل الشبكة سريعا بشكل طبيعى عند توقفها .

عند تحضير توثيق للشبكة يجب مراعاة التالى :

- وضع خريطة مفصلة للشبكة تبين مواقع كل المكونات المادية على الشبكة وعناوين عناصر الشبكة ونوع تمديدات الكبلات بتفاصيلها .
- وضع سجل لكل أجهزة ومكونات الشبكة يتضمن تفصيل المكونات المادية وملفات تجهيز النظام وبيانات تشكيل النظام لكل جهاز على الشبكة والمكونات البرمجية والمادية الملحقة وأى تغيير أو تعديل لهذه التفاصيل .
- معلومات النسخ الاحتياطى بوضع سجل يتضمن الأفراد المسموح لهم بالنسخ واسترجاع الملفات وتوقيتات النسخ وسجل عمليات النسخ التى تتم .
- مكان حفظ أقراص البرامج الأصلية ودليل الاستخدام للبرامج والمكونات المادية وفهرستها فى سجل ضمن التوثيق مع أرقام الإصدارات وكلمات سر تركيبها وأرقام التسجيل كل منها .
- سجل معدات وأدوات الصيانة وبرامج الصيانة والفحص .
- قائمة أرقام هاتف الدعم الفنى وجهات شراء ودعم الأجهزة والبرامج .
- سجل الأعطال وطريقة حلها ومكان حدوثها والأجهزة التى تأثرت بها والبرمجيات المتورطة فيها وتاريخ الأعطال وزمن حلها .
- هناك برمجيات أدوات إشراف إدارى شبكية تساعد على مهام التوثيق توفر مايكروسوفت منها أدوات تسمى SMS أو خادم إدارة النظام System Management Server يمكنها الكشف على الشبكة آليا لجمع المعلومات التى

تبيـــن مخطط الشبكة والمكونات المادية والبرمجية الموجودة وتساعد أيضا على مراقبة الشبكة وتعاون فى عملية تحميل البرمجيات الجديدة .

المعايير المقياسية

استخدام المعايير القياسية فى أى شبكة موحدة المصدر يوفر الآتى :

- ســـهولة الإشراف وكشف الأعطال وتصحيحها مثال استخدام أقراص صلبة أو بطاقات شبكية أو بطاقات شاشة أو شاشات من شركات معينة مما يؤدى إلى معرفة تفاصيل هذا النوع مما يوفر عناء صيانة كل أقراص الشبكة .
- سهولة التغلب على الأعطال بمراقبة مكونات متشابهة وتبديل مكونات مادية موحـــدة وتخزيـــن الحد الأدنى من قطع الغيار والتوصيف البرمجى كما يوفر عبء البحث عن البرمجيات المطلوبة لتشغيل هذه المكونات .

يجـــب وضع معايير لبرمجيات الشبكة أيضا فبشكل عام كلما قل عدد التطبيقات المخـــتلفة علـــى الشـــبكة كلما انخفض احتمال وقوع المشاكل كما أن استخدام المستخدمين لنفس التطبيقات يحل مشاكل التوافق كما يوفر عبء التدريب على برمجيات مختلفة تؤدى نفس الغرض ويقلل من مشاكل صيانتها .

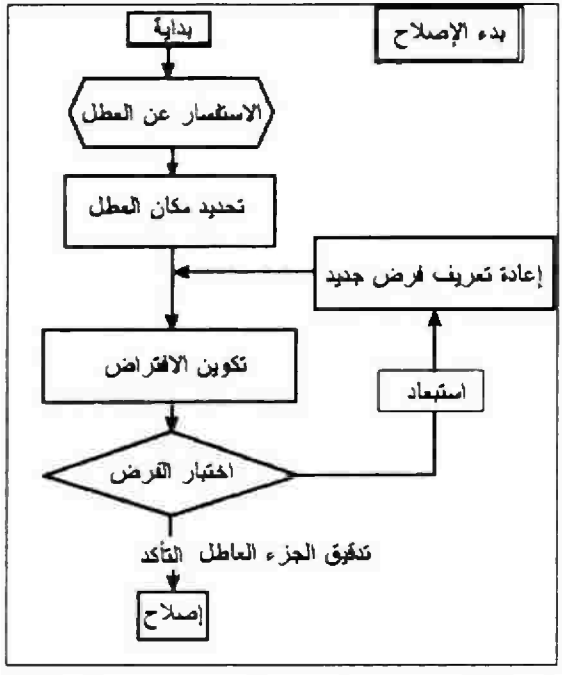
مـــن المستحســـن أيضـــا وضـــع مقايـــيس عامـــة لتسمية مكونات النظام مثل المستخدمين والأجهزة والملفات العامة مما يوفر الكثير من الوقت ويجعل تعقب المشاكل أسهل عند وقوعها .

بداية الإصلاح

يـــبدأ إصـــلاح المشـــاكل بالاستفسار عن المشكلة من الشخص المستخدم الذى عرض المشكلة أو تأثر بها سوف يحدد :

- توقيت حدوث المشكلة .
- الشكل العام للمشكلة .
- الشواهد التى تدل على طبيعة المشكلة .
- الأجهزة والبرمجيات والموارد التى تتأثر بالمشكلة .

- طرق الاقتراب من حل المشكلة .



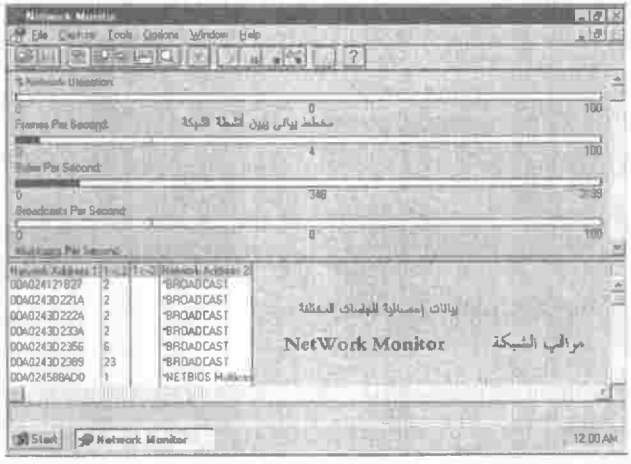
من المعلومات المهمة التى يجب الرجوع إليها عند حدوث مشكلة :

- مراجعة كتيب دليل الاستخدام .
- مراجعة توثيق الجهاز والشبكة ومقارنته بما هو موجود مثل ملفات تجهيز النظام Config.sys وملف التشغيل الحزمى التلقائى Autoexec.bat وملفات النظام والبرامج المثبتة وتسجيلات النظام ورقم الإصدار .
- مراجعة تشكيل مكونات الشبكة المادية وإعدادات البرمجيات .

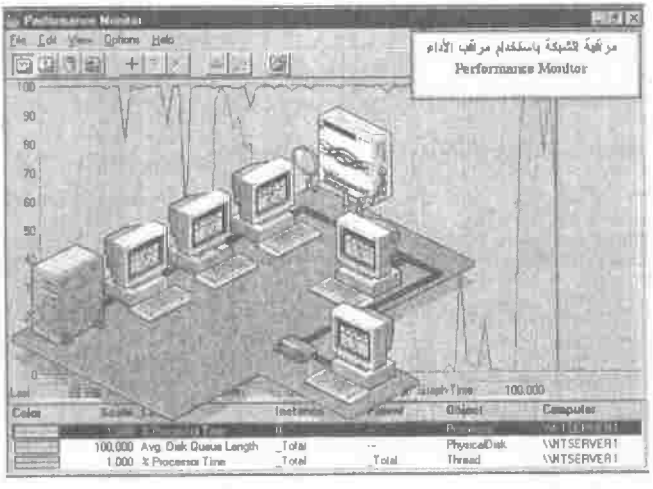
بهذه المعلومات يتكون قدر لا بأس به من المعلومات التى تفيد فى معرفة سبب العطل والتغلب عليه واسترجاع النظام بسرعة .

الاستفادة بالأدوات البرمجية : يتضمن نظام تشغيل Windows NT 4.0 برمجيات مراقبة الشبكة Network Monitor كأدوات قوية تسمح بمراقبة حركة البيانات على الشبكة من وإلى الأجهزة كما أن برمجيات نظام إدارة الخادم System Management Server من مايكروسوفت تتضمن نسخة قوية من

بـــرنامج مراقـــبة الشبكة Network Monitor لمراقبة حركة البيانات على كل أجهزة شبكة تسمح بالتقاط البيانات العابرة إلى جهاز عن بعد .

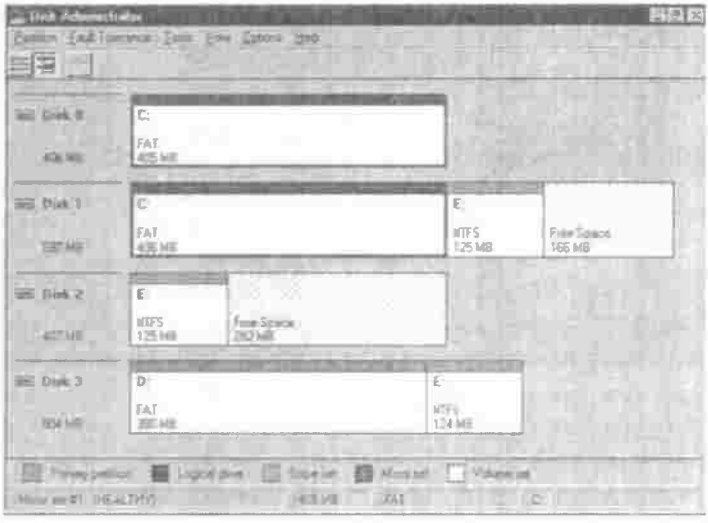


يوفـــر بـــرنامج مراقب الأداء استعراض الأداء من عدة جوانب فتظهر بيانات المراقبة برسم بيانى كما يتيح تسجيل البيانات وإنشاء تقارير للتحليل اللاحق .

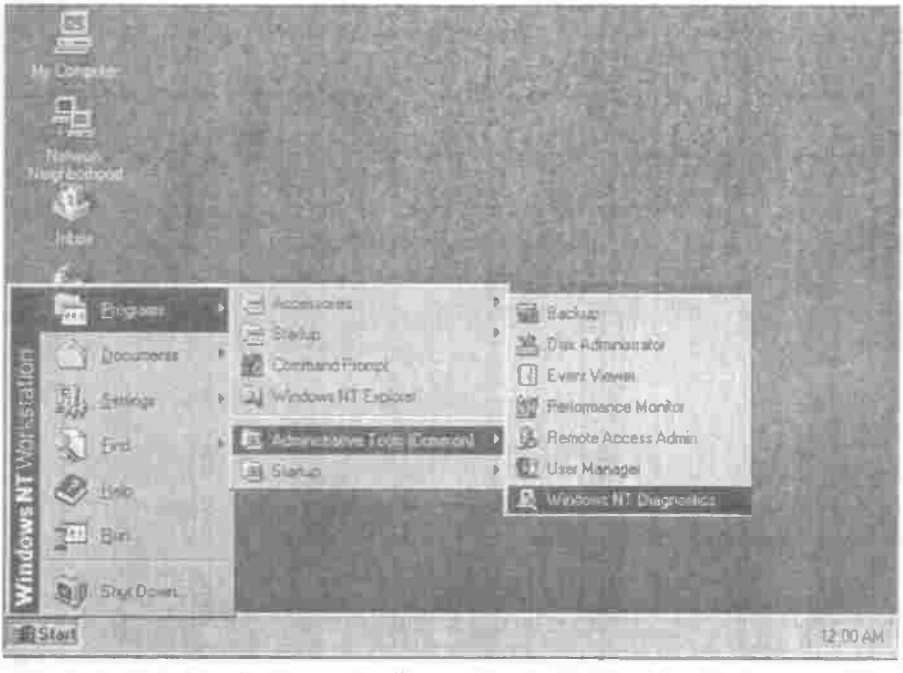


كمـــا تحـــتوى كـــل نظم تشغيل الشبكات على أدوات أخرى للتشخيص وعلاج المشاكل منها :

- بـــرامج لإنشـــاء قرص نظام طوارئ لاستخدامه عند عطل النظام أو تلف ملفات الولوج أو وجود عيب فى التسجيل .
- برامج تشخيص ومعالجة مشاكل الأقراص والمناطق فيه (التقسيمات) .

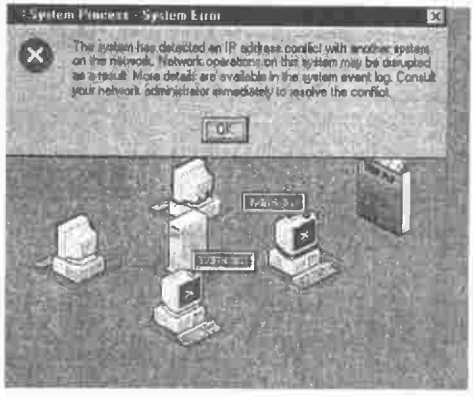


- كما تحتوى أدوات تشخيص ومعالجة مختلفة .



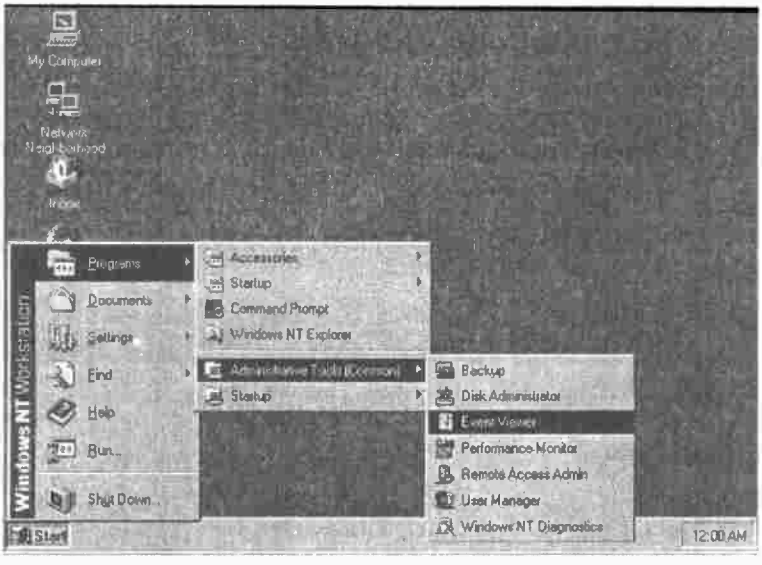
تستطيع عند تشغيل مثل هذه البرامج الحصول على معلومات كافية عن الموارد المستخدمة فى الجهاز وتعقب سرية النظام والاطلاع على معظم محتويات النظام من مكونات وخدمات وبيئة عمل واتصال بالشبكة واستخدامات الذاكرة ومشغلات الأقراص والعرض المرئى لمعرفة سلامة توصيفها وعملها .

عـند حـدوث مشكلة فى أثناء العمل على الشبكة قد تظهر رسالة رمزية تبين موضع الخلل أو العطل .



معاين الأحداث Event Viewer

مثال آخر لبرامج معاينة الأحداث فى الشبكة توفره ويندوز عند عطل جهاز هو بـرنامج معاينة الأحداث Event Viewer الذى يقوم بكتابة معلومات عامة Info والأخطـاء Error التى تحدث والتنبيهات Warnings التى تتم فى جهاز ويضع هذه المعلومات فى ملف .



يمكـن للـبرنامج اسـتعراض محتويات ملف الولوج للنظام System log الذى

يحتوى على بيانات عن أخطاء النظام ، كما يمكنه أيضا استعراض ملف الولوج للتطبيقات Applications Log وتسجيل الأحداث فى ملف ثنائى بامتداد EVT. .

عند تشغيل البرنامج يمكن من قائمة الولوج Log استعراض الولوج إلى النظام System Log والأمن Security Log والتطبيقات Application Log .

يحتاج اختيار بيانات الأمن Security Log لتشغيل التدقيق Audit للحفاظ على الأمن Security فى الشبكة بمتابعة نشاط المستخدمين ومعرفة استخداماتهم .

تتبع الأعطال

كل مكونات الشبكة عبارة عن أجزاء يمكن أن تعمل منفصلة ويمكن تتبع أعطالها منفصلة وهذا الأمر يسهل عملية الصيانة وإن كان يزيد من وقتها وعلى أية حال فإن الأعطال فى أى شبكة يمكن تصنيفها على النحو التالى :

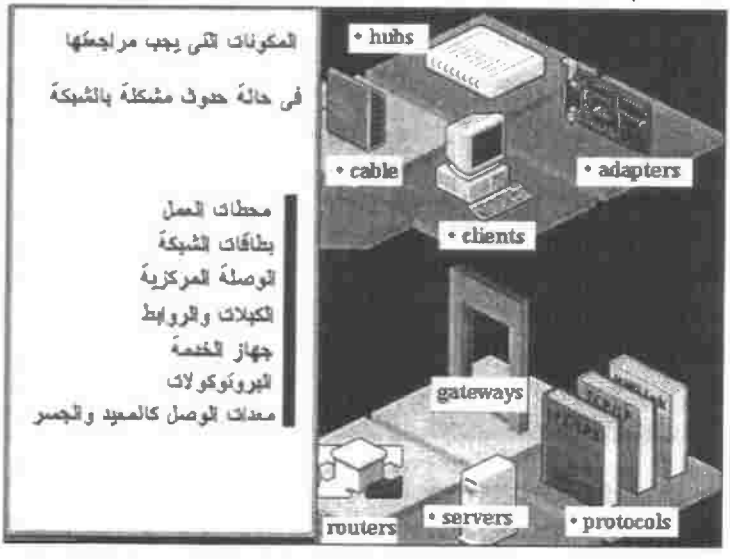
١- أعطال أجهزة الخدمة الرئيسية .

٢- أعطال محطات العمل الفرعية .

٣- أعطال نظم اتصالات الشبكة (تمديدات ومجمعات مركزية وأجهزة ربط) .

٤- أعطال التطبيقات والبرامج والموارد كالطابعة والفاكس .

٥- أعطال النظم الفرعية مثل الاتصال عن بعد .



إن كل مكون من هذه المكونات يجمع عدة نظم فرعية فى داخله كالتالى :

- جهـاز الخدمـة الرئيسى يجمع بين المكونات الوظائفية لجهاز حاسب مع شاشة ولوحة مفاتيح ومشغل قرص مرن ومشغل قرص مضغوط وقرص صلب قـد يكـون مقسـما مع بطاقة شبكة ونظام تشغيل الجهاز وتوصيف المكونات المادية ونظام تشغيل الشبكة وبروتوكولات الشبكة .
- كذلـك الأمـر بالنسبة لمحطة العمل الفرعية التى تتكون من شاشة ووحدة نظـام وقـرص صلب ومشغلات أقراص مرنة وأقراص مضغوطة مع بطاقة شـبكة ونظـام تشـغيل الجهـاز ونظام العميل لنظام تشغيل الشبكة وتوصيف المكونات المادية والبروتوكولات المستخدمة .
- نظام الاتصالات تجمع بين البطاقات وطريقة التوصيل والتمديدات والروابط Connectors وأجهزة التشبيك المشترك (المودم والقناطر والمعيدات والموجهات والبوابات وخطوط الاتصال) وبرامج البروتوكولات ونظام تشغيل الشبكة .
- أعطال التطبيقات والبرامج والموارد والخدمات كالطباعة والبريد يمكن أن تتواجد فى محطة فرعية أو فى بعض المحطات كما يمكن أن تتواجد فى جهاز الخدمة الرئيسى كما يمكن أن تكون موجودة فى أجهزة التشبيك المشترك .
- أعطـال النظم الفرعية قد تشمل بعض أو كل المكونات الموجودة والموارد المـتوفرة كالطابعة والفاكس وخدمات البريد الإلكترونى وخدمات مراقبة النظام وأجهزة التغذية الفورية وغيرها من النظم الفرعية الأخرى .

عـند هـذه الـنقطة يمكن فهم طبيعة أعطال الشبكة ومشاكل الصيانة فيها بفهم صـيانة وإصلاح المكونات منفردة مثل صيانة وإصلاح أجهزة الحاسب منفردة (كجهـاز خدمـة رئيسـى أو كجهاز محطة عمل) والطابعات منفردة وأجهزة الاتصـالات بالـبطاقات وطريقة التوصيل والتمديدات والروابط Connectors وأجهـزة التشبيك المشترك (المودم والقناطر والمعيدات والموجهات والبوابات وخطوط الاتصال) .

أيضا يمكن التعامل مع أعطال التطبيقات والبرامج والبروتوكولات ونظام تشغيل الشبكة منفردة كما يمكن التعامل مع النظم الفرعية لخدمات الطباعة والفاكس والبريد الإلكترونى ومراقبة النظام وأجهزة التغذية الفورية وغيرها من النظم الفرعية الأخرى منفردة (يمكن الرجوع إلى كتاب إصلاح وصيانة أجهزة الكمبيوتر – عبد الحميد بسيونى – مكتبة ابن سينا للطباعة والنشر) .

أعطال معدات التشبيك المشترك

تحتوى جميع معدات التشبيك المشترك مثل الصرة والموجه وبطاقة الشبكة والمعدل (المودم) الخارجى على لمبات بيان Led لبيان حالة التغذية الكهربية الواصلة إليها مع لمبات بيان تبين المكونات المتصلة بها ولمبات بيان حالة نقل البيانات عليها .

الصرة Hub كوصلة مركزية لتوصيل شبكة الأثير بكبل مجدول عليها لمبة بيان لكل توصيلة من توصيلات المحطات الفرعية التى توصل بها مع لمبة بيان التغذية الكهربية ولمبة بيان للصرة نفسها لبيان حالة نقل البيانات فيها .

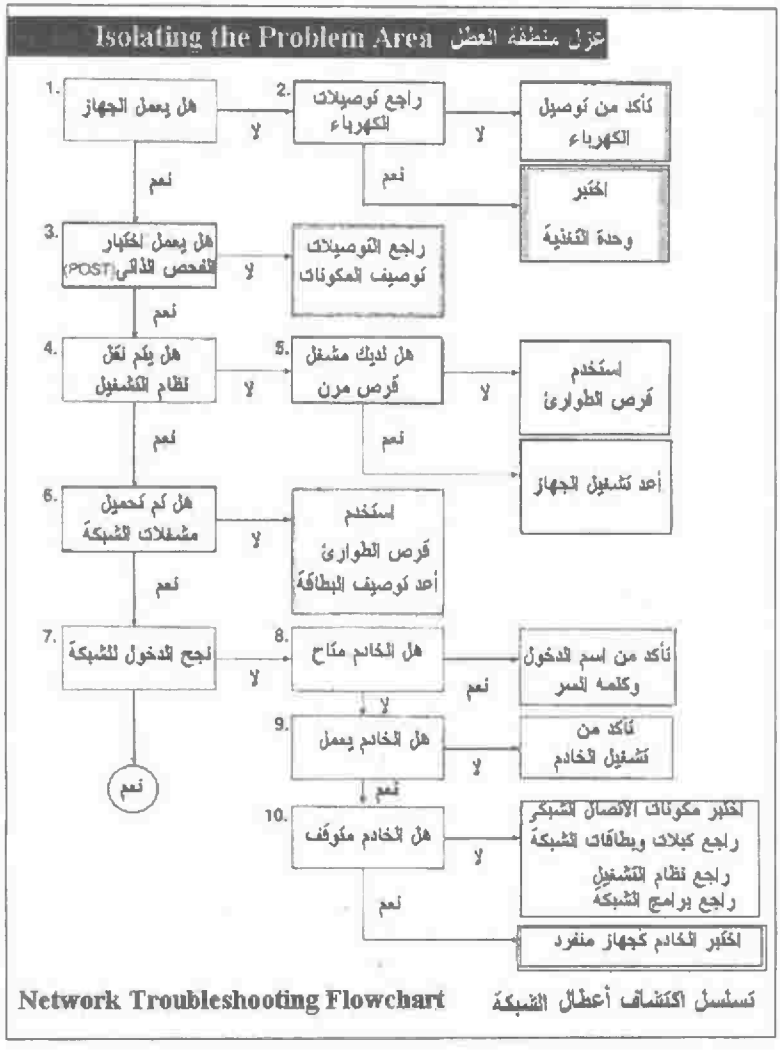
بالمثل فإن الموجه يحتوى على لمبات بيان لبيان حالة التغذية الكهربية ونقل البيانات .

حالة لمبات البيان تبين المكان الذى تذهب إليه عند حدوث عطل فى توصيلات شبكية تعتمد على مثل هذه المعدات .

مراقبة الشبكة تعتبر من الأساليب الأولى المستخدمة فى تحديد الأعطال التى تحدث .

يعتـــبر تجزئ المشكلة لتحديد مكان العطل فى الشبكة هو أحد الأساليب السهلة التى تساعد على التشخيص السريع .

الأجـــزاء الرئيســـية فى نظام الشبكة هى جهاز الخدمة الرئيسى ونظام التشبيك والمحطـــات الفرعية ونظام التشغيل وعطل كل واحد من هذه الأجزاء يكون له مظهر مختلف إلى حد كبير عن عطل الجزء الآخر .



المـــراجـــع

- إصـلاح وصـيانة أجهـزة الكمبـيوتر ـ مكتـبة ابـن سـينا للنشـر والتوزيع والتصدير ـ مهندس / عبد الحميد بسيونى .
- موسـوعة صـيانة وإصـلاح الكمبـيوتر ـ مكتـبة ابـن سـينا للنشـر والتوزيع والتصدير ـ مهندس / عبد الحميد بسيونى .
- شـبكات الكمبـيوتر (العمـل والتشـغيل والصـيانة) ـ الجـزء الأول والـثانى ـ مكتـبة ابـن سـينا للنشر والتوزيع والتصدير ـ مهندس / عبد الحميد بسيونى .
- الشبكات فـى ويـندوز اكس بى ـ مكتبة ابن سينا للنشر والتوزيع والتصدير ـ مهندس / عبد الحميد بسيونى .