الفصل العاشر

إدارة الشبكة المحلية

يبين الفصل المشاكل التى تنجم عن العمل فى بيئة الشبكة المحلية ومهام المشرف على الشبكة فى مناظرة الشبكة وتنظيم الملفات وتخصيص المستفيدين وإعداد أدلة الملفات وتحديدها وكيفية تبسيط العمل وأساليب ووسائل حماية البيانات وتحقيق السلامة الأمنية للشبكة ودور مدير الشبكة فى التأسيسات الأولية والصيانة ومراقبة الشبكة .

من الطبيعى أن تكون هناك مشاكل فى استخدام الشبكة وأجهزة الحاسب فيها وبرامجها وملفات البيانات بها لذلك تحتاج الشبكة إلى خطة منظمة للعمل بها .

إن تعيين شخص واحد لتنظيم الشبكة وحماية بياناتها وإدارة المهام فيها تعد عملية هامة فالوظائف المناطة به تساعد على حماية الشبكة من المشاكل التى تنجم أثناء العمل على الشبكة ، وفى الحقيقة تمثل الشبكة تحديا إداريا كبيرا يجب تناوله بشىء من العمق والفهم .

وظيفة إدارة الشبكة يمكن أن تتحدد بواحد من نوعين من الوظائف الإدارية فإما أن يكون هناك مشرف على الشبكة أو أن يكون هناك مدير لها ، إن وظيفة المدير هى إضافة مستفيدين وتطبيقات إلى الشبكة ومراقبة أمنية الشبكة .

ينبغى للمشرف على الشبكة أن يكون على قدر من الدراية الفنية العالية للقيام بدور فعال فى تشكيل النظام وتخصيص نظام العمل على الشبكة وتحليل أدائها وتنظيم الاستفادة منها ومن تطبيقاتها وغيرها من المهام التى يجب عليه تنفيذها.

إن أكثر نهج عملى لتنظيم الشبكة هو تعيين شخص واحد لإدارتها ، تكون واجبات مشرف الشبكة هى التأكد من أن الفاعلية الوظيفية للشبكة فى أحسن صورها وأن البيانات فى الشبكة محمية من الضياع أو سوء الاستعمال .

إن المشرف يقوم أيضا بنفس الوظائف التى يقوم بها مدير الشبكة ، لكن بدراية فنية أكبر ، فهو يلعب دورا فعالاً فى تشكيل النظام وتخصيص تطبيقات الشبكة وأعمالها الإجرائية ويتدخل فى مفهوم الصيانة وتنفيذها وتوقيتات القيام بها بالإضافة إلى الدور الرئيسى فى الحفاظ على سرية البيانات .

إن الشركات ذات الشبكات الكبيرة ونظم الاتصالات المتعددة تحتاج بالضرورة إلى تطوير مستوى خبرة إدارة الشبكة حتى يمكن الحفاظ على أعلى معدلات الأداء للشبكة والاستفادة القصوى من تطبيقاتها وهنا يقع على عائق المشرف على الشبكة واجب التطوير المستمر لنفسه ولأدائه ولمعلوماته وللنظام فى ذات الوقت .

١٠-١- مهام المشرف علي الشبكة

مهمة مناظرة الشبكة والتخطيط الأولى

تمتلك جميع الشبكات المحلية جهازا يستخدم للتخزين المركزى للبيانات والتطبيقات ويمكن أن يكون التخزين المركزى على واحد أو أكثر من الأقراص الصلبة ، إن أول شىء يجب عمله فى الشبكة هو اتخاذ القرار السليم حول كيفية استعمال نظام تخزين البيانات والتطبيقات بأحسن شكل ، ويتطلب ذلك مناظرة المناطق المرتبطة بالشبكة .

لنفترض وجود مدير للشركة يحتاج للتعامل مع عدد معين من الملفات ذات الموضوعات المعينة فى شبكة العمل المحلية الموجودة فى الشركة كما يوجد اثنان من العاملين فى السكرتارية بالإضافة إلى المستخدمين الموجودين فى الأقسام المختلفة ولهم حقوق دخول مختلفة على الملفات والأدلة .

لنفرض كبيان لتنظيم الملفات والأدلة فى القرص الصلب العامل على جهاز الخدمة الرئيسى فى الشبكة أن الملفات المشتركة للشركة هى ما يلى :

١- قاعدة بيانات العملاء .

٢- قاعدة بيانات طلبات البيع .

٣- العقود والعطاءات .

٤- المراسلات .

٥- المبيعات .

٦- سجلات المبيعات الفردية .

٧- سجلات شئون العاملين .

٨- المشتروات .

٩- المخازن .

١٠- سجلات المديونية .

١١- سجلات التأمينات .

١٢- سجلات الضرائب .

بعد وضع قائمة بأقسام الشركة المختلفة وبيان المستفيدين العاملين على الشبكة وتحديد ملفات البيانات المطلوبة للعمل فى الشركة فإن العنصر التالى فى تخطيط الشبكة يتضمن الكيان المادى للشبكة .

لنفرض أن الشبكة المتكونة فى الشركة تحتوى على جهاز خدمة رئيسى وأن محطات العمل الفرعية هى عبارة عن جهاز حاسب شخصى لكل مستفيد كما تتواجد فى الشبكة طابعة نقطية واحدة سريعة وطابعة ليزر واحدة ، وأن فى كل قسم من أقسام الحسابات والمبيعات والاستلام والشحن طابعة نقطية للأعمال الفرعية البسيطة فى هذه الأقسام ، وبالإضافة إلى هذا فإن جهاز الخدمة الرئيسى يحتوى على قرص صلب واحد ولكل حاسب شخصى يعمل كمحطة فرعية مشغل أقراص مرنة .

تنظيم الملفات

بعد تحديد الملفات (باستعمال قائمة مختصرات) تكون المهمة التالية هى تجميعها على أساس القسم الذى ينشىء بيانات كل ملف وعليه فسجلات شئون العاملين والتأمينات والمراسلات ستأتى من الإدارات الخاصة بها كما يمكن أن تعد سجلات المبيعات الفردية منها أيضا لذا يمكن وضعية تسمية لهذه المجموعة من الملفات على أساس أنها المجموعة التى يتعامل معها المدير أو تلك التى تحمل اسما رمزيا هو اسم « Admin» كاسم مختصر للدلالة عليها ، أما بالنسبة لقسم الحسابات والمديونية والضرائب فيمكن تسميتها باسم الحسابات « Acct» .

وينشىء قسم الشحن والاستلام سجلات الشحن من وإلى الشركة كما يسيطر هذا القسم على البضاعة ومتابعة سجلات طلبيات الشراء والتخزين ويمكن وضع تسمية مختصرة له مثل اسم (SR) .

أما قسم المبيعات فهو مسئول عن إنشاء وتحديث بيانات سجلات العملاء والموردين والمبيعات والعقود والعطاءات وأهداف المبيعات ومن الميسر وضع تسمية له باستخدام مفهومه بالاختصار « Sales » .

وفيما يلى قائمة بالملفات والعاملين عليها من أقسام وإدارات الشركة :

الملـــــف	الاسم الرمزى للقسم
قاعدة بيانات العملاء	Sales
طلبيات المبيعات	Sales
العقود والعطاءات	Sales
المراسلات	Admin
أهداف المبيعات	Sales
طلبيات المبيعات المنفردة	Admin
سجلات شئون العاملين	Admin
المشتريات	SR
المخازن	SR
الشحن	SR
الحسابات	Acct
سجلات التأمينات	Admin
سجلات الضرائب	Acct

تخصيص المستفيدين

الخطوة التالية للعمل هى تحديد المستفيدين وملفاتهم المطلوبة ونوعية الاستخدام المطلوبة للملفات المختلفة مع العلم أن قرار تحديد المستفيدين وصلاحياتهم المختلفة للتعامل مع الملفات خاضع للاختلاف من شركة إلى أخرى حسب تشكيلة الأقسام المختلفة فى الشركة والصلاحيات الممنوحة للعاملين فى الأقسام المختلفة فى الشركة ، لنفترض على سبيل التبسيط وجود ثلاثة مستفيدين فى النظام هم :

١ – المدير العام (M) .

٢ – محاسب قسم الحسابات (A) .

٣ – كاتب الشحن والاستلام (Clerk) .

٤- السكرتارية (Sec) .

وبهذا فإن الملفات التى سيحتاج هؤلاء المستفيدين للوصول إليها هى كما يلى :

الملـــف	القسم	المستفيد
قاعدة بيانات العملاء	Sales	M,A,sec
طلبيات المبيعات	Sales	M,A,sec
العقود والعطاءات	Sales	M,A,sec
المراسلات	Admin	M,sec
أهداف المبيعات	Sales	M,A,sec
سجلات المبيعات الفردية	Admin	M,A,sec
سجلات شئون العاملين	Admin	M,sec
المشتروات	SR	M,A
المخازن	SR	M,sec, A
الشحن	SR	M,A
الديون	Acct	M,A
سجلات التأمينات	Admin	M,A
سجلات الضرائب	Acct	M,A

لكل واحد من هؤلاء المستفيدين استعمالات مختلفة للملفات فقد يحتاج مستفيد ما إلى الاطلاع على محتويات ملف ولكنه لا يريد القيام بتحديث محتوياته لذلك فإن هذا المستفيد يحصل على تصريح بالتعامل مع الملف على أساس امتياز القراءة فقط بينما يكون هناك مستفيد آخر يحتاج إلى التعامل مع هذا الملف لقراءة محتوياته وتعديل البيانات فيه وبالتالى تحديث هذا الملف لذلك فإن هذا المستخدم الأخير يحصل على امتياز قراءة الملف والكتابة فيه .

من وجهة النظر هذه فإن الملفات يمكن تقسيمها من حيث التصاريح

والامتيازات الممنوحة للمستفيدين تبعا لمتطلبات العمل .

إعداد أدلة الملفات

لكل مستفيد مجموعة حقوق معينة لملفات معينة فى أدلة معينة وتختلف كل مجموعة من الأفراد عادة فى استخداماتها ولكن فى المؤسسات الكبيرة يمكن وضع المستفيدين ضمن مجموعات ذات امتيازات وصول متماثلة للأدلة.

لدى المدير فى العمل أو مدير الشبكة بصفته مشرفا على الشبكة شمولية أكبر فى الحقوق وامتيازات أكثر فى التعامل مع الملفات والأدلة والمستخدمين .

بالرغم من أن المدير قد يحتفظ بميزة القراءة فقط لبعض الملفات فإن مشرف الشبكة يقدر على السماح لنفسه بأن يغير هذه الامتيازات ليضيف لنفسه من الامتيازات ما يجعله قادرا على التعامل مع كافة موارد النظام شأنه شأن كل المستفيدين فى أى وقت .

يتم إعداد أدلة الملفات لجميع المستفيدين فى الشبكة بنفس الطريقة حيث يمنح كل مستفيد دليلا للملفات يعكس احتياجات ذلك المستفيد وفاعليته الوظيفية ضمن الشركة .

هناك نقطة هامة يجب ملاحظتها بشأن امتيازات الأدلة ، فعلى الرغم من تخزين مقدار كبير من البيانات فى ملفات الشبكة المختلفة بصيغة قابلة للمشاركة فإن عملية فتح جميع ملفات البيانات لكل المستفيدين ليست ضرورية بل هى فى الواقع عملية غير مرغوبة .

صحيح أن النظام الجيد للتشغيل فى الشبكة يجب أن يوفر مرونة فى هيكلية أسلوب الوصول للمستفيد فإن الشبكة تكون أسهل كثيرا فى الاستخدام عندما يمكن تقليل الأعمال والمهام التى يجب أن يتعامل معها المستفيد فتلك السهولة فضلا عن أنها تسهل عمله وتقلل من الأعباء المطلوبة منه فإنها توفر تكاملا للبيانات .

إن الهدف النهائى من عملية تنظيم الشبكة هو منح كل مستفيد مقدارا من الصلاحيات التى تناسب فعلا ما يحتاجه لإنجاز متطلبات أداء واجب معين ، فمثلا المستفيد فى قسم الشحن والاستلام لايستخدم ملفات الحسابات أو تقارير المبيعات أو حتى نظام التشغيل لذلك يجب ألا تكون هذه الملفات متاحة له لاستخدام ولو على سبيل التدريب ، فللتدريب أوقاته ومهامه التى يضطلع بها مسئولون .

تحديد الملفات العاملة فى الشبكة

لتوضيح التنظيم لنظام نموذجى فقد تم وضع فرضيات عامة حول البيانات التى ستنقل إلى وحدة التخزين المركزية (القرص الصلب الرئيسى) وفى الواقع فإن تحديد الملفات العاملة فى الشبكة يختص بما يجرى فى القرص المركزى بصورة أكثر من الاهتمام بكيفية ترتيب تلك البيانات .

إن أول قرار يجب على المدير اتخاذه هو كيفية جعل البرمجيات التطبيقية تدخل الشبكة فبعض من حزم التطبيقات قد تملأ مجموعة أقراص مرنة ، فلو استخدمت عدة حزم فى النشاط الاعتيادى فيجب امتلاك كمية هائلة من الأقراص فى صندوق كبير وبالتالى استنفاد وقت أطول لتبديل الأقراص أو البحث عنها لذا فإن وضع جميع هذه البرامج على قرص صلب لن يؤدى فقط إلى زوال الحاجة إلى الأقراص المرنة ومكان تخزين البرامج وإنما أيضا يمكن من جلب أى برنامج ببساطة عن طريق أمر معين وتوفير الوقت المستغرق فى البحث والتشغيل .

فى حالة كون التطبيقات ذات إصدار متعدد المستفيدين وليست محمية من النسخ فمن الممكن تخزينها على قرص صلب ومشاركتها من قبل أى شخص فى الشبكة ، ويجب إدراج البرامج فى دليل ملفات كل مستفيد قد يستعمل هذه البرامج وفى معظم الحالات يتم تحديد الوصول إلى البرامج بامتياز القراءة فقط وبهذا تكون البرامج قابلة للاستعمال ولكن بدون إجراء تعديلات ويتم منح

المدير بالطبع امتيازات القراءة والكتابة للبرامج لأغراض صيانتها .

يستطيع المدير إضافة روتينات خدمية والقيام بتخصيصات المفاتيح عند الحاجة، ولكن الشيء المهم الواجب ملاحظته أن ملفات المستفيد تنشأ جميعها بنفس البرامج وبذلك تكون جميع الملفات متوافقة .

عندما تكون البرامج المفضلة محمية ضد النسخ وغير متوفرة بإصدار متعدد المستفيذين فإن الخيارات تكون محدودة أكثر وفى هذه الحالة تبقى البرامج التطبيقية ضمن محطات عمل منفردة وتكون ملفات البيانات فقط الناتجة من هذه التطبيقات على القرص الصلب .

يجب تحديد القرارات التى تخص امتيازات الوصول للملف فى الوقت الذى يتم فيه قبول الملف للتخزين ، وتتضمن هذه القرارات استفسارات حول المسموح لهم بالوصول إلى هذه الملفات وتحديد مستوى الوصول لكل منهم .

فى معظم ملفات البيانات تكون امتيازات الوصول المناسبة لإيجاد القوائم وتحليل البيانات واستخراج التقارير هى امتيازات للقراءة فقط وبالتالى تكون المعلومات منشورة ومتوافرة لكن بدون تبديل فلو أضيفت إلى ملفات القرص المركزى بيانات غير مقصودة فإنها سوف تهمل .

استعمال الأسماء الوصفية لتحديد الملفات

قد يبدو ملف البيانات كلغز لأى شخص عدا الذى قام بتكوينه ، ومن أسهل الطرق لحل هذه المشكلة هو استعمال تسميات مألوفة وشائعة لهذه الملفات فإذا تم اختيار الأسماء بشكل جيد فإن نظرة سريعة على الدليل قد توفر معلومات كافية حول محتوى هذه الملفات .

تسمح نظم التشغيل عامة باستخدام أسماء للملفات ، ويختلف طول هذا الاسم تبعا لنظام التشغيل وفى نظام تشغيل القوص يمكن استعمال ثمانية رموز لاسم الملف متبوعة بثلاثة رموز أخرى إضافية تعزل عن اسم الملف بنقطة تسمى

بالامتداد ، ويحتفظ نظام تشغيل القرص برموز وامتدادات معينة لاستخدامه الشخصى .

فى مثل هذا النظام يمكن البدء بالتسمية باستعمال نوع من المعلومات التى تساعد فى معرفة نوع الملف أو استخدام بعض الامتدادات المألوفة كإضافة لهذا الغرض مثل (DOC) لملف وثيقة ، أو (TBL) كملف جداول وغير ذلك من الامتدادات .

فى حالات عديدة ، هناك حاجة إلى معرفة من قام بآخر تحديث للملف وعليه يمكن استخدام حروف من اسم الملف مثل الحروف الثلاثة الأولى للقيام بهذا التحديد بوضع الحروف الأولى من اسم الشخص فى الحروف الأولى من الملف ثم تشغيل باقى الحروف الخمسة ببيان عن نوع الملف أو استخدام علامات خاصة كعلامة النسبة المئوية (٪) أو ($) لكل مستفيد عند تسميه لملف .

يجب الحفاظ على معيارية معينة فى تسمية الملفات فلكتابة اسم ملف فى قسم المبيعات يحتوى على سجلات مبيعات شهر فبراير فإن اختيار الاسم يكون على الصورة التالية (SALEFEB % DAT) . فبينما يشير الجزء الأول من الاسم إلى أنه عن مبيعات ، يبين الجزء الثانى أن هذه المبيعات تخص شهر فبراير وتبين علامة النسبة المئوية أن الملف قد أعد بواسطة محمود ، وهو الشخص الذى يكون ملفاته باستخدام هذه العلامة كما تم حفظ الملف على صورة بيانات .

من المعروف أن وقت وتاريخ آخر تحديث يعتبر مهما ولنفرض أن لك الخيار أن تختصر هذه المعلومات فى اسم الملف ، وأن معظم الشبكات لديها على أى حال ساعة تبين الوقت والتاريخ لكل كتابة وهذا الوقت والتاريخ يصبح مفيدا إذا صاحب اسم الملف .

بغض النظر عن التسميات الملائمة ، فإن كل مستفيد مطالب بالحصول على معلومات عن الملف قبل تحديثه فمثلا كجزء من إجراءات تحديث الجدول

الإلكترونى يجب على المستفيد أن يعرف متى تم تحديث هذا الجدول فى آخر مرة.

استخدام أسلوب واجهة المستخدم

تعد شبكة العمل المحلية من الإمكانيات ذات القوة العالية وفى معظم الأحيان يكون نظامها معقدا ، وقد تمثل هذه الصورة من التعقيد حاجزا قويا من الرهبة للمستخدم كما قد تورطه فى مشاكل كثيرة نتيجة عدم الألفة والخبرة .

تكون من أكبر مسئوليات المشرف على الشبكة القيام بمهام التدريب الدورى لطاقم العمل فى الشبكة لكن الأكثر فائدة هو أن يقوم مشرف الشبكة بتفصيل الشبكة حسب احتياجات وإمكانيات كل مستفيد ، بحيث يرى كل مستفيدالقدر الكافى والضرورى له من الشبكة ويعمل عليه دون تعقيد بحيث تصبح السياسة المتبعة للإفادة من الشبكة هى تبسيطها للمستفيد .

إن تبسيط مهام العمل على الشبكة ممكن بعدة وسائل مثل استخدام القوائم والنوافذ والملفات الحزمية وبرامج المنافع التى تقوم بتنفيذ خدمات القوائم والواجهة البيئية النهائية للمستخدم .

عند الدخول إلى الشبكة تعطى هذه النوعية من الوسائل قائمة رئيسية تضم عدة اختيارات أو تعطى إطارا رسوميا يعطى الإمكانيات المتاحة من البرامج والاختيارات المختلفة عليها كما أن الملفات الحزمية تنفذ الأداء بتسلسل لايستدعى التدخل الكثير للمستخدم ، وفى جميع الأحوال يكون أول ما يظهر على الشاشة أمام المستخدم هو مجموعة من الاختيارات وقد تكون هناك إمكانية المساعدة الفورية التى تتيحها مثل هذه النوعيات من البرامج .

يجب أن لا يكون استخدام هذه النوعية من البرامج عبئا فى حد ذاته بحيث تكون معقدة كما أنها ليست ترفا لكنها وسيلة ناجعة لعدم اختلاط المهام أو عدم وضوح الأداء للمستخدم فإذا لم تتيسر هذه البرامج فإن تكوين القوائم يكون سهلا بواسطة المشرف على الشبكة .

لنفرض مثلا أن هناك عدة اختيارات لتشغيل عدد من البرامج إذن يمكن تكوين برنامج بسيط يحتوى على أسماء البرامج بحيث تظهر هذه الأسماء على الشاشة أمام المستخدم وتكون هناك رسالة فى أسفل الشاشة تطلب الضغط على حرف أو رقم معين لانتقاء الخيار المطلوب وتنفيذ البرنامج الذى يخصه وقد تكون هذه الاختيارات مثلا :

١- معالجة النصوص .

٢- الجداول الإلكترونية .

٣- قاعدة البيانات .

٤- نظام تشغيل القرص .

٥- الخروج من النظام .

فلو ضغطت على رقم (١) فسوف تبرز قائمة فرعية لبرامج معالجة النصوص واختيار الدليل الفرعى للبيانات وجهاز الإخراج وذلك بالضغط على مفاتيح معينة ، وبعد ذلك يتم تحميل التطبيق وعند حفظ الملف يتحول مسار النظام إلى دليل البيانات المختار وعند طباعة الملف فإن الإخراج يذهب إلى الطابعة المختارة ، وبعد الخروج من التطبيق المختار فإن نظام القوائم يتسلم السيطرة على الحاسب مرة أخرى ويعرض القائمة الرئيسية ثانية .

ظاهريا يستخدم جميع مشرفى الشبكات فى الشركات الكبيرة أسلوب قوائم الخيارات والتى توفر جهود تحديد المسارات والأدلة ، وفى الواقع فإنه بسبب قوائم الخيارات للواجهة النهائية سوف لا يحتاج المستفيدون معرفة أى شيء عن الشبكة .

يمكن أن تكون قوائم الخيارات بسيطة كملف نصوص يعرض الخيارات وعدة ملفات حزمية تقوم بتنفيذ الإيعازات ، فمثلا قد تنشيء ملف دفعات بالاسم (A.BAT) وعند ضغط المستفيد على المفتاح (A) فإن الملف ينفذ مكونا

جميع المسارات الضرورية ومحملا التطبيق المطلوب بحيث تحدث جميع هذه العمليات آليا دون أن يلاحظ المستفيد أى شيء عدا الخيارات والنتائج .

تتوافر برامج منافع القوائم الأكثر تقدما وتتيح تشكيلة منوعة من شاشات قوائم الخيارات والقوائم الفرعية وبقية الخدمات (لمزيد من التفاصيل حول برامج منافع القوائم يمكن الرجوع إلى كتاب برامج منافع الكمبيوتر – عبد الحميد بسيونى – دار ابن سينا للطباعة والنشر) .

بالنسبة للمستفيد الذى يعمل على برنامج معين أو تطبيق واحد (Single - application) فمن الواجب تجنيبه استخدام قوائم الخيارات وذلك بعمل ملف حزمى تلقائى التنفيذ (AUTOEXEC.BAT) يقوم الحاسب بتنفيذه تلقائيا فى بداية وقت الدخول فى الشبكة أو عمل ملف حزمى عادى يتم تنفيذه عندما يكتب المستخدم اسم هذا الملف ، ويتكون هذا الملف من مجموعة من الأوامر التى تتولى تحديد المسارات وتحميل التطبيق بدون إشعار المستفيد وبهذا فإن مستفيد الشبكة فى هذه الحالة سيعيش فى بيئة أبسط من تلك القائمة على حاسب مستقل .

حماية البيانات (Data Protection)

تتعدد الوسائل والأساليب المستخدمة لحماية البيانات ومن حسن الحظ أن قدرات وإمكانيات وأساليب حماية البيانات قد تقدمت إلى حد كبير ، ولا يقف أمر حماية البيانات عند حد الحماية من الفقد أو التلف وإنما يتعداها إلى الحماية من التخريب والسرقة والدخول غير الآمن لملفات البيانات وهو الأمر المعروف بسرية وأمن البيانات والمعلومات .

نظام الحماية المصمم بشكل مناسب له تأثيره الجيد ولا ضرر منه ويمكن أن يعزز العمليات الاعتيادية ، ومن أقل المشاكل فى فقد البيانات هى فقدان البيانات نتيجة عطل الجهاز ذلك أن غالبية الشبكات المحلية تستخدم أنظمة متعددة للتغلب على مشاكل الأعطال المادية .

استخدام أجهزة النسخ الاحتياطى

تعتبر عملية النسخ الاحتياطى من العمليات الهامة فى شبكة العمل المحلية والتى يجرى تنفيذها يوميا لحفظ نسخة احتياطية من كافة بيانات القرص الصلب على وسيط تخزين احتياطى حتى إذا ما حدث تدمير للبيانات بطريق الخطأ أو بالتخريب المقصود تكون هناك نسخة احتياطية لإعادة تسجيل البيانات منها مرة أخرى .

يمكن استخدام أنواع مختلفة من الأجهزة والوسائط التى تستخدم لحفظ البيانات احتياطيا مثل وحدات التخزين الأنوية من الأقراص المرنة بأنواعها والأقراص الصلبة الثانوية والأشرطة الممغنطة .

يعتبر جهاز الشريط الممغنط من أكثر الأجهزة استخداما فى النسخ الاحتياطى فى شبكات العمل بسبب عدد من المميزات التى تميزه عن غيره من الوسائط الأخرى المستخدمة فى النسخ الاحتياطى ، ومن هذه المميزات :

١ – السعة الكبيرة للشرائط المستخدمة .

٢ – رخيصة التكلفة بالنسبة لغيرها من الوسائط .

٣ – إمكانية وضعها فى أماكن خارج مكان الحاسب .

اختيار نظام الشريط وتقييم نظام الشريط يبدأ بدراسة عدد من المتغيرات التى تلعب دورا رئيسيا فى تقييم نظام الشريط المستخدم ومنها :

* حساسية الشريط .
* العمر الافتراضى لعمل الشريط .
* العمر الافتراضى لعمل جهاز إدارة الشريط .
* آلية عمل جهاز إدارة الشريط .
* الشركة المنتجة لجهاز إدارة الشريط .

* الشركة المنتجة للشريط .

* موقع الشريط فى داخل جهاز الإدارة .

* توافر الحماية والتأمين للشريط .

* ترتيب البيانات على الشريط وأسلوب توزيع هذه البيانات .

* سرعة الاستدعاء والتخزين وغيرها من العوامل الهامة التى تبين أساس استخدام وتفضيل نوعية معينة من الشرائط وأجهزة إدارتها .

تصحيح الأخطاء (Correcting Errors)

تستخدم أجهزة تشغيل الشرائط الممغنطة عددا من الوسائل لتصحيح الأخطاء فى خلال عمليات القراءة والكتابة ومن بين النظم المستخدمة لتصحيح الأخطاء نظام التحقق من البيانات بالقراءة بعد الكتابة (read - after- write verification) وبموجب هذا النظام فإن البيانات يتم قراءتها بعد أن تكتب فإذا اختلفت البيانات المقروءة عن المفروض تسجيله ، أى لم تتم الكتابة بشكل ناجح فإن الكتابة ستعاد مرة أخرى .

إن تحقيق القراءة بعد الكتابة عادة يكون كافيا مع الأخطاء المتسببة من الوسيلة المستخدمة فى التسجيل أى أن الخطأ يحدث بسبب عطل فى مكون من المكونات المادية مثل الشريط نفسه أو رأس القراءة والكتابة أو غيرها من الأسباب المادية وكمثال لذلك تصل نسبة الخطأ المقدرة بسبب الأوساخ على الشريط إلى ٩٥٪ من إجمالى الأخطاء .

اعتبارات تخص البرامجيات

عند شراء نظام للنسخ الاحتياطى بمكوناته المادية من شرائط وجهاز إدارة الشريط يتم فى نفس الوقت الحصول معه على البرامج الخدمية الخاصة بتشغيل الجهاز ومن الواجب أن تكون البرامج سهلة الاستخدام .

هناك نوعان شائعا الاستخدام من الأنظمة هما النظام الانسيابى ونظام الملف بعد الملف ، وتستخدم أنظمة الشريط الانسيابية لعمل نسخة احتياطية من الملفات على الشريط لتخزين كميات كبيرة من البيانات مثل محتويات القرص بالكامل، أما طريقة الملف بعد الملف والتى تسمى كذلك باسم (البداية – التوقف (start - stop) فإنها يمكنها أيضا عمل نسخة احتياطية لكميات كبيرة من البيانات إلا أن لها فائدة هامة تتحدد فى قدرتها على إعادة تخزين الملفات على القرص الصلب بشكل منفرد لكل ملف .

حماية بيانات نظام فى مجال احتمال الخلل System Fault Tolerant

مجال احتمال الخلل هو عبارة عن خطة تعتمد على أجزاء النظام الإضافية التى تمنع فقدان البيانات بسبب الخلل أو العطل فى أى جزء منفرد من النظام ويمكن النظر إليه على أساس أنه خاصية من خصائص النظام تعتمد على أنه إذا حدث عطل فى أى جزء منفرد من نظام الشبكة فإن نظام الشبكة نفسه يمكن أن يستمر فى العمل ويعتبر احتمال الخطأ مجالاً آخر من المجالات المستخدمة لحماية البيانات يمكن استخدامه مع نظام النسخ الاحتياطى .

إن شبكات العمل المحلية طبقا إلى بنائها الأساسى لها درجة عالية من احتمال الخلل ، فإن الخلل فى محطة عمل منفصلة يجب ألا يؤثر على بقية شبكة العمل المحلية ولا يمنع هذا محطة العمل من أن تستخدم كحاسب شخصى منفرد .

ينجز نظام احتمال الخلل عن طريق إضافة أجزاء إضافية أو احتياطية وعند حدوث خلل فى الجزء الرئيسى فإن الجزء الاحتياطى يكون بديلا لتنفيذ العمل بدلا من النظام الرئيسى حتى يعود النظام الرئيسى للعمل بعد التغلب على المشكلة التى سببت عطله .

بعد أن يتم تجهيز وإعداد نظام احتمال الخلل وتشغيله فى الشبكة فإن حدوث خلل فى النظام الرئيسى يستتبعه أن تظهر رسالة من رسائل الخطأ تشير

إلى ظاهرة الخلل ، وفى هذه الحالة يمكن للمشرف على الشبكة أن يقوم بإعطاء أمر لجعل النظام الثانوى يعمل ، ولا ينفى هذا أن هناك النظم التى تعمل آليا فور حدوث خلل فى النظام .

لنأخذ مثالاً لنظام احتمال الخلل فى شبكة نوفيل – مثلا – فهذا النظام فى شبكة نوفيل يسمى بنظام التغلب على أعطال النظامSystem Fault Tolerant (SFT) وينقسم إلى ثلاثة مستويات .

يتضمن المستوى الأول إنشاء نسخة احتياطية من البيانات الضرورية التى تخص جدول مواقع الملفات وغيرها من البيانات الأساسية على القرص ، ويعطى النظام أيضا مراقبة ديناميكية للقرص وفق جدول تحقيق القراءة بعد الكتابة بحيث تتم القراءة بعد كل كتابة فإذا كانت البيانات غير قابلة للقراءة تعاد كتابتها فى منطقة أخرى من القرص ويتم تأشير المنطقة الأولى باعتبارها رديئة حتى لا يتم استخدامها مرة ثانية عند تسجيل بيانات على القرص .

يوفر المستوى الثانى من مستويات التغلب على أعطال النظام مرآة للقرص (disk mirroring) بحيث يقوم بعمل ازدواجية للقرص الصلب بحيث يكون كل النظام الفرعى للقرص متضمنا وحدة التحكم فى القرص والكابل والقرص متطابقين فإذا حدث خلل فى أى جزء من الأجزاء (أو كلها) فى النظام الرئيسى فإن النظام المزدوج سيكون فى حالة عمل ليحافظ على عمل النظام .

ازدواجية القرص لها فائدة مؤثرة فى تحسين أداء العمل إذ يمكن التعامل مع طلبات القراءة الآتية بشكل متوازى ويؤدى ذلك إلى مضاعفة عرض قناة القرص ولأن قناة القرص لها دور مهم فى الأداء فإن هذه الزيادة فى العرض يمكن أن تحسن بشكل فعال فى أداء النظام .

بالرغم من أن عمليات الكتابة تتطابق على القرصين لذا لا يوجد تحسن فى الأداء فى الكتابة ، لكن بسبب أن قراءة البيانات من القرص هى النوع الرئيسى من الطلبات فى معظم الشبكات لذلك فإن التحسن فى الأداء الناتج عند القراءة

يكون مؤثرا .

المستوى الثالث من مستويات التغلب على أعطال النظام له خصائص المستويين الأول والثانى بالإضافة إلى تعامله مع خدمات الشبكات المزدوجة فالنظام مصمم بحيث أن حدوث خلل فى أحد الخدمات لا يؤثر على باقى الخدمات إذ تستمر الخدمات الأخرى فى العمل .

يتضمن كل من المستوى الثانى والثالث جدولة حماية البيانات المسماه بمسارات المعاملات ، ففى نظم قواعد البيانات قد يؤدى الخلل فى واحدة من محطات العمل أو البرامج التطبيقية إلى خلل كامل لقاعدة البيانات كلها .

لنفرض أن محطة عمل بدأت فى عملية كتابة انتقالية فى ذات الوقت الذى يجرى فيه تنفيذ عملية فهرسة بقاعدة البيانات ، ففى هذه الحالة إذا حدث عطل فى محطة العمل أو فى أحد التطبيقات قبل أن تتم عملية التحديث فإن عملية الفهرسة سيتم قطعها وبالتالى يجعل ذلك قاعدة البيانات غير قابلة للاستخدام .

إن النسخة الاحتياطية للفهرسة المسجلة فى مسارات المعاملات ستبقى حتى يتم إكمال كل المعاملات التى تتم على عملية الفهرسة وبالتالى فإن النسخة الاحتياطية ستظل طالما أن كل المعاملات لم تتم على عملية الفهرسة وما تم تنفيذه فقط هو تنفيذ عدد من المعاملات الجزئية وعليه فإن المعاملات الجزئية التى تمت سيتم إهمالها وتظل قاعدة البيانات نفسها محمية مما جرى .

لا يوجد بالطبع نظام منيع من الأعطال تماما كما أن مجال تحمل الخلل يجب ألا يتم اعتباره بديلا لنظام النسخ الاحتياطى فمجال تحمل الخلل مثلا لا يمكن أن يحمى ضد أخطاء العامل على الجهاز .

نخرج بإيجاز يقول أن الإجراء الجيد للنسخ الاحتياطى بالاشتراك مع الخصائص الملازمة لشبكة العمل المحلية يقلل من خطر فقدان البيانات أو الوقت الضائع فى شبكات العمل المحلية .

عمل أرشيف للملفات

يمكن استخدام أنظمة النسخ كأجهزة لتنظيم الأرشيف ومع الأرشيف فإن البيانات التى من النادر استخدامها تمسح من القرص الصلب وتخزن على الشريط فى مكتبة الأرشيف وعند الحاجة إلى الملفات فبالإمكان تحميلها إلى القرص الصلب .

للأرشيف فوائد من ناحية السرية والتخفيف من عبء ازدحام القرص الصلب ، فجداول المرتبات وبيانات العاملين مثلا يمكن أن تخزن فى مكتبة الأرشيف بدلا من القرص وعند الحاجة إلى استخدامها تحمل إلى الشبكة وبعد انتهاء العمل تحمل ثانية إلى مكتبة الأرشيف وهذا الإجراء يصنف طبقة أخرى من السرية .

السلامة الأمنية (Security)

من السهولة تأمين سلامة الحاسب الشخصى حيث توضع الأقراص المرنة فى مكان أمين ويوضع الحاسب فى مكان مغلق إلا أنه عند ربط الحاسب بشبكة من الحسابات فإن السلامة الأمنية تصبح أكثر تعقيدا .

يمكن للسارق أو المخرب أن يصل إلى أية نقطة من الشبكة حيث يمكن له الدخول إلى النظام بواسطة الحاسب الشخصى الذى يعمل كمحطة عمل وسرقة أو تخريب البيانات إذا امتلك المعرفة اللازمة لذلك .

يجب تحديد التهديدات الموجهة ضد بيانات الشبكة كما أن الحجم المادى للبيانات ذات القيمة هو عنصر آخر يؤخذ فى الاعتبار عند تحليل احتمالات السرقات مما يضيف حسابات إضافية .

يعتبر التخريب الداخلى تهديداً آخر للشبكة ولبياناتها فالعامل المستاء من رئيسه فى العمل قد يقرر إتلاف أو تغيير الملفات المهمة كما قد يحدث التخريب نتيجة للمزاح أو اللعب أو عدم الفهم الجيد لطبيعة محتويات الملفات .

من الواجب تدريب العاملين على العوامل الأمنية والعمل بحزم على عدم تجاوز حدود العمل فى العبث بالملفات والشرح الجيد لطبيعة محتويات الملفات .

إن تحليل المخاطر المنظورة للشبكة سيجعل فى الإمكان الإجابة على العديد من الأسئلة حول حجم المخاطر ومن أين تأتى ؟ وما هى الإجراءات المناسبة والضرورية لإبعادها وما هى الخطوات اللازمة لبناء أمن وسرية الشبكة .

مستويات السلامة (Levels of Security)

لا توجد سلامة بنسبة مائة فى المائة رغم المهارة الكافية والوقت الكافى فإن أنظمة السلامة الفعلية تعتمد على عدة مقاييس لتحقيق السلامة فى شبكة العمل المحلية :

١ – تحقيق السلامة المادية Physical security

٢ – استخدام الهوية الشخصية Personal Identification

٣ – تحويل البيانات إلى شكل غير مفهوم Encryption

٤ – استخدام الحاسب الشخصى الخالى من الأقراص Diskless computer

٥ – الحماية ضد إشعاع السلك Protection against cable radiation

٦ – تحقيق سلامة الاستدعاء Call - back security

السلامة المادية

السلامة المادية للموقع فى الشبكة ولمحطات العمل الموجودة فى الشبكة تتحقق عن طريق عدد من الإجراءات المادية المناسبة مثل وضع قفل على الحاسب نفسه أو وضع حارس على الباب .

الهوية الشخصية

الخط الأول للسلامة فى معظم الشبكات هو الهوية الشخصية ، ويمكن استخدام عدد من التقنيات لحصر التعامل مع الأفراد المخولين فقط باستخدام الشبكة وأجهزتها وتستند كل هذه التقنيات إلى نوع ما من التعريف كأن يكون التعريف شخصيا باستخدام واحد أو أكثر من الآتى :

* استخدام زى خاص .
* استخدام بطاقة للدخول إلى غرف الحاسب .
* استخدام بطاقة توضع على صدر المستخدم (بادج خاص) .
* استخدام مفاتيح لدخول غرف الأجهزة .
* استخدام أسماء للدخول إلى النظام وكلمة سر المرور .

إن الاتصال بالشبكة يتطلب من المستخدم طباعة كلمة سر المرور ويتم اختيار كلمات السر بحيث يسهل تذكرها مما يجعلها سهلة التخمين هذا من ناحية ومن ناحية أخرى فإن كلمات المرور يجب أن يتم تحديدها من قبل مشرف الشبكة نفسه وليس من قبل الأفراد ويمكن الحد من هذه السرية غير الجيدة بإصدر كلمات عبور جديدة على فترات غير منتظمة .

للعديد من أنظمة التشغيل للشبكات برنامج خدمى خاص بكلمة المرور يسمح للمستخدمين المخولين بالتعامل مع الشبكة أن يقوموا بتغيير كلمات المرور الخاصة بهم وعلى ذلك فإن من واجب المشرف على الشبكة أن يقوم بإلغاء إمكانية تشغيل هذا البرنامج الخدمى بواسطة المستخدمين للشبكة .

السرية عند الدخول للنظام

يجب تصميم نظام الشبكة بشكل يمنع محاولات الاتصال بالنظام إلا بصعوبة بالغة ومن الأمثلة المستخدمة فى غالبية البرامج عدم ظهور كلمة المرور

على الشاشة عند كتابتها بواسطة المستخدم لها خلال عملية دخوله إلى النظام .

إن عدد محاولات كتابة كلمة المرور يجب أن لا يزيد عن ثلاث محاولات وبعد ذلك يتم إخبار المشرف على الشبكة بفشل عملية الدخول للنظام ، وهناك إجراء أكثر من التأمين يتم عن طريق تنفيذ عملية مراقبة محاولات الدخول على الشبكة إذ يمكن أيضا تسجيل عدد مرات محاولات كتابة كلمة المرور فى كل محطة عمل أو لكل مستخدم بحيث تتم مراقبة نظام كلمات المرور فى الشبكة بصفة عامة مما يحد من محاولات الدخول غير الشرعى .

هناك أسلوب آخر من أساليب استخدام كلمة السر عن طريق تحويل رموزها إلى شكل آخر خلال محطة العمل ثم تعاد رموزها الأصلية فى المعالج المركزى حتى لا يمكن استخدام البيانات المارة بالسلك .

تحويل البيانات إلى شكل غير مفهوم

تحويل البيانات إلى شكل غير مفهوم فى معظم الشبكات المحلية يستخدم فقط عندما يكون تهديد السلامة أمرا جوهريا ، ومعظم تقنيات تحويل البيانات إلى شكل غير مفهوم تستند إلى عمليات رياضية معقدة تعتمد على الأعداد الأولية.

هناك نوعان رئيسيان من عمليات تحويل البيانات إلى شكل غير مفهوم هما:

١ – تحويل الربط (Link) الذى يستخدم لجعل البيانات غير قابلة للقراءة عند انتقالها من نقطة إلى نقطة مثل اتصال حاسبين شخصيين مما يمنع قراءة البيانات بشكل عرضى .

٢ – تحويل نهاية إلى نهاية (end-to-end) يحمى البيانات فى أى مكان من النظام .

مفتاح تحويل البيانات إلى شكل غير مفهوم (Eneryption Keys) هو عبارة عن صيغة لتشفير البيانات وتفسيرها عن طريق برامج مفتاحية توزع على المستخدمين للشبكة المخولين بتغيير شكل البيانات إلى شكل غير مفهوم حتى إذا

استطاع غيرهم الوصول إليها لم يتمكنوا من فك شفرتها واستخدامها أو الاطلاع عليها .

النظام الخاص ببرامج المفاتيح السرية يكون صعبا فى الاستخدام ومكلفا فى الصيانة وخصوصا عند زيادة عدد المشتركين فى الشبكة وللتخلص من هذه المساوىء فإنه يمكن استخدام برنامج عام كمفتاح تحويل البيانات عامة فى الشبكة يسمى بالمفتاح العام (Public Key) .

توجدطريقة أخرى لتأسيس نظام تشفير فى الشبكة وتحويل البيانات إلى شكل غير مفهوم تتم بوضع صندوق تحويل البيانات للشكل غير المفهوم بين كل محطة عمل محلية وبين اتصالها بالشبكة وعند ذلك فإن كل البيانات التى تنتقل ضمن الشبكة وتلك التى تخزن على القرص الصلب سيتم تحويلها إلى شكل غير مفهوم ولكن هذه الطريقة غير مجدية إذا أمكن الوصول إلى الشبكة من أى محطة محلية فالبيانات فى المحطة المحلية سوف تكون عبارة عن بيانات واضحة غير مرموزة .

الحاسب الشخصى الخالى من الأقراص

من محاسن اتصال الحاسب الشخصى بشبكة العمل المحلية واستخدامه كمحطة فرعية قدرته على العمل منفردا وإمكانياته فى التخزين المحلى لبياناته وبرامجه المستقلة ، وترتبط درجة الاستقلالية مع توافر مشغلات الأقراص المرنة والصلبة له ومجموعة الأقراص المرنة الشخصية للبيانات التى توضع عليها وفى نفس الوقت فإن هذه الاستقلالية تخلق تهديدين لسلامة البيانات .

يكون التهديد الأول بصورة لا ينتبه إليها ، ذلك أن وجود نسختين من البيانات أحدها على القرص المركزى لجهاز الخدمة الرئيسى والثانية محلية فى محطة العمل يعنى أن كل نسخة من البيانات يتم تحديثها بشكل مستقل عن الأخرى وبالتالى فإن البيانات الجديدة فى إحدى النسختين قد يتم فقدها عند دمج النسختين معا .

التهديد الآخر يتمثل فى أن مشغل القرص المرن المحلى لمحطة العمل يسمح بسرقة البيانات فالشخص الذى يتصل بالشبكة وبجهاز القرص المرن المحلى يمكنه نسخ كميات كبيرة من البيانات على الأقراص المرنة فى دقائق فقط .

إن إلغاء جهاز مشغل القرص المرن المحلى يعنى إبعاد خطر سرقة البيانات ولكنه أيضا يقلل قوة واستقلالية الحاسب الشخصى وأحد البدائل الممكنة هو استبدال جهاز القرص المرن المحلى بقرص صلب محلى .

إن الحاسب الشخصى الخالى من الأقراص مقيد بمشاكل البرامج فهناك العديد من البرامج التطبيقية المصممة للتنفيذ عن طريق وضع قرصها فى مشغل القرص المرن المحلى فقط كنوع من الحماية لها ضد النسخ كما أن نظام التشغيل نفسه عادة يتطلب على الأقل مشغل أقراص مرنة محلى واحد على الأقل لكى يقوم بالعمل لذلك فقد يصبح هذا القيد صعب التنفيذ فى الواقع العملى .

الحماية ضد إشعاع الكابل

قد تتعرض المعلومات لأى شخص خلال انتقالها فى الكابلات ويمكن استخدام عدة طرق لحماية البيانات المارة فى الكابل بوضع الكابل فى أماكن تحقق منع تحطيم الكابل مع ملاءمة متطلبات البناء كنوع من السلامة المادية للكابل أما بالنسبة لسلامة المعلومات فى الكابل فيجب وضع الكابلات فى أماكن محمية حيث يكون التعرض لها أقل احتمالا .

إن إشارة الراديو التى تنتشر فى الهواء على شكل موجات يمكن بسهولة التعرض لها وسرقة المعلومات فيها ومن المعروف أن هذه النوعية من الإرسال لا تقتصر على إشارات الراديو المنتشرة فى الهواء فكابل البيانات أيضا يعطى إشارات كهرومغناطيسية يمكن التقاطها .

يمكن التخلص من احتمال اعتراض الإشارات باستخدام الكابل المغلف،

وهناك طريقة أخرى للتخلص من مشكلة إشعاع الكابل بشكل كامل وهى باستخدام كابل الألياف الضوئية ولأنه صعب الاختراق جدا فهو مثالى لأغراض السلامة .

سلامة الاستدعاء

محطات العمل عن بعد هى جزء من مجالات العمل للعديد من شبكات العمل المحلية وتمكن المستعمل من الاتصال بالشبكات عن بعد والدخول إلى نظام الشبكة واستخدام النظام كما لو كان المستعمل يستخدمه محليا ، وتأمين السلامة لهذا النوع من الوصول يتطلب مقاييس خاصة .

سلامة الاستدعاء وإدارة خدمات المستخدمين هى جزء من الأنظمة المزدوجة التى يمكن استخدامها مع شبكة الحاسب الشخصى عن بعد فعند رغبة محطة من المحطات التى تعمل عن بعد فى الاتصال بالشبكة تستطيع نظم الاستدعاء تحقيق هذا الاتصال أو الاستدعاء وكل ما هو مطلوب من الشخص المستخدم هو أن يشير إلى رغبته فى الاتصال بالشبكة وسينظم جهاز سلامة الاستدعاء للموقع الاتصال بالشبكة .

نظام سلامة الاستدعاء يحافظ على أسبقية الاتصالات إذا كانت هناك عدة محطات عن بعد تريد تحقيق الاتصال بالشبكة ففى حالة ما إذا كانت كل خطوط تحقيق الاتصال المتوفرة مشغولة بعدد من المحطات التى تتصل فعليا بالشبكة فإن نظام سلامة الاستدعاء يرتب طلبات المحطات فى طابور انتظار يعتمد على أسبقية الاتصال ويبلغ النظام المستخدم بموقعه من طابور الانتظار .

يقوم نظام سلامة الاستدعاء أيضا بحفظ معلومات إحصائية عن عمليات المرور والاستدعاءات التى تتم من المحطات التى تعمل عن بعد .

١٠-٢- دور مشرف الشبكة في التأسيسات المادية الأولية

سجل التأسيسات (The Installation Long)

تعتبر الشبكة بلا شك أكثر تعقيدا من الحاسب المستقل المنفرد وبعكس الحاسب الشخصى المنفرد فإن الشبكة غير قابلة للنقل بالإضافة إلى أن وقت عطل الحاسب الشخصى المنفرد لا يعطل كليا عمليات المؤسسة بينما وقت عطل الشبكة يمكن أن يؤدى إلى توقف العمل فى المؤسسة .

يجب على القائم بوظيفة الإشراف على الشبكة أن يقوم فى بداية تأسيس الشبكة بالاحتفاظ بسجل للنظام يتضمن التفاصيل الكاملة عن أنواع الكابلات والروابط (connectors) المستخدمة وطريقة تنصيب الكابلات والروابط واسم مجهز الكابل ووصف محددات الشبكة وتحديد عدد العقد وبيان أطوال الكابلات والمسافات بين العقد ورسم المخطط التوضيحى العام لنظام الكابلات ، وترقيم كل حاسب شخصى فى الشبكة وكل قرص صلب ومشغل أقراص مرنة وطابعة وأى جهاز آخر فى الشبكة ثم تمثيل الترقيم على المخطط المرسوم بالإضافة إلى الاحتفاظ بسجلات كاملة لكل جهاز على حدة شاملا بيانا كاملا بمواصفاته الفنية وتوصيفه التجهيزى .

توزيع الكابلات (Cable Distribution)

غالبا ما يتم تركيب الكابلات بوضعها على الجدران الداخلية أو الخارجية من المكان وهذه الطريقة غير مرتفعة الثمن وسريعة التنفيذ وسهلة الصيانة ، ومعظم الطرق المستخدمة الشائعة لتوزيع الكابلات تتم بوضع الكابل على واحد من الأشكال التالية :

١- سطح مدرج .
٢- قناة تحت الأرض .
٣- السقف .
٤- تحت الأرضية .

التخطيط مقدما

قبل بداية تركيب الشبكة من الضرورى للمشرف على الشبكة أن يخطط جيدا للتغييرات المستقبلية والنمو والإصلاحات الدورية التى تتم فى كل من المبانى والشبكة ، فإن مثل هذا التخطيط مهم لأنه يشكل صورة توزيع الكابلات عند بداية تأسيس الشبكة بحيث لاتختلط المهام والأعمال ولا يؤثر بعضها على الآخر .

معالجة الكابلات والروابط

قبل شراء شبكة عمل محلية فإن المعلومات الأساسية عن خصائص الكابل يجب أن تكون واضحة ليس فقط بسبب طريقة توصيل الكابلات (توبولوجى الشبكة) لكن أيضا من وجهة نظر التأمين والسرية ومن وجهة نظر الاحتياجات اللازمة للتمديدات الفعلية بناء على شكل المبنى وأيضا من وجهة نظر أسلوب معالجة الكابلات فى التوصيلات المختلفة .

للكابل المحورى القياسى سلك توصيل مركزى مغلف بغلاف خارجى بينما الكابل الذى له غلاف ثانى يسمى ثلاثى المحور (triax) ، وهناك الكابل الثنائى (Twinax) الذى يوجد فيه سلكان داخليان وغلاف واحد ولا يمكن استبدال الكابلات بسهولة مثل استخدام الكابل الثلاثى بديلا عن الكابل المحورى العادى دون إجراء تحويرات متعددة ، لهذا يجب معرفة خصائص الكابلات قبل تنفيذ التوصيلات حتى يمكن معرفة مدى الحاجة إلى محولات (adapters) تسمح بربط الكابل المزدوج مثلا مع موصل الكابل المحورى .

قد تسبب الرطوبة مشاكل متعددة لتوصيلات الشبكة فإذا وصلت الرطوبة إلى نهاية الكابل المزدوج فإنها سوف تغير من الخصائص الكهربائية لهذا الكابل وتسبب تأكلا فى مادته وتحللا للعزل الكهربى فيه لذلك يجب حماية الكابلات من الرطوبة بوضعها فى مكان يمكن تغطيتها بمواد حافظة .

يمكن شراء كابلات ملائمة للمواصفات المطلوبة فى بناء الشبكة كما يمكن أيضا بناء هيكل الكابلات عن طريق اختيار مجموعة من الكابلات بأطوال مختلفة واستخدام روابط الكابلات الخاصة ، ومن أنواع الروابط الشائعة الاستخدام فى الشبكة الرابطة من نوع BNE وهى تضيف مقاومة قليلة لخط توصيل الكابل ولا توجد حاجة إلى تدريب خاص لكيفية تركيبها وتوصيلها .

هناك نوعان أساسيان متوافران لكابلات بناء الشبكة هما كابل ضفيرة بمفتاح ربط (wrench-crimp type) وكابل ضفيرة العدة (tool-crimp)

النوع الأول يمكن إعادة استعماله وله رابط يجب توصيله باللحام ، ويجب الانتباه عند تعرض الرابط والكابل لحرارة اللحام أو إلى أى مصدر آخر ، أما النوع الثانى لا يحتاج إلى لحام إلا أنه يحتاج إلى أدوات تضفير خاصة لتركيبه.

هذان النوعان من الروابط متماثلان فى الأداء وقوة الربط ، والفرق الوحيد هو أن رابط ضفيرة مفتاح الربط يتطلب وقتا أطول فى التركيب ، ويمكن استخدام الرابط البرميلى BNE خاصة مع كابلات RG-62 .

قبل تأسيس الكابل يجب فحصه بدقة والتأكد من عدم وجود أى قطع أو تلف فى الغلاف ثم اختبار صحة التوصيل الكهربى للكابل وللروابط .

الحماية من التداخل (interference)

عند التخطيط للشبكة المحلية فإن أحد الأهداف الرئيسية التى تؤخذ فى الاعتبار هو تقليل التداخل الكهربائى فى النظام كله مع ملاحظة أن التداخل يتولد داخليا وخارجيا وينتج هذا التداخل من عدة أوجه من بينها استعمال أسلاك توصيلات طويلة وانتقال البيانات بواسطة المجالات المشعة القريبة الناتجة عن المعدات الكهربائية ويمكن تقليل هذا التداخل أو إزالته باستعمال نوعية جيدة من الكابلات والتأكد من إحكام توصيل روابط الاتصال بشكل جيد وتجنب أى مصدر كهربى يولد مجالات كهرومغناطيسية قرب الكابلات .

فى الواقع الحقيقى قد يكون من المستحيل تجنب مصادر التداخل الكهربى دون جهود كبيرة وتكلفة إضافية ، وفى بعض الأحيان تكون مشكلة التداخل متناوبة مثل ظهور التداخل عند بداية جهاز التكييف أو أحد المصاعد فى المبنى لكن فى جميع الأحوال يجب التقليل من التداخل على المعدات .

الأرضية هى عنصر مهم آخر فى تأسيس الشبكة الجيد وقد ينشىء مشاكل متعددة فقد تكون أحد مصادر التداخل وتأريض الأجهزة يسمح للنظام الكهربائى بامتصاص الجهود الكهربية الزائدة التى قد تتلف النظام وأجزاءه ، ومعظم الشبكات المحلية لها أرضية كافية فى تصميمها المادى لكن يجب التأكد من توصيلها جيدا .

١٠-٣- دور مدير الشبكة في الصيانة

تأتى الشبكة المحلية مع معدات تكميلية لجعل كل واحد من المستخدمين فى الشبكة قادرا على تنفيذ عمليات محددة ، وتلبية احتياجاته ويمكن أن تكون محطات العمل فى الشبكة مؤسسة لتنفيذ تطبيقات فردية لكن فى النهاية يبقى العمل الجماعى هو الأساس الذى يبنى عليه مفهوم الشبكة وتؤسس المحطات الفرعية بحيث تعطى مرونة كافية وقوة لروافد الشبكة .

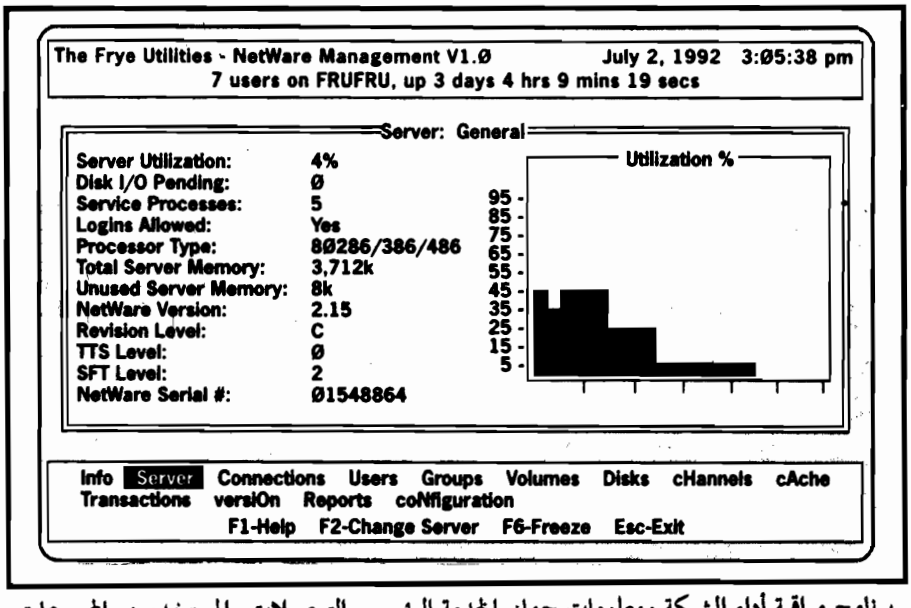
لمعالجة موقف الشبكة ومحطات العمل يجب أن يكون لكل شبكة مشرف له معرفة كافية بطبيعة أعمال الشبكة والمحطات الفرعية فيها وليس ضروريا أن يكون مبرمجا لكن يجب أن تكون له دراية بالبرامج المستخدمة فى الشبكة ويكون مدركا للشبكة ولنظام التشغيل وللبرامج الخدمية .

المدير هو جزء مكمل لتشخيصات الشبكة وهو يحدد طريقة عمل الشبكة ويراقب أداء الشبكة لملاحظة أوقات الاستجابة الأبطأ ونسب الأخطاء العالية وتقع على عاتقه مسئولية تنصيب محطات العمل وصيانة تطبيقات الشبكة ونسخ الملفات وإنجاز المهام الإدارية الأخرى كما أن سلامة الشبكة هى أيضا من مسئولية المدير .

مراقبة الشبكة (Network Monitoring)

من مهام المدير مراقبة الشبكة دوريا لمراقبة نسبة الاستخدام لكل مستخدم وعدد المحاولات المعادة وغير ذلك لملاحظة مدير كفاءة الشبكة فى العمل أحد الأرقام المساعدة هو عدد المعاملات المكتملة فى مدة من الوقت والسجلات يجب أن تحفظ بالساعة وباليوم وبالشهر .

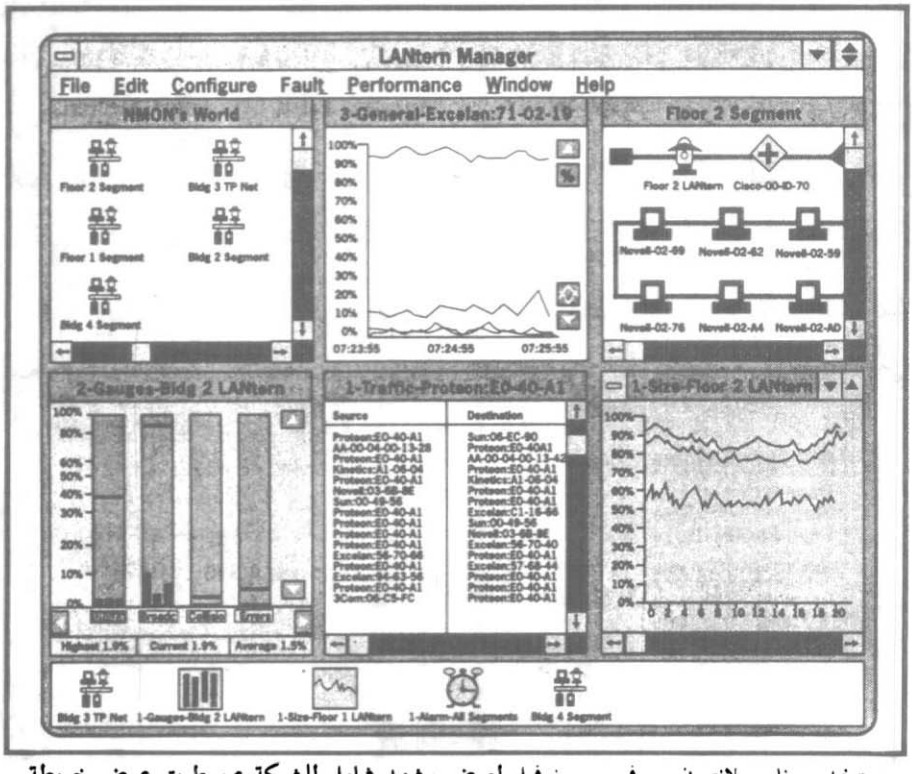
مثل هذه السجلات ستبين ساعات ذروة الاستخدام فى الأيام والشهور بحيث يمكن تنظيم أوقات الذروة بشكل أكثر كفاءة لتسمح بتوزيع عبء العمل كما تساعد هذه السجلات على تحديد أماكن المعوقات فى استخدام الشبكة سواء أكانت هذه المعوقات فى سلك توصيل أو فى محرك القرص أو فى جهاز الطباعة أو فى جهاز الخدمة الرئيسى .



برنامج مراقبة أداء الشبكة ومعلومات جهاز الخدمة الرئيسى والتوصيلات والمستخدمين والمجموعات ومناطق التخزين على الأقراص الصلبة والأقراص وتوليد التقارير وهو برنامج «فراى» ويظهر فى الشكل عرض بيانات جهاز الخدمة .

شكل (١٠-١) مراقبة أداء الشبكة

يخرج المشرف على الشبكة من مراقبته للشبكة ببعض المؤشرات التى تحدد أماكن الخلل فى نظام الشبكة فإذا كانت لمبة بيان القرص الصلب مضيئة معظم أو كل الوقت فإن القرص الصلب قد استخدم أكثر من طاقته ويكون النظام بحاجة إلى قرص صلب أسرع أو قرص صلب ثان أو يحتاج قرصا ثانيا إضافيا سريعا.



يستخدم برنامج لانتيرن سيرفس من نوفيل لعرض مشهد شامل للشبكة عن طريق عرض خريطة توصيلات الشبكة (فى الجزء الأيمن العلوى) وتوصيلات الشبكة فى المبنى (الجزء الأيسر العلوى) ورسم بيانى اتجاهى وإحصائيات المرور فى الشبكة وإحصائيات إجمالية للشبكة ويعمل البرنامج فى بيئة النوافذ على جهاز الخدمة الرئيسى فى الشبكة برامج مراقبة الشبكة .

شكل (١٠-٢) مراقبة أداء الشبكة

نادرا ما تكون الشبكات ساكنة فنمو الشبكة والتخطيط لنموها يعتبر عملا إجباريا وتكون عملية مراقبة الشبكة مقياسا للأداء يساعد على فهم احتياجات النمو والتخطيط له ويجب على المدير أن يكون قادرا على تقدير الاحتياج

للتوسع لكى يمكن التخطيط للتطور التالى .

أداء الشبكة عادة يعرف بالاستجابة السريعة وبالتوفر الجاهز ، لذلك فإن بيانات وقت الاستجابة يجب أن يحافظ عليها لكل حاسب شخصى فى الشبكة وللشبكة ككل ولذلك فإن مراقبة الشبكة لا يعنى فقط مراقبة أداء الأجهزة بل يعنى أيضا مراقبة أداء مختلف حزم البرامجيات التطبيقية .

مراقبة التطبيقات يمكن أن تلعب دورا خاصا فى كل من تقدير الخدمات والتخطيط للتطورات ، فمؤشرات الأداء تبين مدى فاعلية عمل الشبكة ومراقبة التطبيقات تشير إلى مدى إمكانية الشبكة على التعامل مع كل تطبيق منفصل وكيف يؤثر كل تطبيق على وقت الاستجابة .

يتضح مدى الاستفادة الفعلية من مراقبة الشبكة فى أنه يمكن استخدام معلومات الأداء فى السيطرة على تكاليف التشغيل فى الشبكة والمراقبة تعطى أيضا تفصيلاً بتحليل الإنتاجية لكل محطة عمل .

خلاصة

* مهام المشرف على الشبكة .
* مهمة مناظرة الشبكة والتخطيط الأولى .
* تنظيم الملفات .
* تخصيص المستفيدين .
* إعداد أدلة الملفات .
* تحديد الملفات العاملة فى الشبكة .
* استعمال الأسماء الوصفية لتحديد الملفات .
* استخدام أسلوب واجهة المستخدم .

لا يقف أمر حماية البيانات عند حد الحماية من الفقد أو التلف وإنما يتعداها إلى الحماية من التخريب والسرقة والدخول غير الآمن لملفات البيانات وهو الأمر المعروف بسرية وأمن البيانات والمعلومات ، ومن مهام الحماية :

استخدام أجهزة النسخ الاحتياطى

حماية بيانات نظام فى مجال احتمال الخلل System Fault Tolerant

عمل أرشيف للملفات

تحقيق السلامة الأمنية عن طريق

١- تحقيق السلامة المادية .

٢- استخدام الهوية الشخصية .

٣- تحويل البيانات إلى شكل غير مفهوم .

٤- استخدام الحاسب الشخصى الخالى من الأقراص .

٥- الحماية ضد إشعاع السلك .

٦- تحقيق سلامة الاستدعاء .

دور مشرف الشبكة فى التأسيسات المادية الأولية للعمل فى إنشاء سجل التأسيسات وتوزيع الكابلات والتخطيط مقدما ومعالجة الكابلات والروابط والحماية من التداخل .

المدير هو جزء مكمل لتشخيصات الشبكة وهو يحدد طريقة عمل الشبكة ويراقب أداء الشبكة لملاحظة أوقات الاستجابة الأبطأ ونسب الأخطاء العالية وتقع على عاتقه مسئولية تنصيب محطات العمل وصيانة تطبيقات الشبكة ونسخ الملفات .

من مهام المدير مراقبة الشبكة دوريا لمراقبة نسبة الاستخدام لكل مستخدم وعدد المحاولات المعادة .