الفصل الثالث

معالجة البيانات

مهام مدير الشبكة

NETWORK ADMINISTRATOR JOB

مقدمة:

إن وظيفة مدير الشبكة تتضمن مدى واسع من المسئوليات ، والمبادئ الأساسية.

سوف نتمكن من دراسة:

- إدارة التهيئة. Configuration Management
- إدارة الخطأ. Fault Management
- إدارة الأداء. Performance Management
- إدارة الأمان. Security Management
- إدارة الحسابات. Accounts Management

أولاً : إدارة التهيئة :

إنها عملية تتبع عناصر الشبكة وتهيئتها . التاريخ المفصل للتغيرات في الشبكة يقدم مساعدة هائلة للاصلاح . عندما تحدث مشكلة فإن أول شئ تريد معرفته هو (ماذا تغير؟) . إن قواعد بيانات إدارة التهيئة تستطيع أن تقول لك ذلك

ما يلى بضعة أشياء يجب أن تتبعها إجراءات إدارة التهيئة:

١- كل الهاردوير الذى به بيانات حيوية مثل تعديل الـ Firmware (ROM) عند التركيب (كمثال تغير التصميم بدون رقم نوع جديد) وتفاصيل التهيئة مثل المقاطعات Interrupt العناوين Addresses وهكذا .

٢- ملفات تهيئة نطاق العمل مثل Autoexec. bat , config. sys التى تسبب مشاكل كثيرة من تغيرات المستخدمين بها.

٣- برامج الشبكة مثل نتوير وإصدارات الطالب . Requester

٤- رخص البرامج للتأكد من أن شبكتك تعمل فى إطار التراخيص الرسمية بالاستخدام .

٥ــ المشاكل التى تصادفها والحلول المتعلقة بها والتاريخ الذى يعيد نفسه، فإن الحلول لمشاكل كثيرة قد تكون معروفة فوراً ومسجلة.

يمكنك أن تدير التهيئة المناسبة أكثر سهولة إذا استخدمت برامج مصممة للغرض تقدم نوفل برنامج (NMS) مثلاً .

ثانياً:إدارة الخطأ: Fault

يتضمن استخدام أدوات ومنتجات تبادر فى حل مشكلات الشبكة وتساعد على تصحيحها عندما تحدث.

عند حدوث انهيارات فإنه بالاستحواذ على الأدوات المناسبة نستطيع تحسين السرعة التى بها نتمكن من عزل وتشخيص العطل . كثير من هذه الأدوات تطورت حتى النقطة التى تخبر بالأحداث الغير مرئية كمشاكل ولكن هذا يضلل هبوط الشبكة . إذا بطاقة الشبكة تولد أعداد متزايدة من الرزم المدمرة حتى يكون من الواجب إعادة إرسالها ، فإن الأدوات السليمة تقرر الحالة قبل أن تفشل البطاقة أو تولد أخطاء كثيرة تفسر الأداء الكلى للشبكة.

إدارة الخطأ تشمل التمرينات التالية:

١ـ حفظ ونسخ البيانات Data Archiving and Backup :

ليس الحفظ والنسخ الاحتياطى جزء من إجراءات إدارة الخطأ ولكن أن تحفظ جيداً مجموعة أشرطة النسخ الاحتياطى مؤمنة ضد الفقد المفجع للبيانات . منتج نوفل للأرشفة والنسخ الاحتياطى هو برنامج. (SMS)

٢ـ تصميم سماحية الخطأ Fault Tolerant Design :

يمكنك تهيئة العديد من عناصر الشبكة من تهيئة سماحية الخطأ حيث أن انهيار هاردوير واحد لا يغلق الشبكة . توفر نتوير المستويات الثلاثة التالية لسماحية الخطأ للجهاز الرئيسىServer :

أ ــ **Set I (Hot Fix) :** يمكن الأجهزة الرئيسية من أن يسترد من أقل انهيار فى مادة الاسطوانة الصلبة.

ب ــ Set II (Disk Mirroring , Duplexing) : يمكن الأسطوانات الصلبة من أن تعمل بالتوازى حتى إذا حدث انهيار لإحداها لا يستدعى فقط البيانات أو أن تنقطع الخدمة.

جـ ــ Set III (Server Duplexing) : يمكن أزواج الأجهزة الرئيسية Pairs of Servers أن تعمل حتى لو حدث انهيار كلى لإحداها لن يسبب فقد للبيانات أو انقطاع للخدمة.

يمكنك تحقيق سماحية الخطأ بتصميم مسارات وافرة و HUB لسماحية الخطأ وجهاز استمرار التيار UPS وأخرى.

٣ـ نظم إدارة الشبكة :

بروتوكولات إدارة الشبكة تتضمن بروتوكول SNMP أى:
Simple Network Management Protocol

وهو البروتوكول الذى فى جعبته TCP/IP وهو البروتوكول المسيطر على إدارة الشبكة و (CMIP) أىCommon Management : Information Protocol

الأجهزة التى تدير هذه البروتوكولات (مثل الموجهات Router والهب HUB والسويتشات Switches والبطاقات Managed Nic وهكذا) تستطيع توليد رسائل إدارة الشبكة الموجهة إلى شاشة مراقبة إدارة الشبكة والتى تحلل معلومات الرسائل القادمة وتولد احصائيات عن أداء الشبكة والتحذيرات .

شاشة المراقبة أيضاً تستطيع أن يحوز على القدرة على إدارة أجهزة الشبكة عن بعد فى هبات HUB الشبكة المدارة ، كمثال فإن شاشة المراقبة Console قد تغلق ميناء هب الذى يولد عدد كبير من الأخطاء . إن SNMP هو إدارة لشاشة المراقبة والتى تستطيع أن تستخدم لها SNAP-in كمنتجات ملحقات لتمديد قدرتها.

٤ــ محللات البروتوكول Analyzer تستقبل كل الرزم على الشبكة وتفك رموزها للتحليل :

كثير من مشاكل الشبكة تضلل نفسها فـــى شـــكل رزم شـــاذة . مديـــرى الشبكات يمكنهم السيطرة على الرزم من سيل بيانات الشبكة واختبارها لشذوذيتها .

الاصدارات الأخيرة لمحللات البروتوكولات تؤدى كثير من التحليلات آلياً وتساعد الباقى . بعض النظم الخبيرة المدمجة تستطيع تشخيص مشـــاكل الشـــبكة بذكاء . تقدم نوفل برنامج Lanalyzer للويندوز.

٥ــ مختبرات الكوابل متاحة عند مستويات عديدة رفيعة:

أفضل مختبرات الكوابل Cables Tester تعزل الخطأ إلى منطقة للكيبل وتدلك مباشرة عندما يشتغل الكيبل.

ثالثاً : إدارة الأداء: Performance Management

إن إدارة الأداء هى الرفيق الفعال لإدارة الخطأ . مراقبة أداء الشبكة يوفر قاعدة أساسية للبيانات حيث لقطة أداء الشبكة الجيدة تحت الظروف الطبيعية التـــى تثبت قيمة تعريف فساد أداء الشبكة ــ وكمقياس للمقارنة ــ عند حـــدوث انهيـــار للشبكة

يجب أن تراقب العوامل Paramater الآتية :

ــ زمن الاستجابة. Response Time

ــ Throughput .

ــ حمل الشبكة Network Load وهو قياس لحركة المرور على الشـــبكة كنسبة مئوية لقدرة الأداء الكلى.

ــ الأخطاء : Errors

كل الشبكات تعرض بعض الأخطاء ولكن ارتفاع مستويات الخطأ تكـــون مؤشر واضح على مشكلة وشيكة الحدوث.

إدارة الأداء تمكنك من تخطيط تحسينات الشبكة فى المستقبل بالإضافـــة لمساعدتك فى توقع المشاكل . عند تصاعد الطلبات على الشبكة يمكنك إضافة قدرة قبل أن يدرك المستخدمين المشاكل.

رابعاً : إدارة الأمان: Security Management

أى فرد قد أدار نتوير من قبل يكون قد تعامل مع إدارة الأمـــان . أحـد مهامك هو أن تتجنب تهديدات الأمان وتنشئ إجراءات وقائيـــة . قـد تـأخذ فـى الاعتبار اختيار بعض تجهيزات الأمان التالية:

١ــ بناء أمان المستخدم والمجموعة.

٢ــ تطويع الوصول الداخلى والخارجى للبيانات.

٣ــ التعامل مع تخمينات مخاطر الأمان.

٤ــ إعداد سياسات الأمان.

٥ــ حماية الشبكة من الفيروسات.

٦ــ فحص الشبكة لتصيد أى اختراق للأمان.

نتوير (٤) تقدم فاحص للشبكة بتدعيم إنشاء فاحص الشبكة الذى يمكنهـم العمل مستقلين عن مديرى الشبكة . Network Administrator

فاحص الشبكة فى نتوير (٤) يستطيع مراقبة كل عمليات الشبكة لتصيـد اختراقات الأمان شاملاً أداء هؤلاء المراقبين. Supervisors

خامساً : إدارة الحساب : Accounting Management

تهتم إدارة الحساب بتخمين تكاليف اســتخدام مـوارد الشـبكة . بعـض المؤسسات تستخدم هذه المعلومة كى تتقاضى من الإدارات تكاليف استخدام الشبكة. هذه التكاليف يمكن استخدامها لتوفير الرغبة لاستخدام موارد الشبكة المحلية بذكاء. طلب المستخدم لسعة تخزين إضافية على الشبكة المحلية يؤدى إلى ارتفاع ســريع إذا ما تم التحكم فى ذلك.

مؤسسات أخرى تستخدم ببساطة معلومـات الحسـاب لتنظيـم التكـاليف وتخطيط التحسينات . عندما تجهز تحسينات الشبكة فإن بيانات الحساب تساعد فى تحديد نسبة التكلفة إلى الأداء لاختيارات مختلفة.

المهام العامة لمدير الشبكة

بصفة عامة هو مسئول عن انسيابية العمل على الشبكة ، ويعمل في خمسة حقول :

١ــ تنظيم المستخدمين : إعداد وحفظ وإلغاء سجلات المستخدمين ـــ إعداد تصاريح الوصول للمستخدم للاستفادة من موارد الشبكة ـــ والكشف عن مشاكل سجلات وتصاريح المستخدم.

٢ــ تنظيم الموارد : تخطيط وصياغة وحفظ موارد الشبكة مثل الطابعات والتطبيقات وقواعد البيانات.

٣ــ إدارة الأداء : من إدارة الأداء يمكنه الكشف عن المشاكل قبل وقوعها ــ قدرته على حذف أو إضافة أجهزة للشبكة أو توسعتها.

٤ــ توفير الحماية : لجعل الشبكة آمنة من التخريب المتعمد ومن الأعطال والأخطاء المفاجئة.

٥ــ إدارة المشاكل : القدرة على تصحيح وضع الشبكة عند تعطلها ويكون لديه خطة عمل جاهزة للطوارئ.

سوف نتناول بالتفصيل أهم استراتيجيات إدارة الشبكة.

أولاً : لتنظيم المستخدمين : User Manager في ويندوز إن.تي:

من قائمة بدء التشغيل اختار برامج ثم أدوات إدارية ثم مجال المستخدم ، اختار مستخدم جديد ، حدد معلوماته ثم اختار إضافة . كما يمكنك تحديد تاريخ ووقت دخول المستخدم إلى الشبكة وتحديد محطات العمل التى يمكنه الدخول منها كما يسمح له الدخول من بعد ويحدد له أيضاً ملف يستخدم عند كل دخول إلى الشبكة أيضاً يمكن إعداد سجل للمجموعات المكونة من عدة مستخدمين . وعند إضافة مستخدم لمجموعة يتم اكتسابه لكل حقوق المجموعة . وهى نوعان: مجموعة محلية ــ مجموعة عامة .

ـ **المحلية** : مجموعة على الشبكة تمنح حق النسخ الاحتياطى واستعادة الملفات

ـ **الشاملة** : تنظم سجلات مستخدمى الشبكة .

من قائمة بدء التشغيل اختار برامج ثم أدوات إدارية ثم مجال المستخدم اختار مجموعة شاملة جديدة أو مجموعة محلية جديدة . أدخل اسم ووصف المجموعة . تجد أعضاء المجموعة الجديدة فى قائمة . يضاف سجل المدير تلقائياً إلى لائحة الأعضاء . ثم تجد قائمة ببقية غير الأعضاء . لإضافة سجل جديد اختار الاسم من لائحة غير الأعضاء.

ثانياً: تنظيم الموارد: تجهز وندوز إن تى مجموعات جاهزة لتسهيل العمل : سجل العاملين – الإداريون – النسخ – الإدارى – الضيوف – المستخدمين – الطباعة – الجهاز الرئيسى.

ثالثاً : (لمراقبة الأداء : Performance Monitor): كمثال يسهل مراقبة أداء المعالج الرئيسى كما يستخدم بروتوكول TCP/IP لمراقبة : أجهزة الكمبيوتر الموجه والقنطرة والبوابة والمعدات الأخرى الشبكية.

فى الشبكات التى تستعمل NMP تحمل برامج عميل SNMP على الأجهزة المراد مراقبتها وبتطبيقات تتبع SNMP يمكن أخذ المعلومات اللازمة وتحليلها.

رابعاً : حماية الشبكة : يوضع مستوى الحماية اعتماداً على مدى الحماية المطلوبة. فبالنسبة للمعلومات عالية السرية مثل الطبية والقانونية يوضع مستوى عالى من الحماية أعلى من حماية معلومات عن بيع منتجات عادية .

وسياسة الحماية تغطى ما يلى :

١ـ خطة وصول المستخدمين إلى البيانات والموارد . من له حق الوصول ومتى وحق تعديل مستوى الوصول.

٢ـ شروط وضع الهاردوير أيها يغلق عليه الباب – لسلامته – وكيفية تأمين محطة عمل المستخدم عند غيابه عنها ـ وكيفية تأمين تمديدات الشبكة.

٣ــ سجلات المستخدمين وكيفية اختيار كلمات السر وفترتها ومستويات السماح والحقوق الممنوحة.

٤ــ تدريب المستخدمين على كيفية استخدام الشبكة لتحميها من التلف الغير مقصود .

٥ــ تصعيب الوصول إلى الجهاز الرئيسى للشبكة والتمديدات المختلفة لإبعادها عن التلاعب.

٦ــ بالنسبة للجهاز الرئيسى : يجب وضعه فى غرفة مغلقة أو فى غرفة مدير الشبكة والحرص من أن يأخذ شخص ما النسخة الاحتياطية أو الاسطوانة الصلبة كما يمنع أى شخص يحاول إصلاح عطل الجهاز الرئيسى بدون خبرة الحرص فى الدخول من بعد عبر الهاتف واتخاذ الاحتياطات التالية:

أ ــ تسجيل دخول المستخدم للتأكد من أصالة المستخدمين.

ب ــ التحدث فيما بعد . تسمح للجهاز الرئيسى بإقفال الخط مع المستخدم عن بعد وإعادة الاتصال فى رقم يتفق عليه.

جـ ــ التدقيق . تتم متابعة المستخدمين عن بعد وتسجيل وقت الدخول والملفات والمميزات التى يستعملونها من الشبكة.

٧ــ بالنسبة للتمديدات : بسبب سهولة التصنت على الشبكة من خلال تحديداتها فيمنع الاقتراب من هذه التمديدات من خارج المبنى أو داخله . ويجب تمريرها فى الجدران.

٨ــ كلمات السر وحق الوصول للموارد والبيانات : على مستوى المشاركة ــ على مستوى المستخدمين.

أ ــ على مستوى المشاركة : يجهز كل مورد بكلمة خاصة به : ويكون للقراءة فقط أو مشاركة كاملة أو حسب كلمتى السر واحدة لحق القراءة فقط والثانية للوصول الكامل له ــ يفيد ذلك الأسلوب فى الشبكات الصغيرة وشبكات الند

للند . أما فى الشبكات الكبيرة فيسبب حرجاً . فكلما زاد عدد المـــوارد زادت كلمات السر.

ب ــ على مستوى المستخدم : توجد كلمة سر لسجلات المستخدمين ــ سجل فيهـا الدخول على الشبكة ــ وتعطى تصاريح الوصول إلى مـوارد المسـتخدمين على أساس فردى. عند إضافة مستخدم جديد لقائمة المستخدمين الذين لهـــم حق الوصول يعطى تصاريح محددة للوصول منها : القراءة ــ التعديل ـــــ الإلغاء ــ أو منع الوصول.

هذا الأسلوب أقوى من مستوى المشاركة للتحكم فى الوصـــول للمـــوارد ويقلل من عدد كلمات السر.

٩ــ التدقيق : يتيح تتبع نشاط أى مستخدم على الشبكة . يمكنك معرفة أى مهمة قام بها ومتى. كما تعرف أى محاولة دخول صحيحة أو خاطئـــة أو تعديـــل لطريقة الحماية . فى وندوز إن تى من حوار . Audit Policy

١٠ــ الترميز : يتم ترميز الرسائل بحيث تصعب معرفة محتوياتها . يوجد تطبيق من شركة RSA يستعمل مفتاح عام يعرفه الجميع ومفتاح خاص يعرفـــه صاحب الملف . المعيار المعروف هو. DES

١١ــ الحماية من الفيروسات : يقوم الفيروس بنشر نفسه أولاً ثم أداء مهام مجـــددة مثل تدمير المعلومات . برامج الحماية تقوم عند بدء التشـــغيل بفحـــص الذاكرة ثم الاسطوانة الصلبة ثم إذا وجدت فيروس تعزلها وتدمرها وتلغى الملفات الملوثة . تأكد من نقل ملفات نظيفة من خارج جهازك إلى الشبكة. يجب التدريب على خطوات الوقاية من الفيروسات لجميع المستخدمين.

١٢ــ تفادى فقد البيانات : تأكيد النسخ الاحتياطى والاسترجاع السريع فـــى حالـــة انهيار الشبكة . كذلك استخدام جهاز منع قطع التيار . UPS بالنسبة للنسخ الاحتياطى : حدد ما يجب نسخه ثم جدولة النسخ ثم حدد أنـــواع النســـخ

واستراتيجية مدير الشبكة فى النسخ الاحتياطى هى : تحديد البيانات الواجب نسخها ومتى ــ تحديد معلومات الهاردوير الواجب حفظها ــ تحديد مكان تخزين البيانات خارج وداخل الموقع ــ التدريب على ذلك.

خامساً : إدارة المشاكل:

مدير الشبكة يضع سياسة حل مشاكل الشبكة فى الاتجاهات التالية :

أولاً : وضع خطة لنسخ البيانات المهمة وتأمينها وحماية الشبكة وتوثيق معلومات الشبكة وقياسات الهاردوير وخطة التحسين والتوسعة . يعرف كل ذلك بأسلوب منع المشاكل قبل حدوثها

ثانياً : مراقبة نشاط الشبكة وأداؤها.

ثالثاً : اتباع وسائل حذيثة وجيدة لكشف الأعطال.

رابعاً : فهم أدوات كشف الأعطال.

خامساً : تحديد الجهة التى تلجأ إليها عند الحاجة الماسة.

أولاً : منع المشاكل قبل حدوثها:

١ــ النسخ الاحتياطى : للمعلومات الهامة :

أ ــ يجب تحديد ما يجب نسخه احتياطياً مثل البيانات التى ينتجها المستخدم والمعلومات الحيوية للنظام . أى يجب نسخ ما يصعب إعداده مرة أخرى .

ب ــ تحديد كيفية النسخ . فى الشبكات الصغيرة يقوم كل مستخدم بنسخ المعلومات الهامة على جهازه الخاص أو تمرير جهاز نسخ على كل الأجهزة . أما على الشبكات الضخمة فيوضع جهاز النسخ على الجهاز الرئيسى.

جـ ــ مواعيد النسخ . يتم تحديد الفترات حسب أهمية المعلومات. يتم عمل فحص دورى لضمان سلامة عملية النسخ الاحتياطى والاسترجاع.

٢ــ حماية الشبكة :

١ــ تخطيط وصول المستخدمين إلى موارد الشبكة بوضع سرية للوصول على مستوى المشاركة وعلى مستوى المستخدم.

٢ــ حماية الهاردوير بوضع الجهاز الرئيسى فى غرفة مغلقة أو مع المدير ومراقبة التمديدات داخل وخارج المبنى.

٣ــ توثيق معلومات الشبكة : يقوم المدير بتسجيل أسلوب العمل وخريطة توزيع الشبكة والمهام اليومية ووضع سجل لكل الأجهزة التى على الشبكة ومعلومات عن النسخ الاحتياطى . وتوفير مستودع لكتيبات الشبكة وتسجيل تليفونات جهات الدعم الفنى . الأهم من ذلك تسجيل مشاكل وحل الأعطال كلما حدثت.

٤ــ معايرة الهاردوير : إذا جاءت مكونات الشبكة من منتج واحد يسهل ذلك الاشراف والاصلاح. يجب تقليل عدد التطبيقات المتنوعة للوظيفة الواحدة.

٥ــ التحسين والتوسعة : هى عملية دائمة الحركة على أى شبكة يجب فحص الاصدارات الجديدة على جهاز شخصي قبل وضعه على الشبكة ثم افحصه على مقطع من الشبكة ثم إعلانه للمستخدمين وتدريبهم عليه.

ثانياً : مراقبة نشاط الشبكة وأداؤها:

سوف تلاحظ ارتفاع وانخفاض حركة الشبكة على أوقات مختلفة . ومن ذلك تعرف كيف تتصرف الشبكة حيال الأحمال العالية وأى التصرفات أدى إلى المشاكل.

١ــ حدد الخطوط العريضة لأداء الشبكة فى فترة عادية من العمل.

٢ــ مراقبة سير العمل مع هذه الخطوط العريضة . إذا بعد سير العمل عنها قد يتطلب الأمر تعديل هذه الخطوط . يساعد ذلك فى حل مشاكل الأداء.

٣ــ يوجد برنامج من ميكروسوفت لنظام تشغيل الشبكة بوندوز إن تى يسمى Performance Monitor يستعرض برسوم بيانية أداء الشبكة وينشئ تقارير وتحاليل.

ثالثاً : كشف الأعطال :

بعض مديرى الشبكات يجازف بحل المشكلة مباشرة ثم يبدأون فى استخدام الأدوات المناسبة . يتسبب ذلك فى نتائج عكسية وقد تنشأ مشاكل جانبية لم تكن

موجودة من قبل . يجب وضع نهج محدد للكشف وإصـــلاح الأعطـــال . خمـــس خطوات يجب اتباعها:

١ــ جمع المعلومات . ٢ــ حصر الأسباب.

٣ــ تقييم الوضع . ٤ــ حل المشكلة.

٥ــ توثيق الحدث.

رابعاً : أدوات كشف الأعطال:

من أدوات كشف الأعطال ما يقيس الإشارة أو يتفاعل معها علـــى كوابـــل الشبكة منها : قياس الجهد رقمياً ــ قياس الزمن TDR ــ قياس الذبذبات.

ومنها ما يحصر المشكلة ويحللها مثل : فاحص الكيبل ــ مراقبة الشبكة ــ محلل البروتوكول.

خامساً : المساندة الفنية :

توجد عدة مصادر تساعد على إدارة الشبكة منها المطبـــوع ومنهـــا عـــبر الانترنت مثل :

Technet من ميكروسوفت – Download library مـــن ميكروســـوفت – Usenet من ميكروسوفت.

توسعة الشبكة

ـ حدود الشبكة يعرف من طرفها إلى الطرف الأخير.

ـ عند توسعة الشبكة يؤخذ فى الاعتبار حساب التكلفة مقابل الفائدة العائدة .

ـ ثلاثة طرق لتوسعة الشبكة:

١ـ تمديد الكيبل الموجود ـ حسب 10 Base2 أقصى مسافة ١٨٥ متر بين طرف الكيبل كمثال.

٢ـ إضافة Repeater ينشئ مقطعين على الشبكة كل منها ١٨٥ متر.

٣ـ تغيير وسط الارسال.

ـ من أهداف توسعة الشبكة إضافة أجهزة عليها . يمكن إضافة جهاز بقطع الكيبل الرئيسى وتوصيل كيبل ساقط للجهاز الزائد ـ المسافة بين كيبلين ساقطين تكون ٢,٥ متر كحد أدنى.

ـ يمكن تقسيم الشبكة إلى مقاطع بما يلى : القناطر ـ الموجه ـ البوابة ـ المحولات .

الشبكة الواسعة
Wide Area Network (WAN)

تربط عدة شبكات صغيرة معاً . فور اتصال مستخدم عن بعد تعتبر هـــذه WANيمكن استخدام اتصالات سلكية أو لاسلكية لإنشاءها . من أنواعها:

١ــ شبكة دوائر التحويل (شبكة الهاتف PSTN ــ شبكة ISDN ــ تحويلة. (07

٢ــ شبكة مباشرة مؤجرة بين نقطتين (قياسية. (T1 - T3

٣ــ شبكة حزم التحويل . حيث تجزأ المعلومات إلى حزم صغيرة ترسل عبر عدة طرق وتجمع عند الوجهة المطلوبة حسب المسارات المتوفرة والسهلة.

من تقنياتها : بروتوكول . X. 25 - Frame Relay - SMDS

توجد عدة تقنيات لشبكة WAN أوسع وأوثق منها :

١ــ النقل الغير متزامن . ATM

٢ــ الألياف الضوئية. FDDI

٣ــ المتزامنة الضوئية. SONET

ــ يجب الأخذ فى الاعتبار عند تصميم WAN ما يلى : التدرج فى ربط المواقع ــ المسافة يتبعها التكلفة – السرعة أيضاً.

ــ سوف تجد أن أى WAN بها تقنيات متعددة لأنها تشكيلة من عدة شبكات.

الدخول إلى الشبكة عن بعد

Remote Access

قد يكون الوصول لشبكة ما ــ علاوة على التواجد داخل الشبكة ــ قد يكون من خارجها عن بعد عبر مدينة أو دولة أو منطقة . وظهرت ضرورة ذلك بتزايد الأشخاص الذين يعملون من منازلهم للوصول إلى موارد الشبكة مثل الملفات أو قواعد البيانات أو البريد الالكترونى أو الانترنت.

يتطلب ذلك أمرين:

١ــ برامج الاتصال عن بعد.

٢ــ هاردوير للوصول عن بعد .

مثل وندوز إن تى بها تطبيق SAR . بالنسبة للهاردوير مثل الموديم الذى يتبع الاتصال بنوعين : المتزامن والغير متزامن .

مستلزمات الاتصال عن بعد :

١ــ الموديم : نوعين خارجى وداخلى فى الكمبيوتر . يوصل بالميناء المتتالىRS - 232 بكيبل وبهما فتحة للتوصيل بالتليفون العادى . يوجد معياران للموديم .HAIS , ITU ويتم الاتصال بأسلوبين المتزامن والغير متزامن.

٢ــ الناقل : هو شركة توفر خدمة الاتصال بنوعين : التحويلى والمباشر.

٣ــ البرامج RAS-1 : على وندوز إن تى . يمكنه توصل ٢٥٦ مكالمة فى نفس الوقت على الجهاز الرئيسى أما محطة العمل فمكالمة واحدة.

2 ــ MPR .