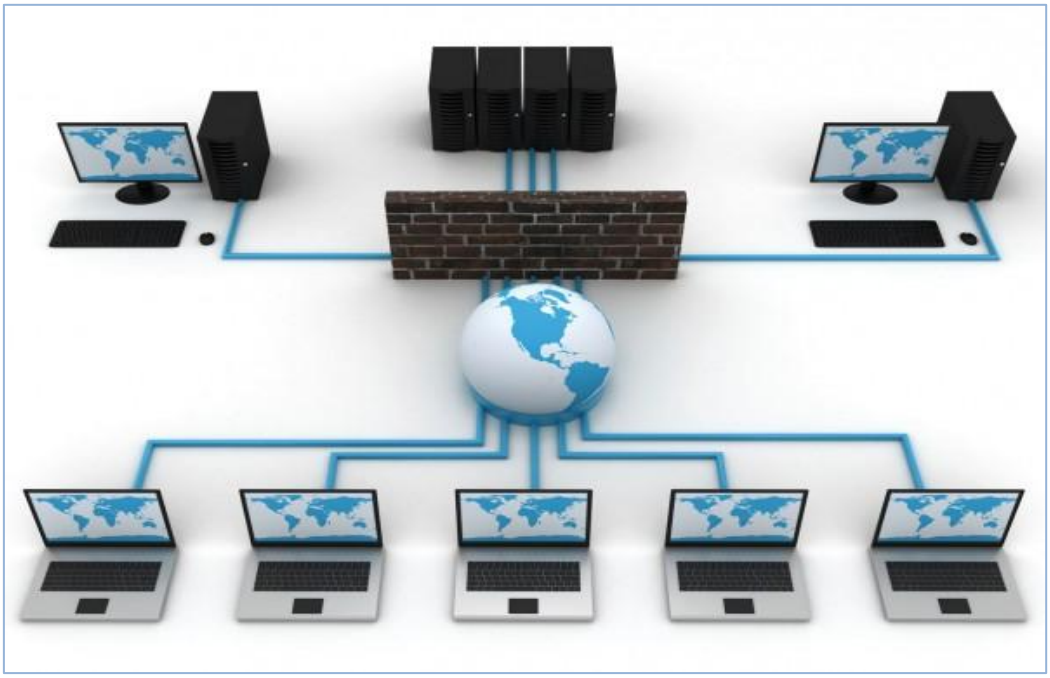
عنـــاصر وهيئـــات الشبكـــة

Computer Networks



ازداد استخدام شبكات الحاسب الآلي خلال السنوات القليلة الماضية، حيث أصبح من النادر وجود حاسوب في شركة أو مؤسسة غير متصل بشبكة حواسيب. ويعود السبب في ذلك إلى ما وجدته هذه الشركات من فوائد تعود عليها من وجود هذه الشبكات من المشاركة في الأجهزة كالطابعات والراسمات والوصول إلى الشبكة العالمية (Internet) وغيرها، وكذلك المشاركة في المعلومات التي تعتبر العنصر الأهم لأي شركة.

- تعريف شبكة الحاسب الآلي

مجموعة من الحواسيب المرتبطة مع بعضها البعض من خلال وسط ناقل بهدف تبادل البيانات ومشاركتها وغير ذلك من الفوائد الناتجة من بناء شبكات الحاسب الآلي.

- تصنيف شبكات الحاسب الآلي:

يمكن تصنيف شبكات الحاسب الآلي اعتمادا على عدة معايير منها:

أولاً: حسب التوزيع الجغرافي:

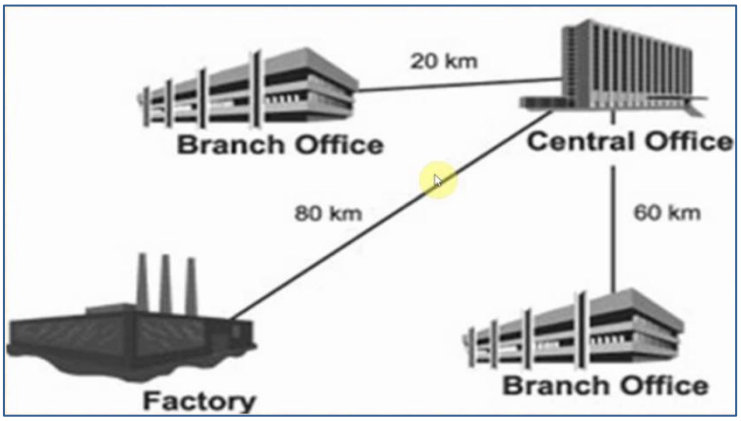
ا- الشبكات المحلية Local Area Networks (LAN)

وهي الشبكات التي تربط مجموعة من الحواسيب المتواجدة في مكان واحد (معمل، بناء)، وهي أبسط أنواع شبكات الحواسيب ويمكن أن تحتوي على مئات الحواسيب المتصلة مع بعضها ضمن بناء أو أكثر متجاورة. الحاسوب المتصل بهذه الشبكة بإمكانه الوصول إلى الموارد الأخرى من المعلومات المتواجدة على أي حاسوب آخر كالبرامج والملفات، كما وتتشارك هذه الحواسيب مع الأجهزة الملحقة مثل الطابعات والراسمات وأجهزة الفاكس وغيرها.

الشبكة المحلية

٢- شبكات المدينة Metropolitan Area Networks (MAN)

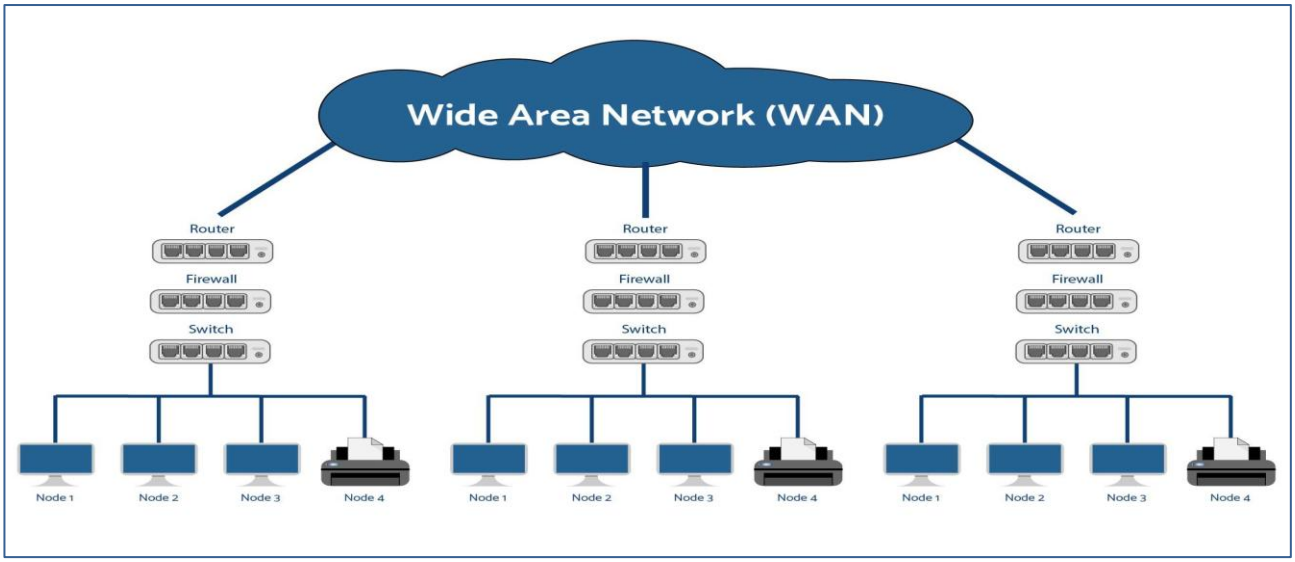
وهي الشبكات التي تربط عدد من الشبكات المحلية (LANs) المتواجدة في مدينة واحدة، وهي تعمل بسرعات عالية وتستخدم عادة كابلات الألياف الضوئية (Fiber Optic)، وعادة ما تغطي مساحة واسعة تتراوح بين (٢٠ – ١٠٠ Km).



شبكة المدينة

٣- الشبكات الواسعة Wide Area Networks (WAN)

في بداية ظهور شبكات الحاسب الآلي، لم تستطع الشبكات المحلية (LANs) من دعم احتياجات الشبكات للشركات الكبيرة التي تتوزع مكاتبها على مساحات واسعة، من الممكن في عدة دول، لهذا كان لابد من تطوير نوع جديد من الشبكات يقوم بربط الشبكات المحلية المتواجدة في أنحاء مختلفة من دولة أو عدة دول مختلفة، وأطلق على هذا النوع من الشبكات اسم الشبكات الواسعة (WAN) وباستخدام هذا النوع تزايد عدد المستخدمين بشبكة الحواسيب في الشركات الكبيرة إلى آلاف الأشخاص.



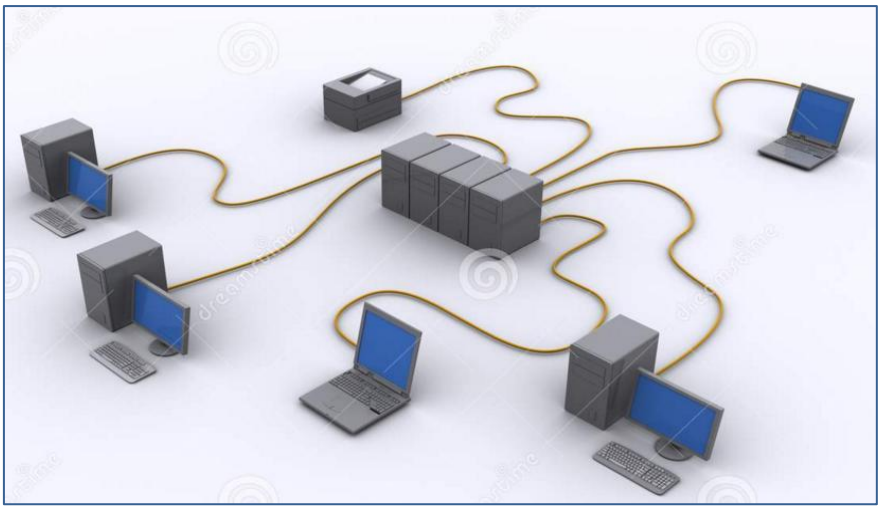
الشبكة الواسعة

ثانياً: حسب الوسط الناقل:

هناك عدة أنواع من وسائط النقل المستخدمة في ربط وتوصيل أجهزة الشبكة مع بعضها بعض منها السلكي ومنها اللاسلكي، وعليه فقد تم تصنيف الشبكات بحسب الوسط الناقل إلى:

١- الشبكات السلكية Wired Networks:

وهي الشبكات التي تستخدم الكابلات فقط في ربط وتوصيل أجهزة الشبكة.



الشبكة السلكية

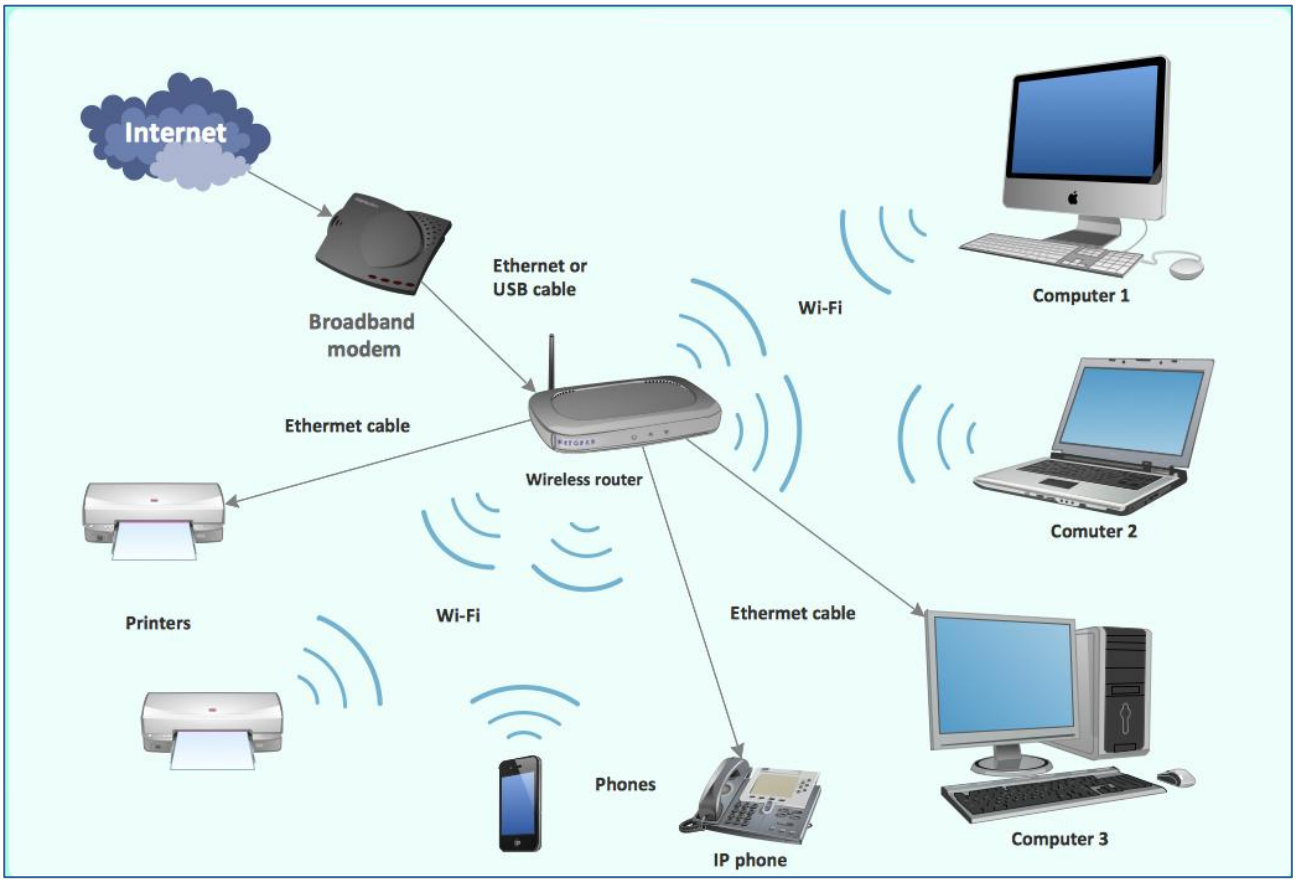
٢- الشبكات اللاسلكية Wireless Networks:

وهي الشبكات التي لا تستخدم الكابلات في ربط وتوصيل أجهزة الشبكة بل تستخدم الفراغ الجوي في نقل الإشارة بين الأجهزة المتصلة.

الشبكة اللاسلكية

٣- الشبكات الهجينة Hybrid Networks:

أي الشبكات السلكية- اللاسلكية وهي الشبكات التي تستخدم كلاً من الكابلات والفراغ الجوي في ربط وتوصيل أجهزة الشبكة مع بعضها بعض.



الشبكة الهجينة

ثالثاً: حسب نظام تشغيل و إدارة الشبكة:

لكي تستطيع شبكات الحاسب الآلي توفير الفوائد والخدمات التي ذكرت سابقاً، لابد من توفر نظام تشغيل وإدارة للشبكات قادر على تحقيق ذلك، لذلك يمكن تصنيف شبكات الحاسب الآلي حسب نظام التشغيل وإدارة الشبكات إلى نوعين رئيسين:

١- شبكات مجموعات العمل الند للند Peer-to-Peer

- وهي الشبكات التي تتكون من مجموعة من الحواسيب المتصلة معاً ولها حقوق متساوية و كل حاسوب بها يمكن أن يكون خادم وعميل في نفس الوقت. أي أن كل حاسوب على الشبكة يمكن أن يزود غيره من الحواسيب بالمعلومات وفي نفس الوقت يمكن أن يأخذ المعلومات من غيره من الحواسيب المتصلة بالشبكة.
- وهي تعتبر أن كل حاسوب في الشبكة له إدارة مستقلة لموارده بحيث يقوم المسئول عنه بتوزيع صلاحيات الدخول إلى حاسوبه من قبل الآخرين وتحديد نوع الخدمات التي يمكن أن يوفرها للغير.
- لا يحتوي هذا النوع من الشبكات على خادم (Server) بل كل حاسوب في الشبكة يمكن أن يكون خادماً وعميلاً بنفس الوقت. أي لا توجد إدارة مركزية أو حاسوب مركزي يتم حفظ التطبيقات المشتركة عليه.
- يطلق على هذا النوع من الشبكات اسم آخر هو مجموعة العمل (Workgroup)، وذلك لأنها تحتوي مجموعة من الحواسيب التي تتعاون فيما بينها لإنجاز عمل معين، ويعتبر هذا النوع من الشبكات مناسب في الحالات التالية:

١. عدد الحواسيب لا يتجاوز ١٠ أجهزة.

٢. لا توجد إدارة مركزية.

٣. أن لا يكون أمن الشبكات ذو أهمية وذلك لأن كل مستخدم في الشبكة يقوم بوضع نظام الحماية المناسب له.

٤. تكلفة محدودة.

٥. لا يحتاج إلى برامج إضافية على نظام التشغيل.

٦. تركيب و صيانة سهلة.

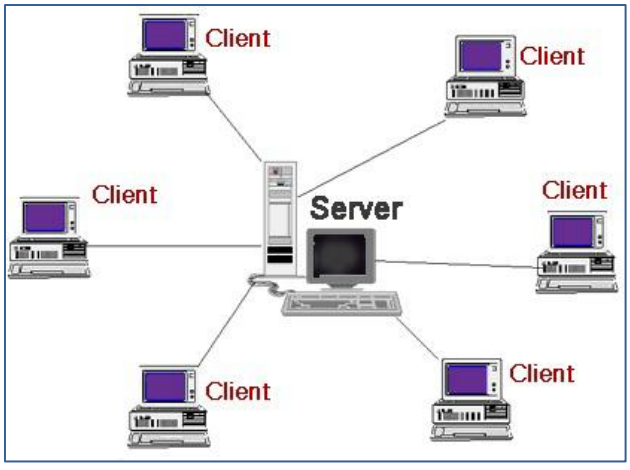
٧. لا تحتاج إلى حواسيب ذات مواصفات عالية وذلك لأن إدارة موارد الشبكة موزعة على حواسيب الشبكة.

أما العيب الرئيسي لهذا النوع من الشبكات هو أنها غير مناسبة للشبكات الكبيرة، وذلك لأنه عند نمو و توسع الشبكة وزيادة عدد مستخدميها يؤدي إلى مشاكل كثيرة.

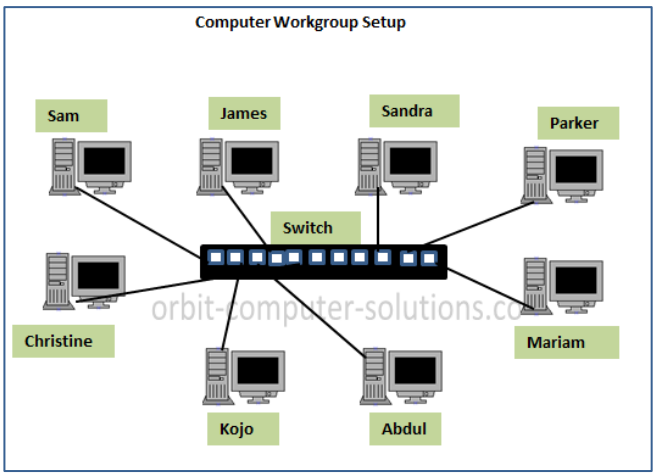
٢- شبكات الخادم/العميل Client / Server

- وهي الشبكات التي تعتمد على وجود حاسوب ذو مواصفات عالية ووحدات تخزين كبيرة الحجم، ويتم وضع البرامج التطبيقية المشتركة على ما يسمى الخادم (Server) وهذا الحاسوب يعمل كخادم، ويمكن أن يحتوي هذا النوع من الشبكات على أكثر من خادم في حالة اتساع الشبكة وفي هذه الحالة تتوزع المهام على هذه الخادمات مما يزيد من كفاءتها. ومن أنواع الخادمات (خادم ملفات File Server، وخادم طباعة Printer Server، وخادم تطبيقات Application Server، وخادم قواعد بيانات Database Server، وخادم البريد الإلكتروني Mail Server)، وتتصف شبكات الخادم/العميل بالمواصفات التالية:

١. يدعم هذا النوع من الشبكات آلاف المستخدمين.
٢. ليس من الضروري أن تكون حواسيب العملاء قوية وذات كفاءة عالية.
٣. توجد إدارة مركزية وجهاز واحد هو الخادم ويقوم بإدارة ومراقبة الشبكة.
٤. في هذا النوع من الشبكات يوفر الخادم حماية عالية من خلال السماح لشخص واحد هو مدير الشبكة (Administrator) بالتحكم في إدارة موارد الشبكة وإعطاء الصلاحيات وأذونات الوصول للمستخدمين.
٥. التركيب والصيانة صعبة مقارنة بشبكات الند للند.
٦. التكلفة مرتفعة مقارنة بشبكات الند للند.
٧. حماية بيانات وبرامج المستخدمين من خلال استخدام برامج الجدر النارية (Fire Walls).



شبكة الخادم والعميل
Client-Server



شبكة مجموعة العمل
Workgroup

- فوائد شبكات الحاسب الآلي

إن الهدف الرئيسي لإنشاء شبكات الحاسب الآلي هو الفوائد الكثيرة التي تقدمها، نذكر منها:

١- تبادل المعلومات

من أهم أسباب بناء شبكات الحاسب الآلي وهو تبادل المعلومات و الملفات بسهولة و بسرعة عالية.

٢- المشاركة في استخدام موارد الشبكة

إن وجود الشبكة يؤمن التشارك في استخدام التجهيزات المادية المرتبطة بالشبكة (الطابعات، الراسمات، الماسحات الضوئية، والوصول إلى الشبكة العالمية Internet... الخ).

٣- التشارك في البرمجيات

تؤمن شبكة الحاسب الآلي للمستخدمين إمكانية التشارك في البرمجيات كقواعد البيانات التي يمكن أن توضع على الخادمات (Servers) وتوفر الشبكة إمكانية استخدامها من قبل كل أقسام الشركة.

٤- الإدارة المركزية

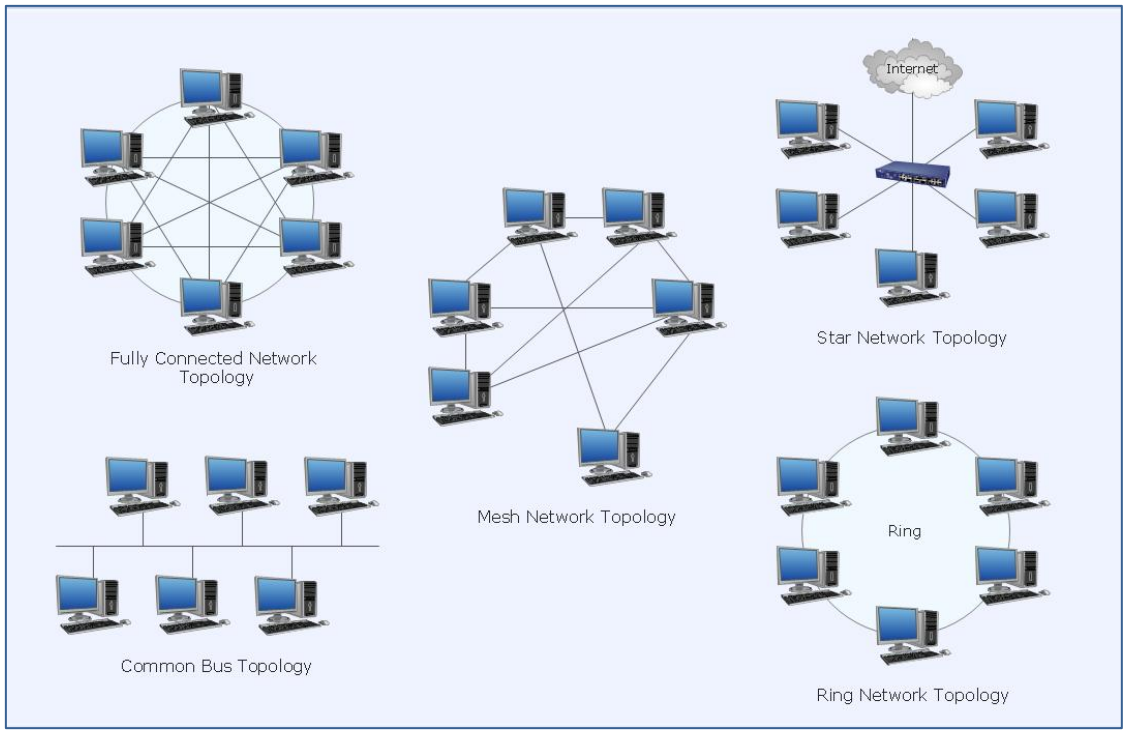
عندما يكون نظام تشغيل وإدارة الشبكات هو من نوع الخادم/العميل (Client/Server) عند ذلك يتم إدارة الشبكة إدارة مركزية أي أن هناك مدير للشبكة (Administrator) هو الذي يستطيع إدارة ومراقبة الشبكات والتحكم بها من مكان مركزي، وبالتالي إمكانية إدارتها بشكل جيد ورفع مستوى أداء العمل وأمان الشبكة.

٥- تأمين الاتصال السهل

تؤمن شبكات الحاسب الآلي سهولة إجراء الاتصالات وذلك من خلال توفير خدمة البريد الإلكتروني، وكذلك يمكن أن توفر بعض شبكات الحاسب الآلي خدمة مؤتمرات الفيديو (Video Conference)، والتي تتيح تشارك مجموعة من المستخدمين معاً في جلسة نقاش واحدة.

تقنيات ربط الشبكات ومعايير الكابلات

Network Topologies

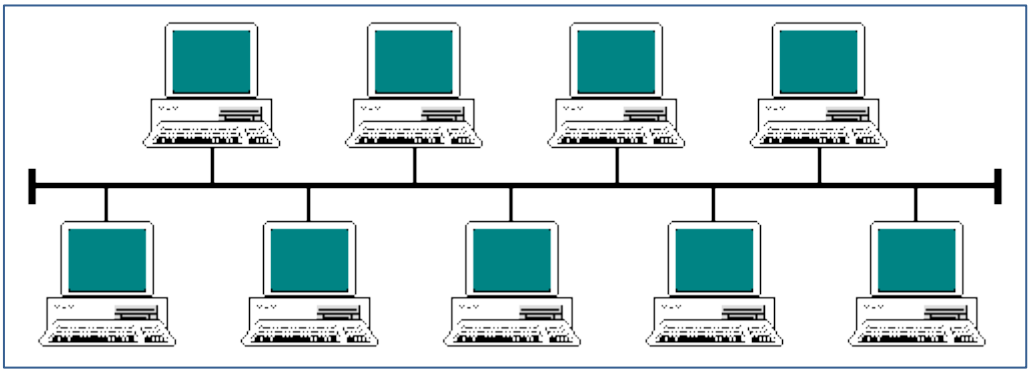


طبولوجيا الشبكات Networks Topology

يطلق اسم طبولوجيا الشبكات Networks Topology على الطريقة التي يتم فيها تحديد كيفية ربط الحواسيب و المكونات الأخرى بالشبكة ببعضها البعض بحيث تعطي التوصيف السليم للبنية العامة لشبكة الحواسيب.

إن اختلاف طريقة التوصيل يؤدي إلى اختلاف في المعدات التي تحتاجها الشبكة (نوع الكابلات ، نوع بطاقة الشبكة، نوع الوصلات) كما يؤثر أيضاً على توسيع الشبكة مستقبلاً، وبشكل عام يمكن تصنيف طبولوجيا الشبكات المحلية إلى الطرق التالية:

ا- طريقة التوصيل الخطي Bus Topology



الشبكة الخطية

- يطلق على هذا النوع من طرق التوصيل عدة مسميات منها (الشبكة الخطية، الشبكة الخاملة، شبكة المنازعة، شبكة CSMA).
- تعتبر هذه الطريقة من أبسط أنواع التوصيل، حيث يتم ربط الحواسيب باستخدام كابل واحد يصل ما بين هذه الحواسيب.
- يتم إرسال الإشارات إلى كل الحواسيب في الشبكة، حيث أن حاسوب واحد فقط يمكنه الإرسال وباقي الحواسيب تنتظر حتى يفرغ هذا الحاسوب من الإرسال، ولكنها تؤخذ فقط من حاسوب واحد الذي يتوافق عنونته مع العنوان الخاص بالإشارات.
- إن كل حاسوب على الشبكة يبث إشارات البيانات في الاتجاهين على طول الكابل، فإذا لم تجد هذه الإشارات نهاية ممانعة عندما تصل إلى نهاية الكابل فإنها تعكس اتجاهها في الكابل مما يمنع الحواسيب الأخرى من إرسال إشارتها، لذلك يتم وضع نهاية ممانعة (Terminator) عند نهاية الكابل، وذلك لإيقاف الإشارات ومنعها من الارتداد، أي أنه يقوم بامتصاص الإشارات الحرة وهذا ينظف الكابل مما يسمح لحاسوب آخر بالإرسال.
- تعمل هذه الشبكة على تقنية CSMA/CA أو CSMA/CD.

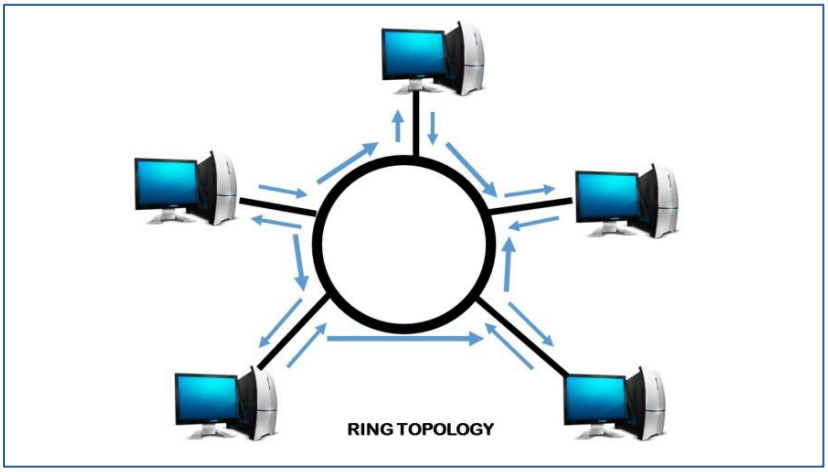
مميزات طريقة التوصيل الخطي

- إمكانية توسيع الشبكة بسهولة باستخدام الوصلات أو مقويات الإشارة.
- ذات تكلفة منخفضة لأنها تحتاج إلى أقل عدد من الكابلات مقارنة بطرق التوصيل الأخرى.
- تعتبر أبسط وأسهل طرق التوصيل لأنها عبارة عن كابل واحد يصل ما بين جميع الحواسيب.

عيوب طريقة التوصيل الخطي

- كلما ازداد عدد الحواسيب، كلما ضعفت الإشارة أكثر.
- جهاز واحد فقط يقوم بالإرسال.
- يجب أن تكون الأجهزة متقاربة من بعضها بعض.
- من الصعب معرفة العطل.
- تتعطل الشبكة بشكل كامل إذا ما تعطلت وصلة الحاسوب أو حدث عيب في الكابل في أي منطقة.

٢- طريقة التوصيل الحلقي Ring Topology



طريقة التوصيل الحلقي

- تأخذ الشبكة في هذا التصميم شكل الحلقة حيث يتم وصل الحواسيب في الشبكة على شكل حلقة مغلقة.
- في هذه الطريقة كل حاسوب يقوم بإرسال البيانات إلى الحاسوب الذي يليه، حيث يأخذ الحاسوب البيانات ثم يعيد إرسالها مرة أخرى إلى الحاسوب الذي يليه، وهكذا بحيث تنتقل الإشارات ضمن الحلقة باتجاه واحد وبترتيب واحد، فكل الحواسيب متساوية.
- بما أن كل حاسوب يستقبل البيانات ثم يعيد إرسالها على الشبكة إلى الحاسوب التالي، لذلك فكل حاسوب على الشبكة يقوم بعمل مقوي الإشارة، حيث يقوم بتقوية الإشارة المارة من خلاله وهذا يؤدي إلى عدم ضعفها.
- كلما ازداد عدد الحواسيب يزداد وقت الاستجابة.
- تنتقل البيانات باستخدام طريقة ما يسمى مرور الشارة (Token Passing)، والتي تعتبر وسيلة سريعة لنقل البيانات.
- عندما يريد حاسوب ما على الشبكة إرسال بيانات ما، فإن عليه الانتظار حتى يتسلم الشارة فارغة (Free Token)، تخبره على أنه قادر على إرسال بياناته على الشبكة.
- تستخدم وعدة توصيل مركزية نوع MAU في توصيل الأجهزة.

مميزات طريقة التوصيل الحلقي

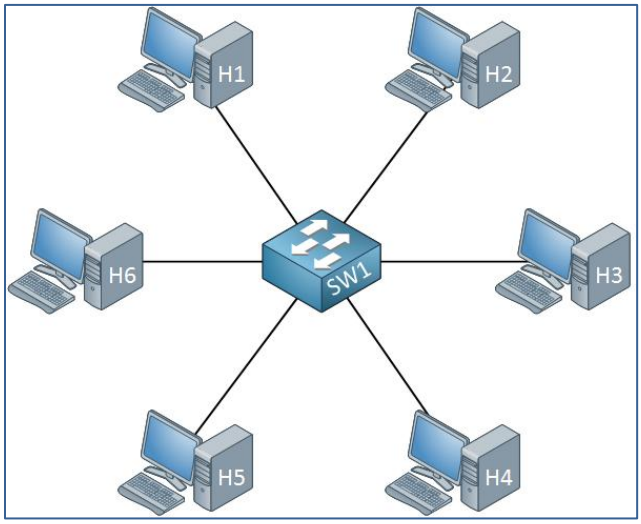
- تستخدم في الشبكات عاليـــة الأداء والتي تحتاج إلى نقل كميات كبيرة من المعلومات.
- هذه الطريقـة تستخدم طريقة مرور الشارة (Token Passing) التي تعتبر من الوسائل السريعة، حيـث أن الإشارات تنتقل من حاسوب إلى آخر بسرعة مقاربة لسرعة الضوء.
- لا يوجد تصادم في طريقة التوصيل هذه.

عيوب طريقة التوصيل الحلقي

- غالية التكاليف.
- جهاز واحد فقط يقوم بالإرسال.
- تتعطل الشبكـــــة بشكـــل كامـــل إذا تعطلـــت وحـــدة التوصيـــل المركزيـــة.

٣- طريقة التوصيل النجمي Star Topology

تعتبر طريقة التوصيل النجمي من أشهر الطرق المعروفة لربط مكونات الشبكة ببعضها، حيث يتم فيها ربط كل حاسوب في الشبكة بكابل خاص إلى منافذ وحدة التوصيل المركزية، وفي النهاية يصبح الشكل النهائي للتوصيل يشبه النجمة Star لذا سميت هذه الطريقة بالتوصيل النجمي.



الشبكة النجمية

تنتقل الإشارات من الحاسوب المرسل الذي يرغب في إرسال البيانات إلى جهاز الربط المركزي ومنه إلى الحواسيب المرتبطة بها.

مميزات طريقة التوصيل النجمي

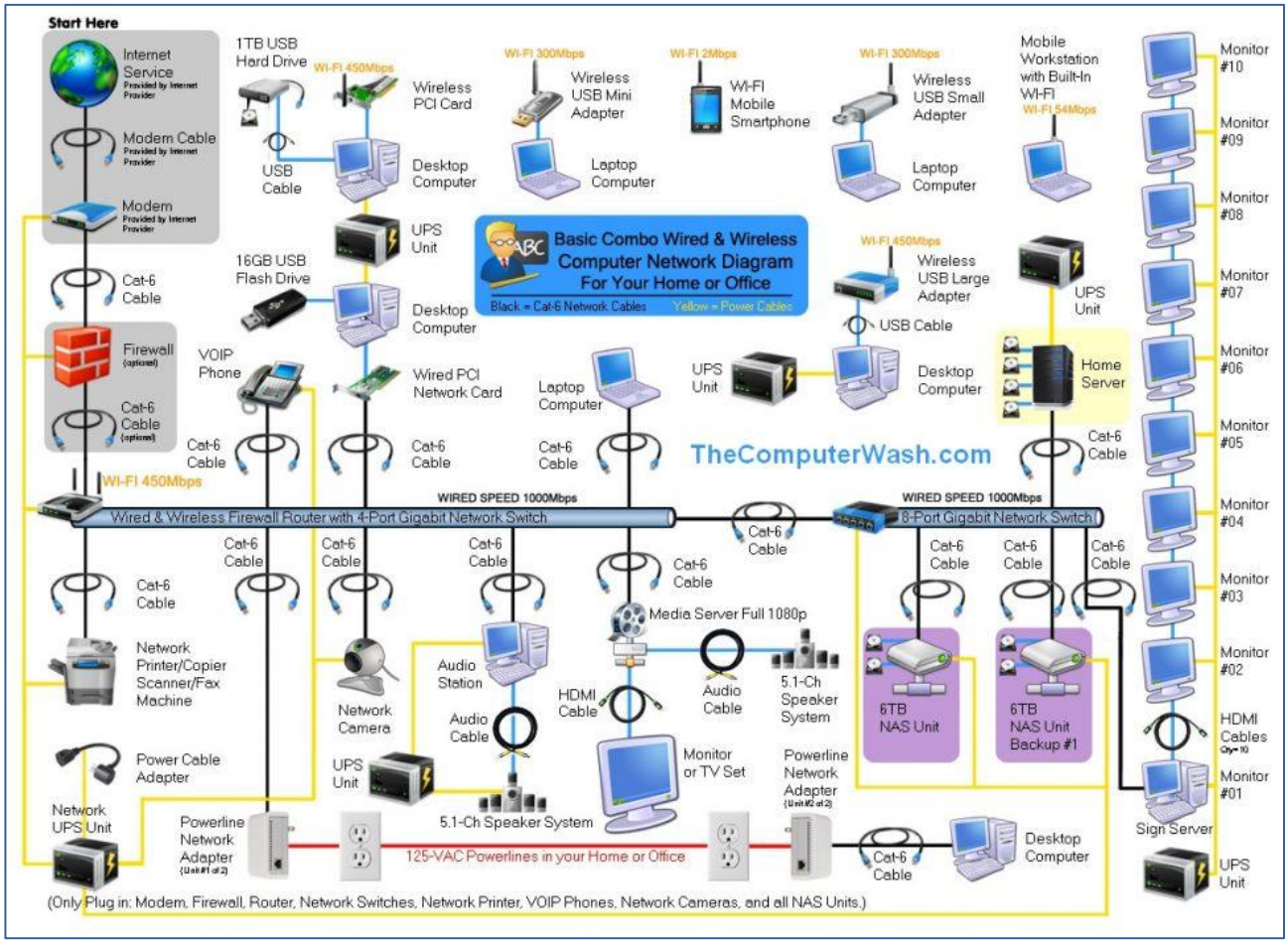
- من السهل توسيع الشبكة (إضافة حواسيب جديدة) فكل ما نحتاجه هو كابل لوصل الحاسوب بأحد منافذ وحدة الربط المركزي.
- إذا تعطل أحد الحواسيب أو انقطع الكابل الخاص به ،استمرت الشبكة بالعمل ولا يتعطل غير هذا الحاسوب.
- يمكن تحريك الحواسيب من مكانها وصيانتها وتغيير التوصيلات دون أن تتأثر الشبكة.

عيوب طريقة التوصيل النجمي

- تعتبر هذه الطريقة ذات تكلفة مرتفعة لأنها تحتاج كابلات أكثر ووحدات توصيل مركزية.
- تتعطل الشبكة بشكل كامل إذا تعطلت وحدة التوصيل المركزية.

الموصلات والكابلات

Connectors and Cables



وسائط النقل المستخدمة في ربط وتوصيل أجهزة الشبكة:

إن وسائط نقل البيانات هي الوسائد التي يتم من خلالها انتقال البيانات إما سلكياً أو لاسلكياً، يشار إلى هذا المصطلح بالكابلات المستخدمة في توصيل الشبكات على الشبكة، وعلى الرغم من انتشار الشبكات اللاسلكية واستخدامها لتقنيات مختلفة في الاتصال بلا أسلاك إلا أن الشبكات السلكية تستخدم عدة أنواع من الكابلات منها:

ا. الكابلات المحورية Coaxial Cables:

هذا النوع من الكابلات يشبه إلى حد كبير الكابلات المستخدمة في وصلات التليفزيون أو الـ Satellites ويطلق عليه اختصاراً (Coax) وهي تعتمد على جزء نحاسي في المنتصف داخل جزء بلاستيكي ومن فوقه معدني آخر مكسو بالبلاستيك أو PVC.

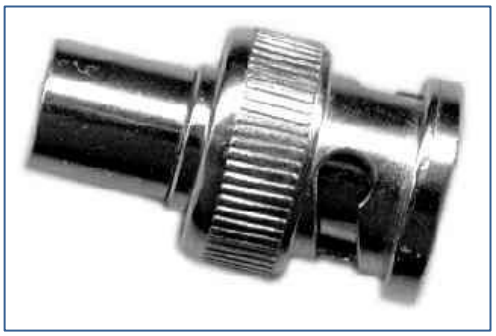
وهذه الكابلات لها نهايات طرفية خاصة لتوصيلها ببطاقة الشبكة وأيضا بطاقة الشبكة لابد أن تكون مجهزة لتوصيل هذا النوع من الكابلات.

الكابلات المحورية

الموصلات (Connectors) المستخدمة في توصيل الكابلات تسمى وهي BNC Connectors .

إلا أن هذه الأنواع من الكابلات يحدث بها ما يسمى Signal Bounce أو ارتداد الإشارة من نهاية الكابل إلى داخله مرة أخرى، ولهذا فهي تحتاج إلى ما يمسى (Terminators) في النهاية لامتصاص هذه الإشارات حتى لا تنعكس مرة أخرى في الكابل وتؤدي إلى مشاكل كبيرة في الشبكة وفقد للمعلومات والتوصيل.

وصلة BNC



وصلة Terminator

٢. الكابلات المجدولة Twisted Pairs:

هذا النوع من الكابلات هو الأكثر شيوعا هذه الأيام وهو عبارة عن مجموعة من الأزواج من الأسلاك Pairs يتكون منها الكابل الأساسي، تُستخدم قطعة بلاستيكية في طرف الكابل من أجل توصيلة بمنفذ بطاقة الشبكة للجهاز أو أحد منافذ وحدة التوصيل المركزية ويطلق عليها (RJ45)، هذه الكابلات منها ما يتكون من زوجين أو أكثر حسب النوع وهذه الكابلات تنقسم إلى قسمين UTP أو Unshielded Twisted Pair وهي الكابلات الغير معزولـــة وهي مستخدمـــة اكثر في شبكات Star وهناك النوع الثاني وهو STP أو Shielded Twisted Pair ويستخدم اكثر في شبكات Token Ring وهذه الكابلات لها فئات وأنواع مختلفة تعرف باسم CAT اختصاراً لـ Category.

فئات الكابلات المجدولة:

الفئة CAT	الخصائص
CAT1	تتكون من زوجين (أربعة أسلاك) لنقل الصوت فقط (أسلاك الهاتف).
CAT2	تتكون من أربعة أزواج (٨ أسلاك) لنقل الصوت والصورة بسرعة نقل 4Mbps.
CAT3	تتكون من أربعة أزواج (٨ أسلاك) لنقل الصوت والصورة بسرعة نقل 10Mbps.
CAT4	تتكون من أربعة أزواج (٨ أسلاك) لنقل الصوت والصورة بسرعة نقل 16Mbps.
CAT5	تتكون من أربعة أزواج (٨ أسلاك) لنقل الصوت والصورة بسرعة نقل 100Mbps.
CAT5e	تتكون من أربعة أزواج (٨ أسلاك) لنقل الصوت والصورة بسرعة نقل 1000Mbps.
CAT6	تتكون من أربعة أزواج (٨ أسلاك) لنقل الصوت والصورة بسرعة نقل 1000Mbps (1Tbps) لأول ٥٥ متر ثم تقل السرعة إلى (1000 Mbps).
CAT6a	تتكون من أربعة أزواج (٨ أسلاك) لنقل الصوت والصورة بسرعة نقل 10000Mbps (1Tbps).

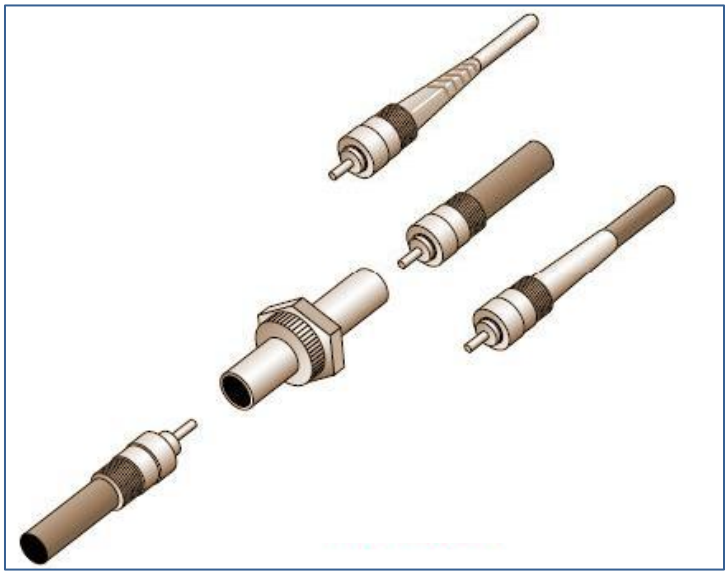
كابل UTP

وصلة RJ45

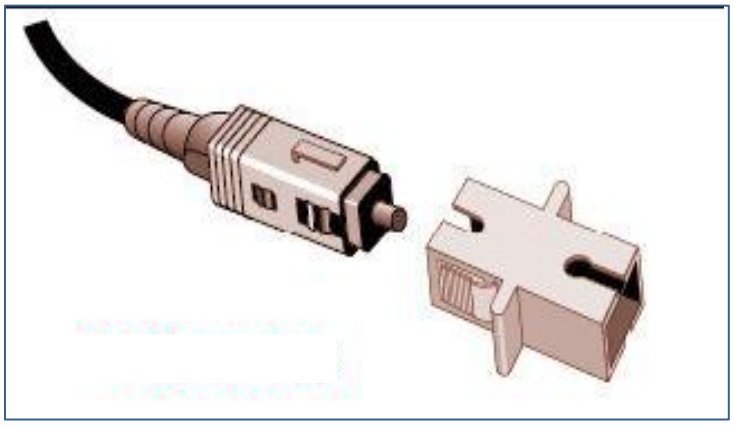
٣. الكابلات الألياف الضوئية Fiber Optic:

جميع الكابلات السابقة تتكون من مادة نحاسية وعليه فإنها تتأثر بما يطلق على التداخل الكهرومغناطيسي EMI أما هذا النوع من الكابلات فهي تستخدم الضوء في نقل البيانات وعليه فإنها لا تتأثر أبداً بالـ EMI ولكنها قد تتأثر بالضوء الشديد جداً لذلك فهي تعتبر من أغلى أنواع الكابلات المستخدمة في ربط الشبكات.

تستخدم هذه الكابلات مقابس توصيل مثل ST Connecter أو SC Connector. يستخدم هذه النوع من الكابلات لنقل البيانات لمسافات بعيدة تصل لعدة كيلو مترات.



ST Connector



SC Connector

العوامل التي تؤثر على اختيار الكابل:

لكي يتم اختيار أفضل نوع للكابل بحيث يناسب طبيعة الشبكة التي نقوم بتصميمها فإنه يجب أولاً دراسة مجموعة من العوامل التي يجب أن تؤخذ بعين الاعتبار، ومن هذه العوامل:

١. التكلفة Coats:

حيث تلعب التكلفة دوراً كبيراً في اختيار نوع الكابل المستخدم، فغالباً ما يكون هنالك ارتباط وثيق بين سرعة نقل المعلومات وتكلفة الكابل، فإذا كانت التكلفة الموضوعة لهذه الشبكة كبيرة فإنه يمكن اختيار كابل ذو تكلفة عالية وعليه ستكون سرعة النقل فيه عالية أيضاً، أما لوم كانت التكلفة المخصصة قليلة فإنه يجب مراعاة العلاقة بين تكلفة الكابل وسرعة النقل.

٢. متطلبات التركيب Installing Requirements:

تختلف طريقة التركيب لكل نوع من أنواع الكابلات، منها السهل حيث يمكن للشخص العادي تركيبها ومنها ما يحتاج إلى خبرات كبيرة وشركات مختصة في التعامل معها وتركيبها.

٣. سرعة النقل Transmission Speed:

لكل نوع من أنواع الكابلات سرعة نقل مختلفة، وتقاس سرعة نقل المعلومات بـ Mbps.

٤. التضاؤل Attenuation:

تنتقل المعلومات عبر الكابلات النحاسية على شكل إشارات كهرومغناطيسية، وهذه الإشارات تضعف قوتها على طول الكابل وتعرض البيانات لعدة مقاومات أثناء انتقالها عبر الكابل، أي أن هناك علاقة عكسية بين التضاؤل وطول الكابل وبالتالي يتم تحديد طول الكابل المراد استخدامه بناءً على أثر عامل التضاؤل ولذلك يجب مراعاة الحد الأقصى لطول الكابل لتجنب اضمحلال الإشارة وتضاؤلها.

٥. أثر التداخل الكهرومغناطيسي EMI:

إن أغلفة الحماية التي وضعت على الكابلات قد قللت إلى حد ملموس من تأثر البيانات المارة عبر الكابل بالتداخل الكهرومغناطيسي ولكنها لم تمنعه نهائياً لذلك فإن بعض أنواع الكابلات يتأثر بالـ EMI أكثر أو أقل من نوع آخر من الكابلات.

والجدول التالي يبين مقارنة بين أنواع الكابلات المختلفة وخصائص كل نوع منها

الخصائص / نوع الكابل	التكلفة	المرونة وسهولة التركيب	التضاؤل (Meter)	التأثر بالـ EMI	سرعة النقل (bps)
UTP 10 Base T	رخيص التكاليف	سهل التركيب	100 M	أكثر أنواع الكابلات تأثراً	على حسب الفئة المستخدمة
STP 10 Base T	رخيص التكاليف	سهل التركيب	100 M	يتأثر بنسبة أقل من UTP	على حسب الفئة المستخدمة
محوري رفيع 10 Base 2	رخيص التكاليف	سهل التركيب	185M	يتأثر بنسبة أقل من UTP و STP	10-100 Mbps
محوري سميك 10 Base 5	أغلى من المحوري الرفيع	سهل التركيب	500 M	يتأثر بنسبة أقل من UTP و STP والمحوري الرفيع	10-100 Mbps
الألياف الضوئية 10 Base L	أغلى أنواع الكابلات	يحتاج إلى شركات مختصة	يصل لحد ٤ كيلو متر بدون مقوي إشارة	لا تتأثر أبداً بالتداخل الكهرومغناطيسي	سرعة الضوء

أجهزة الشبكات وتقنيات الشبكات اللاسلكية

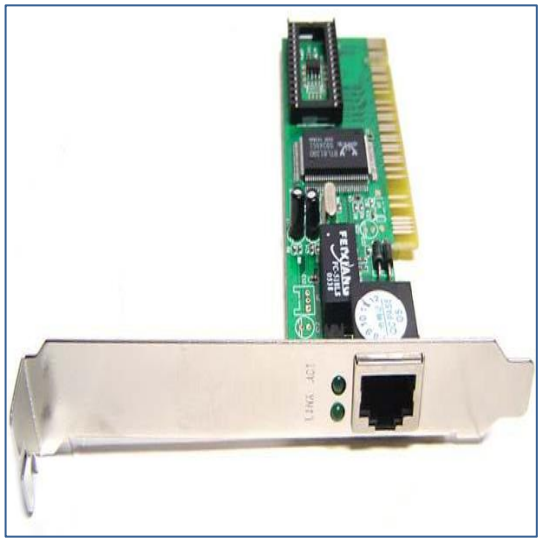
Networking Devices and Wireless Networking Technologies

تختلف أجهزة الشبكة والتقنية المستخدمة فيها اعتمادا على عدة عوامل كالمساحة الجغرافية التي ستشغلها الشبكة أو اعتمادا على نوع الوسط الناقل المستخدم في بنائها وعليه فقد تعددت الأجهزة المستخدمة في بناء وتوصيل الشبكات نذكر منها:

أولاً- بطاقة الشبكة NIC:

بطاقة الشبكة أو بطاقة واجهة الشبكة (NIC) هي عبارة عن بطاقة إلكترونية تحتوي على دارات إلكترونية لإرسال واستقبال الرسائل، حيث توضع هذه البطاقة في إحدى فتحات التوسع Expansion Slots الموجودة في الحاسوب سواء أكان هذا الحاسوب يعمل مخدماً للشبكة أو يعمل كمحطة عمل بحيث يقوم بعملية التوصيل بين الحاسوب وكابل الشبكة.

يحتاج كل حاسوب في الشبكة إلى بطاقة شبكة تعمل على تحويل الإشارات الواصلة فتستقبل البيانات من الحاسوب بشكل متوازي Parallel من خلال فتحة التوسع التي تركب فيه على اللوحة الرئيسية Mother Board للحاسوب لتنتقل هذه البيانات إلى كابل الشبكة وبشكل تسلسلي Serial من خلال الوصلة التي تصلها مع كابل الشبكة وبالطبع تجري أيضاً العملية المعاكسة.



بطاقة شبكة سلكية

بطاقة شبكة لاسلكية

وظائـــف بطاقـــة الشبكـــة :

تقوم بطاقة الشبكة بالوظائف الأساسية التالية :

أ. استقبال البيانات الصادرة عن الحاسوب وتحويلها إلى إشارات كهربائية من أجل إرسالها في كابل الشبكة:

عندما تستقبل بطاقة الشبكة البيانات الصادرة من الحاسوب، تقوم بتحويل هذه البيانات من الشكل الذي يفهمه الحاسوب إلى إشارة كهربائية ليتم نقلها في كابل الشبكة.

تنتقل البيانات داخل الحاسوب على شكل مجموعات في ممرات تسمى BUS وهي تتكون من عدة أسلاك موضوعة بجانب بعضها حيث تنتقل البيانات في الحاسوب بشكل متوازي Parallel وبالتالي تستقبل بطاقة الشبكة البيانات على التوازي وتنظمها من أجل الإرسال بشكل متسلسل Serial عبر الكابل ويتم هذا بتحويل البيانات الرقمية في الحاسوب إلى إشارة كهربائية تنتقل في كابل الشبكة و العنصر المسؤول عن هذا التحويل داخل بطاقة الشبكة هو (المرسل-المستقبل) Transceiver .

ب. استقبال البيانات من الكابل وتحويلها إلى الشكل الذي يفهمه الحاسوب .

وهنا تقوم البطاقة بعكس العملية التي تمت في النقطة السابقة (أ).

ج. التعرف على الأجهزة المتصلة بالشبكة.

لكل بطاقة شبكة عنوانها الخاص والفريد على مستوى العالم سواء كانت بطاقة سلكية أو لاسلكية يطلق على هذا العنوان بعنوان التحكم بالنفاذ إلى الوسط (MAC Address) أو العنوان الفيزيائي ، وهذا العنوان الخاص بها من أجل تمييزها عن البطاقات الأخرى المتصلة بالحواسيب في الشبكة. وطول هذا العنوان 48 bit . حيث أن أول (24 bit) مخصصة لرمز الشركة المصنعة للبطاقة وثاني (24 bit) هي الرقم التسلسلي للبطاقة.

د. تنظيم حركة مرور البيانات من وإلى الكابل.

بما أن سرعة نقل البيانات من الحاسوب إلى بطاقة الشبكة أسرع من نقلها إلى الكابل لذا يخصص الحاسوب جزء من ذاكرته ليحتفظ فيها بالبيانات وتأخذها بطاقة الشبكة على فترات ويسمى ذلك بالنفاذ المباشر إلى الذاكرة DMA(Direct Memory Access) ، لذلك توضع البيانات بشكل مؤقت في ذاكرة عزل Buffer بشكل مؤقت حتى تطلبها بطاقة الشبكة.

كيف تعمل بطاقة الشبكة للنفاذ إلى الذاكرة :

عندما تحتاج بطاقة الشبكة إلى البيانات المخزنة في الذاكرة تقوم بالعمليات التالية :

١. تبعث بإشارة مقاطعة (Interrupt Request) IRQ إلى الحاسوب.
٢. عندما يستقبل الحاسوب إشارة المقاطعة ينهي العملية التي يقوم بها ويستجيب لطلب المقاطعة ويقوم بإرسال البيانات على الممر BUS الخاص ببطاقة الشبكة من الجزء المحجوز في الذاكرة لبطاقة الشبكة.
٣. قبل أن يتم إرسال البيانات في الشبكة تقوم بطاقة الشبكة بإرسال رسالة إلكترونية إلى بطاقة الشبكة في الحاسوب المستقبل يتم الاتفاق على ما يلي :

أ. الحجم الأعظمي للبيانات المرسلة.

ب. سرعة نقل البيانات بحيث تستطيع بطاقة الشبكة في الجهاز المستقبل من استقبالها.

ج. المدة الزمنية بين إرسال كل دفعة.

د. المدة الزمنية لاستقبال رسالة التأكيد باستقبال البيانات بشكل سليم وخالي من الأخطاء.

هـ. حجم البيانات التي تستطيع بطاقة الشبكة استقبالها قبل أن تمتلئ.

كيفية اختيار بطاقات الشبكة :

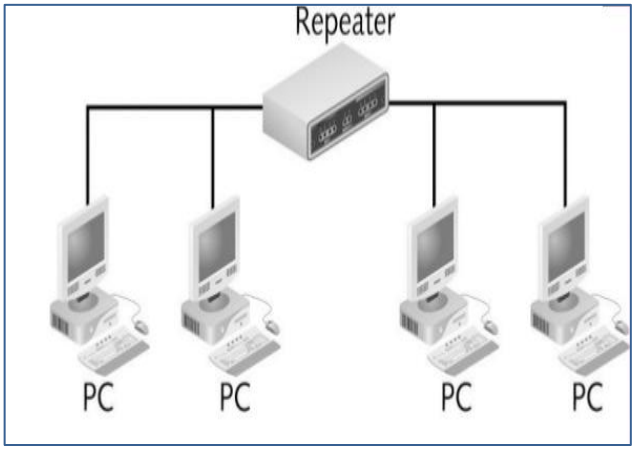
عند اختيار بطاقة الشبكة، هناك عدة أمور يحب أخذها بعين الاعتبار :

١. نوع ممر البيانات Bus الذي سوف تثبت به بطاقة الشبكة (ISA, EISA, MAC, PCI).
٢. نوع الشبكة (سلكية أو لاسلكية).
٣. نوع الوصلات اللازمة من أجل التوصيل إلى الكابل.

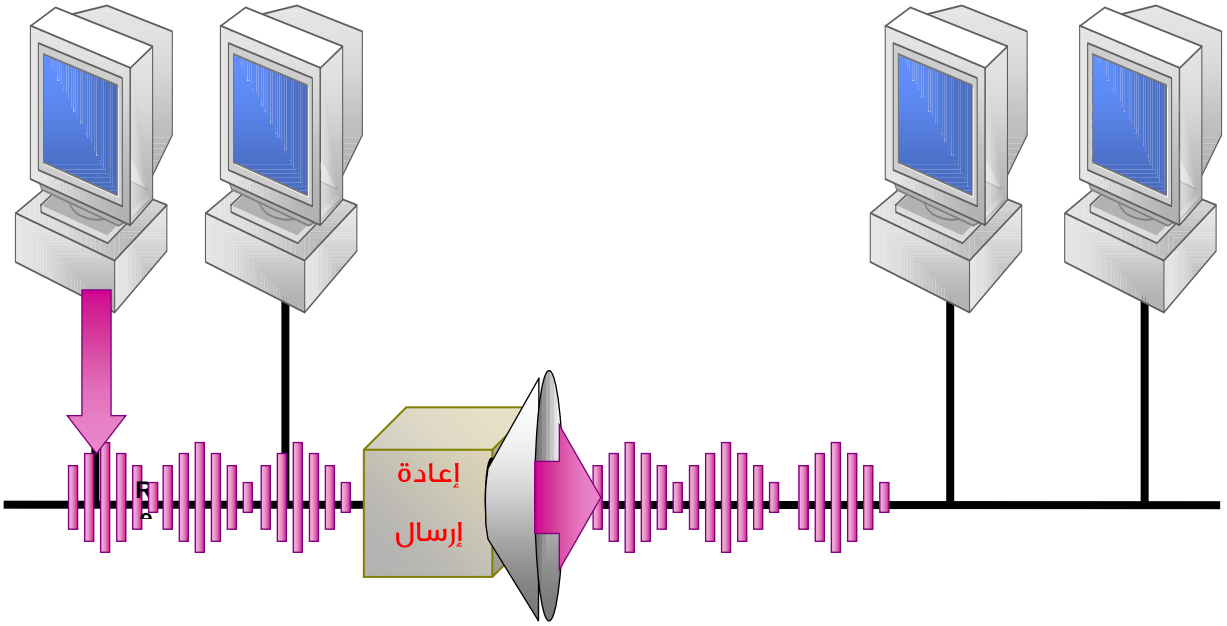
ثانيـاً- مقوي الإشارة Repeater:

هو جهاز مكون من دارات كهربائية، يقوم بتحويل الجهود ومواصفات الإشارة بما يتناسب ووسـائط النقـل، حيـث تستخدم مقويات الإشارة لتضخيم الإشارة بهدف إرسالها لمسافات بعيدة وضمن نوع واحد مـن الشـبكات. وذلـك لأن الإشارة تتعرض أثناء انتقالها إلى التضاؤل Attenuation عند انتقالها لمسافات بعيدة مما يؤدي إلى تشويهها وصعوبة معرفتها أو عدم وصولها للطرف المستقبل.

تعمل مقويات الإشارة في الطبقة الفيزيائية لنظام السبع طبقات (OSI)، لـذلك فهـي تسـتطيع ربـط شـبكتين مختلفتين بالطبقة الفيزيائية فقط.



مقوي الإشارة Repeater



ثالثـاً- وحدة التوصيل المركزية HUB:

هي أجهزة إلكترونية تعمل في الطبقة الفيزيائية في نظام السبع طبقات (OSI) حيث تتلقى الإشارة مـن منفـذ معين ثم تُرسلها إلى جميع المنافذ وتحتاج هذه الأجهزة إلى مزود طاقة ويوجد بجانب كـل منفـذ ديـودات ضـوئية تشير عن حالة الطاقة والكابلات المتصلة بالمنافذ.

تستخدم وحدات التوصيل المركزية (HUBs) في الشبكات التي تستخدم طريقة التوصيل النجمي.

أنواع وحدة التوصيل المركزية HUB:

١. وحدة التوصيل المركزية الخاملة: (Passive hubs)

تقوم بوظيفة توصيل الأجهزة بعضها ببعض، ولا تقوم بتقوية الإشارة الضعيفة، لذلك فهي لا تحتاج إلـى مصـدر للطاقة لكي تعمل.

٢. وحدة التوصيل المركزية الفعّالة: (Active hubs)

تقوم بوظيفة توصيل الأجهـزة بعضـها بـبعض بالإضـافة إلـى تقويـة الإشـارات الضـعيفة، ويمكنهـا اكتشـاف التصادمات (Collisions) وتجنبها، لذلك فهي تحتاج إلى مصدر للطاقة لكي تعمل.

٣. وحدة التوصيل المركزية الذكية: (Smart hubs)

تقوم بعمل مشابه لوحدات التوصيل المركزية الفعّالة ولكن تزيد عليها إمكانية إدارتها والتعامل مع البروتوكول (SNMP) الذي يعمل على إدارة الشبكات.

وحدة التوصيل المركزية الخاملة

وحدة التوصيل المركزية الفعّالة

وحدة التوصيل المركزية الذكية

رابعـاً- الجسر Bridge:

هو جهاز مادي يقوم بربط الشبكات المحلية معاً وهذا ما كان يفعله مقوي الإشارة لكن الجسر يعمل في طبقة ربط البيانات، فهو يستطيع ربط شبكتين مختلفتين في خصائص ومواصفات طبقة ربط البيانات في نظام السبع طبقات (OSI) لكنها متماثلة في بنى الطبقات الأعلى.

وبما أن طبقة ربط البيانات قد قُسمت إلى طبقتين فرعيتين وهما :

طبقة التحكم بالنفاذ إلى الوسط (MAC).

وطبقة التحكم بالاتصال المنطقي (LLC). فإن الجسور تعمل في طبقة التحكم بالنفاذ إلى الوسط (MAC). لذلك فهي تهتم بالعناوين الفيزيائية (MAC Address) للجهات المتبادلة للأطر (Frames) وطرق النفاذ إلى الوسط الناقل، ولكنها لا تتعامل مع وظائف الطبقات الأعلى من طبقة ربط البيانات.

تحتوى الجسور على ما يسمى بجداول التوجيه (Routing Tables).

ما هو جدول التوجيه؟

تقوم الجسور ببناء جداول التوجيه على أساس عناوين الحواسيب التي قامت بإرسال البيانات في الشبكة بالاعتماد على عناوين الجهة المرسلة للأطر.

عندما يصل الإطار إلى الجسر فأنه يقرر إهماله أو تمريره وإذا قرر تمريره فعليه أن يعرف أين سيضعه. و لكي يستطيع الجسر اتخاذ هذا القرار يجب أن يحتفظ بجداول التوجيه للحواسيب المرتبطة بالشبكة المحلية أو الشبكات المحلية التي يقوم بمهمة وصلها معاً، وعند استقباله إطار ما فإنه يقوم باختبار عنوان الجهة المرسل إليها تلك الإطار، فإذا كانت جهة الاستقبال تقع ضمن الفرع ما قبل الجسر، فإن الجسر يقوم بمنعه من المرور عبره إلى الفروع الأخرى من الشبكة، أما إذا كانت الجهة المستقبلة تقع في أحد الفروع الواقعة ما بعد الجسر فإنه يسمح له بالمرور، وبذلك فإن الجسر يقوم بتخفيف كمية المرور عبر الفروع المختلفة في الشبكات المحلية المترابطة.

أما إذا كان عنوان الجهة المستقبلة غير موجود في جداول التوجيه، فإن الجسر يُرسل الإطار إلى كل الأجهزة المتصلة على شكل رسالة مذاعة (Broadcast). أما إذا كان عنوان الجهة المستقبلة موجود في جدول التوجيه، فإن الجسر يُرسل الإطار إلى جهاز الجهة المستقبلة فقط.

كيفية بناء جداول التوجيه:

في بداية العمل يكون جدول التوجيه للجسر فارغاً، بعد ذلك وعندما تبدأ الحواسيب بنقل الأطر يضع عناوين الحواسيب المرسلة في جدول التوجيه، يتم بناء هذه الجداول بأن يستمع الجسر للشبكة، فعندما يرى حاسوب يُرسل يأخذ منه العنوان الفيزيائي (MAC Address) ومكانه في الـ Segment ويضعها في جدول التوجيه، فعندما يطلب أحد أن يرسل إلى هذه العنوان سيُحدد الجسر فوراً مكانه من الجدول ويرسل إليه الإطار دون أن تشعر بقية الحواسيب، أما إذا لم يجد هذا العنوان في الجدول يُذيع رسالة مذاعة (Broadcast) إلى جميع الشبكات (Segments) المتصلة بالجسر ما عدا التي تأتي منها الرسالة.

وظائف الجسور:

تمتلك الجسور كل مواصفات وإمكانيات مقويات الإشارة من حيث:

١. زيادة حجم الشبكة.
٢. زيادة عدد الحواسيب التي يمكن أن تستوعبها الشبكة.
٣. تعمل في طبقة ربط البيانات فهي تستطيع ربط شبكتين مختلفتين في طبقة ربط البيانات لكنها متماثلة في بنى الطبقات الأعلى.
٤. تحتوي على جداول التوجيه التي تحوي على العناوين الفيزيائية (MAC Address).
٥. تقلل الجسور من تدفق البيانات والازدحام وذلك عن طريق تقسيم الشبكة.

الجسر Bridge

خامساً- وحدة التوصيل المركزية Switches:

هو جهاز يعمل في طبقة ربط البيانات مثل الجسور لكنها تختلف في أن الـ Switches تحتفظ بجداول التوجيه (Routing Tables) مادياً بينما تحفظها الجسور في ذاكرة عشوائية (RAM) مما يعطي للمبدلات (Switches) سرعة أكبر من الجسور، كما أنها تقوم بربط أكثر من Segment مع بعضها بعض على عكس الجسور التي تقوم بربط مقطعين أو أربعة كحد أقصى.

تعمل المبدلات في طبقة ربط البيانات وبالتالي فهي تؤدي نفس وظائف الجسور وتستخدم للفصل بين الشبكات المحلية المختلفة وهي الأكثر استخداماً الآن حيث أنها تقوم بتخصيص دارات خاصة بكل شبكة محلية (Segment).

وحدة التوصيل المركزية Switch

سادساً- الموجه Router:

هو جهاز يعمل في طبقة الشبكة ويقوم بتوجيه الرسائل بين الشبكات لتذهب كل رسالة لمكانها الصحيح، ويتعامل مع مستوى طبقة الشبكة ويتميز بذكاء أكبر من الجسر.

- كما كانت الجسور تقوم بتسليم الأطر من شبكة لأخرى فإن الموجهات تقوم بتسليم الرزم من طبقات الشبكة من شبكة لأخرى دون أي تغيير في بنية الرزمة حيث تقوم بتوجيه الرزم إلى الطريق الصحيح عبر اختيار المسار الأفضل من بين عدة مسارات.

- يوجد في الموجهات أيضاً جداول التوجيه (Routing Tables) ولكن هنا تحتوي على العناوين المنطقية (IP Address).

أنواع الموجهات Routers:

١. الموجهات الساكنة:

وهي الموجهات التي يتم فيها إدخال المسارات بشكل يدوي بواسطة مدير الشبكة حيث يقوم بإضافتها إلى جداول التوجيه. وإذا تم تحديد المسار المتبع بين شبكتين فإن هذا المسار سيُسلك بشكل دائم.

٢. الموجهات الديناميكية:

وفيها يتم بناء جداول التوجيه بشكل ديناميكي بواسطة عدد من البروتوكولات حيث تُستخدم البروتوكولات المختلفة بإيجاد أفضل المسارات وتعديل جدول التوجيه مثل بروتوكول (RIP، OSPF، IGRP، EIGRP)

وظائف الموجهات Routers:

١. تعمل الموجهات في طبقة الشبكة، لذلك فهي تستطيع ربط شبكتين مختلفتين بطبقة الشبكة لكنها متماثلة في بنى الطبقات الأعلى.

٢. تحتوى جداول التوجيه في الموجهات على العناوين المنطقية IP Address.

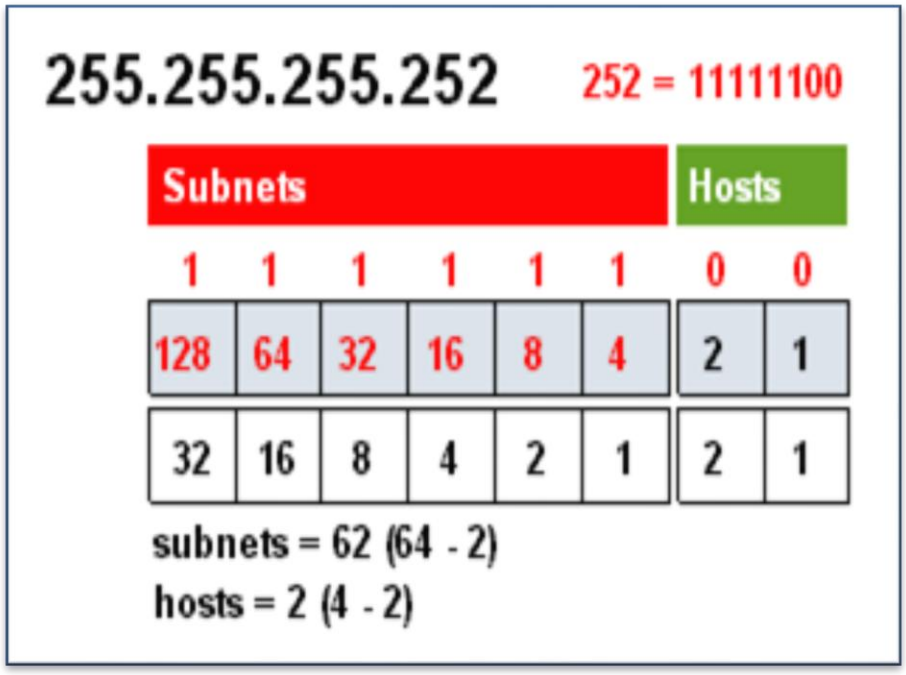
٣. اختيار المسار الأفضل حيث تستطيع الموجهات أن تختار المسار المناسب من عدة مسارات.

٤. تعمل الموجهات مع البروتوكولات الموجهة.

الموجه Router

بروتوكول IP وتقسيم الشبكة

IP Addressing and Subnetting



تتم عملية تجزئة الشبكة إلى شبكات جزئية من خلال تقسيمها إلى عدد من الشبكات الجزئية الصغيرة بحيث تحتوي هذه الشبكات الجزئية الصغيرة على عدد من المحطات يتوقف عددها على طريقة العنونة المستخدمة أو الفئة التابع لها العنوان المستخدم.

فمثلاً يمكن لمنظمة ما أن تملك عنواناً وحيداً للشبكة معروفاً بالنسبة للمستثمرين من خارج المنظمة وأن تستطيع المنظمة تشكيل الشبكة داخلياً بحيث يتم تقسيمها إلى شبكات جزئية خاصة بكل قسم في المنظمة.

فوائد تقسم الشبكة:

١- التقليل من حركة المرور و الازدحام على الشبكة، حيث كلما قل عدد الأجهزة على الشبكة قل الازدحام فيها و يمكن تحقيق ذلك بتقسيم الشبكة الكبيرة إلى شبكة أصغر تحتوي على عدد أقل من الأجهزة.

٢- تحسين أداء الشبكة.

٣- تسهيل إدارة الشبكة و حل مشاكلها.

عنوان IP وعنوان الشبكة:

- يعرف عنوان IP address بأنه معرف رقمي يتم تعيينه لكل جهاز على الشبكة بحيث يصبح عنواناً خاصاً لـه بحيث يَسهُل الوصول إليه و تحديد موقعه على الشبكة ويُسمح له بالاتصال بغيره من الأجهزة، وهو يتكون من 32 bit مقسمة إلى أربعة أقسام كل قسم من الأقسام الأربعة عبارة عن Byte واحد.
- كما يعرف عنوان الشبكة Network address بأنه العنوان المستخدم لإرسال البيانات الى شبكة محددة عن بُعد.

مثال:

الشبكة رقم: 100.0.0.0

الشبكة رقم: 172.16.0.0

الشبكة رقم: 192.168.1.0

عنوان البث:

- عنوان البث Broadcast address و هو العنوان الذي يُستخدم من قِبل الأجهزة و التطبيقات لإرسال المعلومات الى جميع الأجهزة على الشبكة.

عنوان الشبكة	عنوان البث
100.0.0.0	100.255.255.255
172.16.0.0	172.16.255.255
192.168.1.0	19.168.1.255

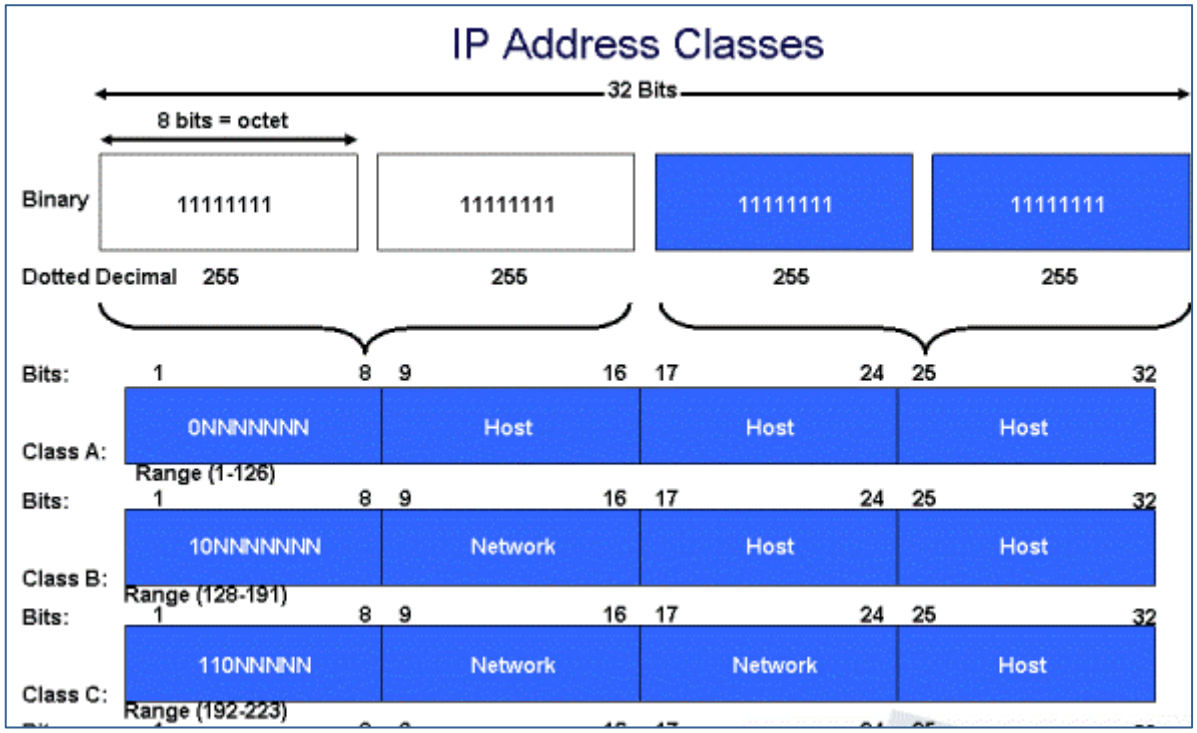
عنوان IP:

يتكون العنوان IP من حقلين هما:

١. حقل رقم الشبكة Network Identifier (Net ID) يتم من خلاله تمييز الشبكة التي يكون الجهاز عضواً فيها.

٢. حقل رقم المشترك Host Identifier (Host ID) يتم من خلاله تمييز الرقم الخاص للجهاز بداخل الشبكة.

بحيث يكون للأجهزة ضمن الشبكة الواحدة نفس رقم الشبكة، أما الرقم الخاص بالجهاز فيجب أن يكون وحيداً وفريداً ضمن هذه الشبكة.



عناوين IP الغير مسموح باستخدامها للأجهزة:

١. العنوان (0.0.0.0): حيث يستخدم هذا العنوان من قِبل موجهات شركة Cisco للإشارة الى الوجهة الافتراضية (Default Route) عند توجيه حزم البيانات.

٢. العنوان (255.255.255.255): وهو يستخدم لبث أو إرسال البيانات الى جميع الأجهزة على الشبكة الحالية.

٣. العنوان (127.0.0.1): و هو يستخدم تلقائيا من قبل الجهاز لغرض اختبار اتصاله بأن يقوم بإرسال حزمة من البيانات إلى نفسه. (Local Loop Back Self-Test).

٤. لا يمكن أن يكون الجزء من عنوان IP الخاص برقم الجهاز (Host ID) كله 255 أو 0

أمثلة لعناوين IP خاطئة:

العنوان	128.2.255.255	128.2.0.0	192.168.1.255	192.168.1.0
سبب الخطأ	عنوان بث	عنوان شبكة	عنوان بث	عنوان شبكة

٥. لا يمكن أن يكون الجزء من عنوان IP الخاص بعنوان الشبكة (Net ID) كله 255 أو 0 ،

مثال لعنوان IP خطأ:

- 0.10.20.30
- 0.0.10.20
- 0.0.0.70

فئات عنوان IP:

يوجد في عنونة IP فئات مختلفة من العنونة بحيث تحدد كل فئة جزءاً مختلفاً لكلٍ من (رقم الشبكة ورقم الجهاز). وهذه الفئات هي:

١. الفئة A (Class A):

تُخصص هذا الفئة للشبكات التي تحتوي على عدد كبير جداً من المشتركين .

Net ID	Host ID	Host ID	Host ID
01111111	00000000	00000000	00000000

في هذه الفئة من عناوين IP، يجب أن تكون قيمة البايت الأول تتراوح ما بين (1) و (126).

حيث يخصص الرقم (0) للبت الأول من NETID، وعليه فإن عدد الشبكات الفرعية الممكن تجزئتها من الفئة A هو (126) شبكة فرعية فقط وذلك من خلال المعادلة التالية: 2-(2^7)، حيث أن العدد (V) يمثل عدد (الواحدات) في جزء (NetID).

01111111	00000000	00000000	00000000

أما العدد الأقصى من الأجهزة الممكن ضمه لكل شبكة فرعية لهذه الفئة من عناوين IP هـي (216777214) جهاز، وهذا الرقم ناتج من المعادلة التالية:

2-(2^24)، حيث أن الرقم (٢٤) يمثل عدد الأصفارفي جزء (Host ID).

01111111	00000000	00000000	00000000

سؤال: لنفترض أن لدينا شبكة تابعة للمدى Class A و عنوانها 100، ما هي العناوين التي يمكن استخدامها للأجهزة؟

الجواب:

١. عنوان الشبكة هو : 100.0.0.0
٢. عنوان البث هو: 100.255.255.255
٣. عناوين الأجهزة تتراوح بين (100.0.0.1) و (100.255.255.254)

٢. الفئة B (Class B):

في هذه الفئة يتم تعيين البايت الأول و الثاني لعنوان الشبكة بينما يخصص البايت الثالث والرابع لعناوين الأجهزة، بحيث تكون قيمة البايت الأول تتراوح ما بين (128) و (191). حيث يخصص الرقم (10) للبت الأول والثاني من البايت الأول من NETID، وعليه فإن عدد الشبكات الفرعية الممكن تجزئتها من الفئة B هو (16382) شبكة فرعية وذلك من خلال المعادلة التالية: 2^14 -2).

Net ID	Net ID	Host ID	Host ID
10111111	11111111	00000000	00000000

حيث أن العدد (١٤) يمثل عدد (الواحدات ما بعد الصفر) في جزء (NetID).

أما العدد الأقصى من الأجهزة الممكن ضمه لكل شبكة فرعية لهذه الفئة من عناوين IP هي (65534) جهاز، وهذا الرقم ناتج من المعادلة التالية:

2^16)-2، حيث أن العدد (١٦) يمثل عدد (الأصفار) في جزء (HostID).

10111111	11111111	00000000	00000000

سؤال: لنفترض أن لدينا شبكة تابعة للمدى Class B و عنوانها 172.16، ما هي العناوين التي يمكن استخدامها للأجهزة؟

الجواب:

١. عنوان الشبكة هو : 172.16.0.0
٢. عنوان البث هو: 172.16.255.255
٣. عناوين الأجهزة تتراوح بين (172.16.0.1) و (172.16.255.254)

٣. الفئة C (Class C):

في هذه الفئة يتم تعيين البايت الأول و الثاني والثالث لعنوان الشبكة بينما يخصص البايت الرابع فقط لعناوين الأجهزة، بحيث تكون قيمة البايت الأول تتراوح ما بين (١٩٢) و (٢٢٣). حيث يخصص الرقم (110) للبت الأول والثاني والثالث من البايت الأول من NETID، وعليه فإن عدد الشبكات الفرعية الممكن تجزئتها من الفئة C هو (2097150) شبكة فرعية وذلك من خلال المعادلة التالية: 2-(2^21).

Net ID	Net ID	Net ID	Host ID
11011111	11111111	11111111	00000000

حيث أن العدد (٢١) يمثل عدد (الواحدات ما بعد الصفر) في جزء (NetID).

أما العدد الأقصى من الأجهزة الممكن ضمه لكل شبكة فرعية لهذه الفئة من عناوين IP هي (254) جهاز فقط، وهذا الرقم ناتج من المعادلة التالية:

2-(2^8)، حيث أن العدد (٨) يمثل عدد (الأصفار) في جزء (HostID).

11011111	11111111	11111111	00000000

سؤال: لنفترض أن لدينا شبكة تابعة للمدى Class C و عنوانها 192.168.1، ما هي العناوين التي يمكن استخدامها للأجهزة؟

الجواب:

١. عنوان الشبكة هو : 192.168.1.0
٢. عنوان البث هو: 192.168.1.255
٣. عناوين الأجهزة تتراوح بين (192.168.1.1) و (192.168.1.254)

مثال: باستخدام بتقسيم عنوان IP: 192.168.10.1إلى 4 شبكات فرعية:

الحل: لإيجاد المطلوب يجب أولا معرفة كل من:

١. قناع الشبكة الافتراضي.
٢. قناع الشبكة الجديد. (الذي سيعطى للشبكات الفرعية الجديدة).
٣. العدد الأقصى من الشبكات الفرعية الممكن إيجادها.
٤. عدد الأجهزة الأقصى في كل شبكة فرعية.
٥. عناوين الشبكات الفرعية الجديدة.
٦. عناوين البث للشبكات الفرعية الجديدة.
٧. عناوين IP الأجهزة في كل شكة من الشبكات الفرعية الجديد.

نحدد IP من أي فئة:

ننظر لأول خانة في IP وبعدها نحدد نوع الفئة:

A	١-١٢٦ أنه من كلاس
B	١٢٨-١٩١ أنه من كلاس
C	١٩٢-٢٢٣ أنه من كلاس

المطلوب هو **اربع شبكات**
أي يتم تغيير ٣ أصفار إلى واحدات.

IP :192.168.10.1

القناع الافتراضي لكلاس C هو
255.255.255.0

ثم نحدد كم شبكه مطلوبة :
مثلاً المطلوب ٤ **شبكات وفي هذا الجدول يبين لنا كم عدد البتات ومقابلها الشبكة**

عدد الشبكات	البتات
2	2
3-6	3
7-14	4
15-30	5

القناع الافتراضي هو : 255.255.255.0

11111111.11111111.11111111.00000000

Net Id Host Id

بما ان عدد الشبكه المطلوب هو
أربع شبكات أي نأخذ ٣ بت

255.255.255.11100000

يتم العمل في Host Id أما Net Id فيترك تماماً

128	64	32	16	8	4	2	1
1	1	1	0	0	0	0	0

128+64+32=**224**

- **القناع الجديد هو:**

255.255.255.224

عدد الشبكات الكلي هو : 2 - (2^3) = 8-2 = 6 شبكة

عدد الأجهزة هو : (2^5)-2 = 32-2 = 30 جهاز

وبعد ذلك نستخرج عناوين الشبكات

4	2	1	
~~0~~	~~0~~	~~0~~	ملغي X
0	0	1	الشبكة رقم ١
0	1	0	الشبكة رقم ٢
0	1	1	الشبكة رقم ٣
1	0	0	الشبكة رقم ٤
1	0	1	الشبكة رقم ٥
1	1	0	الشبكة رقم ٦
~~1~~	~~1~~	~~1~~	ملغي X

عناوين الشبكات المطلوب

192.168.10.32
192.168.10.64
192.168.10.96
192.168.10.128
192.168.10.160

4 2 1

128	64	32	16	8	4	2	1	
0	0	1	0	0	0	0	0	32
0	1	0	0	0	0	0	0	64
0	1	1	0	0	0	0	0	96
1	0	0	0	0	0	0	0	128
1	0	1	0	0	0	0	0	160

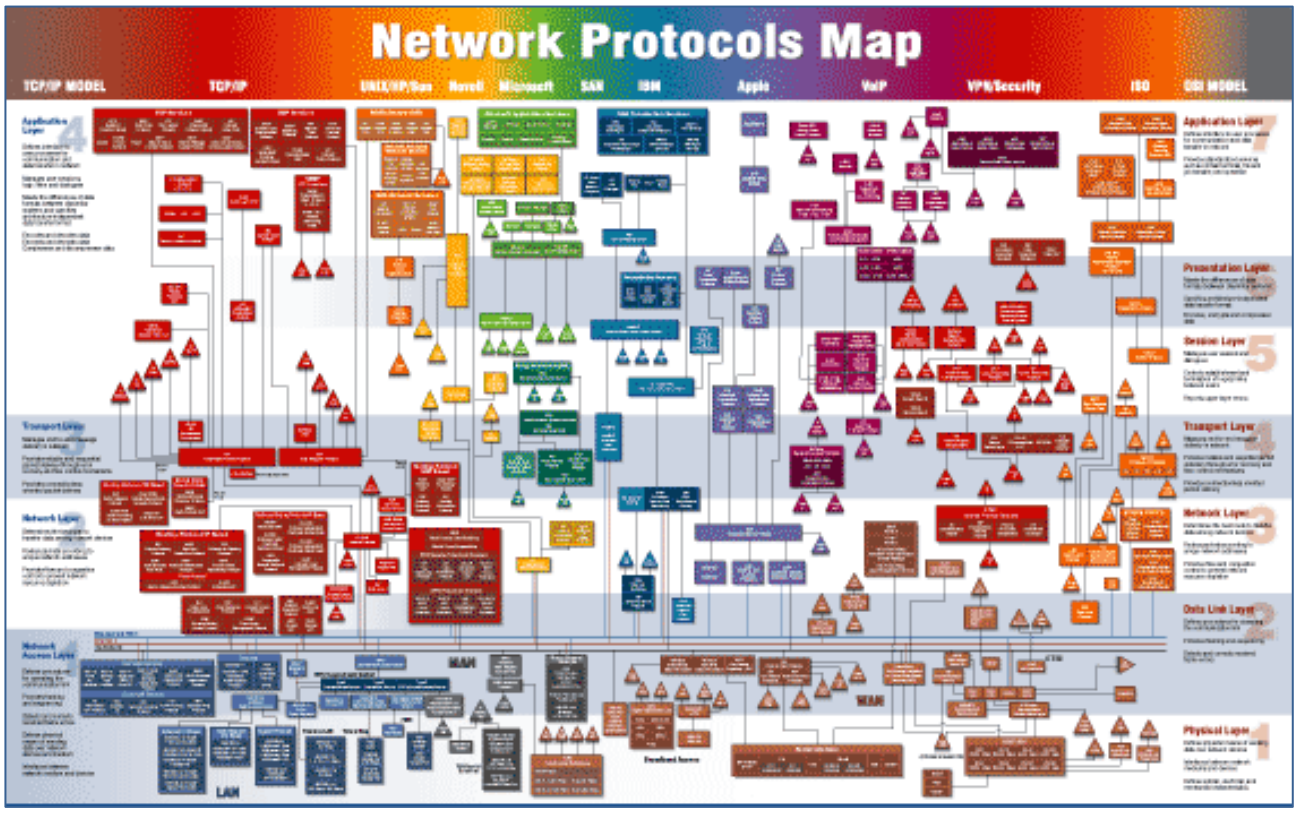
عنوان الاجهزه في كل شبكة	عنوان البـــــث	عناوين الشبكات
من 194.180.10.33 إلي 194.180.10.62	194.168.10.63	194.180.10.32
من 194.180.10.65 إلي 194.180.10.94	194.168.10.95	194.180.10.64
من 194.180.10.97 إلي 194.180.10.126	194.168.10.127	194.180.10.96
من 194.180.10.129 إلي 194.180.10.158	194.168.10.159	194.180.10.128
		194.180.10.160

عنوان البث :هو عنوان الشبكة اللاحقه ناقص واحد .

عناوين الأجهزة : من عنوان الشبكة +١ الى عنوان البث -١.

بروتوكولات الشبكة ووظائفها

Networking Protocols and its Services



يعرف البروتوكول بشكل عام بأنه مجموعة القواعد والقوانين التي تؤدي إلى تنفيذ العمل المتفق عليه بشكل سليم وخالي من الأخطاء. إن عملية تبادل المعلومات الرقمية الصادرة من حاسوب إلى آخر لابد أن تخضع إلى مجموعة من القواعد والقوانين بحيث تصل بشكل سليم، وبالتالي يمكن تعريف البروتوكول المستخدم في شبكات الحاسب الآلي بأنه مجموعة من القواعد والقوانين التي تنظم عملية الاتصال بين الحواسيب بحيث يضمن تبادل المعلومات بشكل سليم وخالي من الأخطاء. وبسبب عدم قدرة شبكات الحاسب الآلي الاتصال ببعضها البعض، لتتمكن من تبادل المعلومات، قامت عدة هيئات ولجان دولية بوضع معايير قياسية مناسبة لشبكات الحاسب الآلي لجعل هذه الشبكات تتصل فيما بينها.

المهام الأساسية لبروتوكول شبكات الحاسب الآلي

قبل أن نقوم بدراسة أهم البروتوكولات المستخدمة في شبكات الحاسب الآلي المختلفة، لابد من معرفة أهم المهام الأساسية التي يجب أن تتوفر في بروتوكول شبكات الحاسب الآلي، هذه المهام تختلف حسب ما يكون هذا الحاسوب هو الذي يقوم بإرسال المعلومات أو أن يقوم باستقبال هذه المعلومات.

مهام البروتوكول في الحاسب المرسل

١. تقسيم المعلومات إلى رزم صغيرة.
٢. إضافة معلومات خاصة بالعنونة إلى الرزم.
٣. إضافة معلومات خاصة باختبار حدوث الخطأ في البيانات.
٤. إضافة معلومات خاصة بنوع البروتوكول.

بعد ذلك يتم إرسال هذه الرزم عبر بطاقة الشبكة ومن ثم عبر الكابل إلى الحاسوب المستقبل.

مهام البروتوكول في الحاسب المستقبل

١. استلام الرزم من الكابل.
٢. نقل هذه الرزم عبر بطاقة الشبكة إلى الحاسوب.
٣. بعد التأكد من سلامة المعلومات يتم حذف معلومات التحكم.
٤. تجميع الرزم وإعادة تشكيل المعلومات الأصلية لإعطائها إلى البرنامج.
٥. اختبار سلامة المعلومات من الأخطاء بعد التجميع.

مهام البروتوكول

١- تقسيم المعلومات إلى رزم صغيرة

لا يمكن لمعلومات كبيرة الحجم أن تنتقل دفعة واحدة عبر الكابل، لذلك لابد من تقسيمها إلى رزم صغيرة للأسباب التالية:

- عند تقسيم المعلومات إلى رزم صغيرة، هذا يؤدي إلى أن الحاسوب لا يستأثر بالكابل لوقت كبير ، مما يسمح لحواسيب أخرى بالإرسال عبر الكابل.
- عند حدوث خطأ في الإرسال فإنه من السهل إعادة إرسال الرزم الذي حدت فيها الخطأ.
- إن عملية تقسم المعلومات إلى رزم صغيرة يسمح للحواسيب المستقبلة استخدام ذواكر صغيرة لاستقبال الرزم.
- بعض شبكات الاتصالات قد لا تكون قادرة على التعامل مع المعلومات ذات الحجم الكبير.

مساوئ تقسيم المعلومات إلى رزم صغيرة

- إن عملية إضافة معلومات التحكم إلى الرزم يؤدي إلى زيادة المعلومات المرسلة.
- زيادة طلبات المقاطعة في الحاسوب المستقبل، مما يؤدي إلى توقيف الأعمال التي يقوم بها الحاسوب والاتجاه إلى خدمة هذه المقاطعة.
- زيادة زمن المعالجة كلما ازدادت عدد الرزم.

٢- إضافة معلومات خاصة بالعنونة إلى الرزم

هذه المعلومات تحتوي كل من عنوان الحاسوب المرسل وعنوان الحاسوب المرسل إليه.

٣- معلومات خاصة باكتشاف حدوث خطأ

هذه المعلومات تسمى (CRC Cyclical Redundancy Check)، وتنتج عندما يقوم الحاسوب المرسل بإرسال الرزمة، يقوم بإجراء عملية حسابية على البيانات الموجودة في الرزمة قبل إرسالها، ويضع ناتج هذه العملية الحسابية في حقل اكتشاف الأخطاء CRC، وعند وصول هذه الرزمة إلى الحاسوب المستقبل فإنه يقوم بإجراء نفس العملية الحسابية على البيانات في الرزمة ويقارن نتيجة العملية الحسابية مع ما هو موجود في حقل كشف الخطأ (CRC) للتأكد من أن البيانات قد وصلت بشكل سليم، أما إذا اختلفت النتيجة عند وصول الرزمة عن ما هو موجود في الحقل (CRC) فهذا يدل على أن البيانات بها أخطاء ولم تصل بشكل سليم.

تصنيف البروتوكولات حسب التوجيه

١. البروتوكولات الموجهة Routable Protocols

وهي البروتوكولات التي تسمح بمرور البيانات بين الشبكات وفق مسارات متعددة، حيث أن البيانات تنتقل من شبكة محلية إلى شبكة محلية أخرى عبر المسارات المختلفة باستخدام الموجهات Routers.

٢. البروتوكولات غير الموجهة Non Routable Protocols

وهي البروتوكولات التي لا يسمح لها بالمرور عبر الموجهات.

تصنيف البروتوكولات حسب طريقة توصيل البيانات

١. طريقة توصيل البيانات المضمون Oriented Connection

تعتمد هذه الطريقة بأن ينتظر المرسل من المستقبل وصول رسالة تأكيد Acknowledgement بوصول البيانات بشكل سليم وخالية من الأخطاء، هذه طريقة مضمونة في إرسال البيانات، ولكن عيبها هو البطء وزيادة الضغط على الشبكة بسبب ضرورة انتظار استقبال رسالة تأكيد وصول من المستقبل.

بعض أنواع بروتوكولات الشبكة:

أ. البروتوكول NetBEUI (Network BIOS Extended User Interface)

وهو بروتوكول يعمل في طبقة النقل أنتجته شركة Microsoft للربط بين شبكاتها، هذا البروتوكول سريع في الشبكات الصغيرة، ولا يمكن نقله عبر الموجهات، لذا فهو يعتبر من البروتوكولات غير الموجهة Non Routable Protocol.

- إذا كانت الشبكة صغيرة، وكل منتجاتها من شركة Microsoft ولا يستخدم فيها الموجه Router فأفضل بروتوكول يستخدم هو NetBEUI.
- يفضل استعمال البروتوكول NetBEUI وبروتوكول آخر وليكن TCP/IP على كل حاسوب بحاجة إلى الوصول إلى شبكة واسعة WAN أو عبر الموجهات Routers.
- عند تثبيت بروتوكولين على الحاسوب، يستعمل البروتوكول NetBEUI للاتصال بين الحواسيب ضمن كل جزء من شبكة محلية LAN ويستعمل البروتوكول TCP/IP للاتصال عبر الموجات Routers إلى الأجزاء الأخرى في الشبكة WAN.

ب. البروتوكول IPX/SPX :

- يستخدم هذا لبروتوكول في شبكات Novell في نظام التشغيل Netware لنقل البيانات داخل الشبكات .
- إن كلمة IPX/SPX:

Sequenced Packet Exchange / Internet Packet Exchange.

فهو يتكون من جزئين :

أ.البروتوكول SPX: وهو مسؤول عن نقل البيانات في طبقة النقل .

ب.البروتوكول IPX: وهو مشابه لعمل البروتوكول IP وهو يعمل في طبقة الشبكة ، إن البروتوكول IPX/SPX هو برتوكولاً موجهاً Routable ويستخدم في الشبكات الواسعة WAN والشبكات المحلية LAN وهو أسرع من البروتوكول TCP/IP لأنه لا يحتاج إلى عملية ضبط مثل البروتوكول TCP/IP.

ج. البروتوكول NWLink :

وهذا البروتوكول مشابه للبروتوكول IPX/SPX وأصدرته شركة Microsoft لتتفاهم مع شبكات Novell.

د. بروتوكول طبقة المقابس الآمنة SSL (Secure Sockets Layer)

بروتوكول تشفير يعمل على توفير بيئة آمنة خلال نقل البيانات المشفرة بين المتصفح وجهاز الخادم في الموقع، وما يحدث باختصار هو أنّ المتصفح يقوم بإرسال رسالة من خلال بروتوكول SSL إلى جهاز الخادم فيستجيب ويرسل شهادة (SSL Certificate) تتضمن في محتواها المفتاح العام للموقع (Public Key)، ومن ثم يقوم المتصفح بالتحقق من هذه الشهادة من خلال ثلاثة ركائز أساسية:

١. أن تكون الشهادة آتية من طرف موثوق به.
٢. التحقق من سريان مفعولها في الوقت الحالي، وذلك من خلال إلقاء نظرة على تاريخ إصدار الشهادة وتاريخ انتهائها.
٣. المقارنة بين اسم الموقع في الشهادة واسم الموقع في الخادم للتأكد من أن الشهادة مرتبطة بالموقع وقادمة منه.

وبعد التحقق من الشهادة يعمل على إنشاء مفتاح متناظر للتشفير (Symmetric Key Encryption) يقوم بدوره على تشفير البيانات التي تنتقل من المتصفح إلى جهاز الخادم باستخدام بروتوكول التحكم بالإرسال وبروتوكول الإنترنت (TCP/IP) مما يضمن عدم التعرّض لهذه البيانات من قبل أي جهة أخرى فلا يمكن لأحد قراءتها سوى المرسل والمستقبل، وفي نهاية المطاف يقوم الموقع بفك شيفرة الرسالة الواردة إليه من

المتصفح وذلك باستخدام مفتاح خاص بالموقع ذاته (Private Key) ثم يستخدم المفتاح العشوائي لبقية الاتصال.

الجدير بالذكر أن استخدام هذه التقنية يعمل على إحداث تغيير طفيف في عنوان الموقع الإلكتروني كالبنك مثلاً وهذه دلالة واضحة على وجود أمن معلوماتي في المنشأة. وعند التطرق إلى مثال البنك فإننا نلحظ عند الدخول إلى موقع البنك بأن عنوانه يبدأ بـ (http) ولكن بمجرد الضغط على صفحة تسجيل الدخول إلى الحساب فإن العنوان يتغير إلى (https)، بالإضافة إلى أيقونة الأمان والتي تظهر في أسفل صفحة الموقع.

هـ. البروتوكول TCP/IP: (Transmission Control Protocol / Internet Protocol) يتكون من جزئين:

أ- البروتوكول TCP: وهو بروتوكول التحكم بالنقل، وهو المسئول عن عملية نقل البيانات في طبقة النقل.

ب- البروتوكول IP: وهو بروتوكول الإنترنت، وهو البروتوكول الأساسي في الإنترنت والمسئول عن تنظيم عناوين الإنترنت، ويعمل في طبقة الشبكة.

إن البروتوكول TCP/IP ليس بروتوكول واحد أو اثنين، وإنما هو عبارة عن مجموعة من البروتوكولات ذات المعايير الصناعية صممت لتكون قابلة للتوجيه، ولتعمل بشكل موثوق وبفاعلية كبيرة.

- يعتبر البروتوكول TCP/IP البروتوكول الأساسي للإنترنت وهو بروتوكول موجه Routable Protocol أي أنه يمكن تمريره عبر الموجهات Routers التي تربط الشبكات بعضها مع بعض.
- يحتاج هذا البروتوكول إلى ضبط المتغيرات التالية:
  - IP Address عنوان الإنترنت.
  - Subnet Mask قناع الشبكة.
  - Default Gateway البوابة الافتراضية وهو عنوان بوابة الشبكة (عنوان الـ Router الذي يستخدم كبوابة للشبكة).
  - IP Address of DNS Server.

البروتوكولات التي تعمل تحت بروتوكول TCP/IP:

١. **SMTP** : بروتوكول نقل البريد الإلكتروني (Simple Mail Transfer Protocol).
وهـو البروتوكـول المستخـدم في إرسـال واستقبـال البريـد الإلكترونـي في الإنترنت.

٢. **SNMP** : بروتوكول إدارة الشبكات (Simple Network Management Protocol)
يستخدم هذا لبروتوكول في إدارة ومراقبة الشبكات.

٣. **FTP** : بروتوكول نقل الملفات (File Transfer Protocol)
يستخدم هذا البروتوكول في نقل الملفات من حاسوب لآخر داخل الشبكة.

٤. **TFTP** : (Trivial File Transfer Protocol)
هو نسخة مصغرة من بروتوكول FTP حيث يستخدم لنقل الـ Boot Image للأجهزة التي لا يوجد بها قرص إقلاع (Boot Disk) وأيضاً من و إلى الموجهات (Routers).

٥. **POP** : (Post Office Protocol)
هو البروتوكول الذي يستخدمه عميل البريد الإلكتروني لاسترجاع بريده من الخادم، بحيث يسمح هذا البروتوكول للمستخدم بتحميل جميع الرسائل إلى جهازه ومن ثم قراءتها، فهو مناسب للمستخدمين ذوي الاتصال الضعيف أو المتقطع أو ذو التكلفة العالية لأنه يمكنهم من تصفح الرسائل في حلة عدم الاتصال بالإنترنت.

٦. **IMAP** : (Internet Message Access Protocol)
يسمح هذا البروتوكول للمستخدم بالدخول إلى الخادم واختيار الرسائل التي يرغب في قراءتها والاطلاع عليها مع إمكانية تحميلها مع بقاءها على الخادم دون حذفها ودون الحاجة لتحميلها كاملة، لذلك فهو مناسب للذين يملكون اتصالا جيدا ومستمرا بالإنترنت ورخيص التكاليف. كما يتميز هذا البروتوكول بإمكانية البحث في الرسائل الموجودة على الخادم وإمكانية الوصول للبريد من عدة أطراف (جهاز عمل، جهاز المنزل، الهاتف الذكي، ..... إلخ) مع إمكانية تقسيم الرسائل إلى عدة صناديق يريد إضافة إلى أن الرسائل عبر هذا البروتوكول أدعى للحفظ خصوصاً عند المحافظة على أخذ النسخ الاحتياطية بشكل مستمر.

٧. **Telnet** : (Terminal Emulation Protocol)
يستخدم هذا البروتوكول في إنشاء اتصال عن بُعد بالأجهزة على الشبكة.

٨. **ICMP** : (Internet Control Message Protocol)

يستخدم هذا البروتوكول مع الأمر (Ping) وذلك للتحقق من وجود جهاز (Host) على الشبكة.

٩. **HTTP** : (Hypertext Transfer Protocol)

يستخدم هذا البروتوكول من أجل فتح مواقع الإنترنت على متصفحات الإنترنت (Internet Browsers) حيث يشكل هذا البروتوكول وسيلة التخاطب ما بين الأجهزة وخوادم الإنترنت (Web Servers).

١٠. **ARP** : (Address Resolution Protocol)

يستخدم هذا من أجل معرفة معلومات عن بطاقة الشبكة و عنوان IP الخص بها.

١١. **NTP** : (Network Time Protocol)

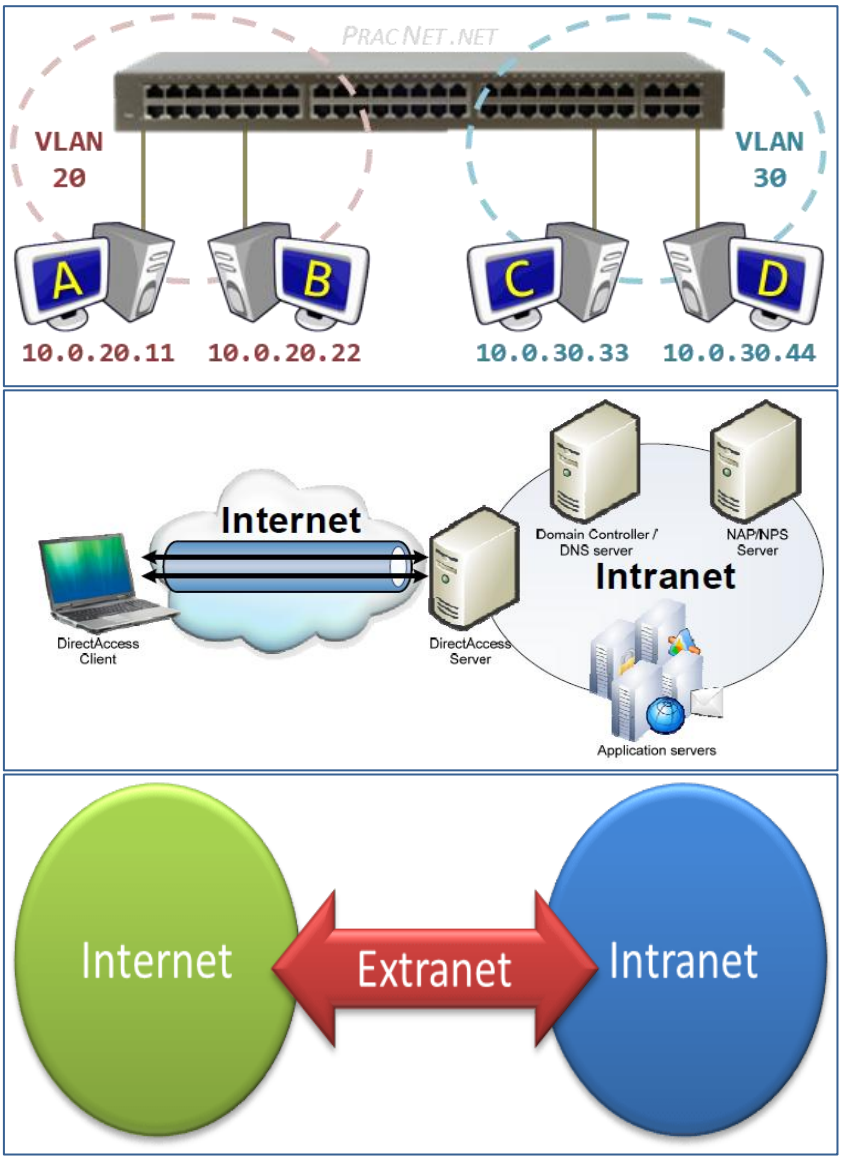
يستخدم هذا البروتوكول من أجل توحيد توقيت الأجهزة المتصلة بالشبكة.

١٢. **UDP** : (User Datagram Protocol)

يستخدم هذا البروتوكول من أجل توفير اتصال مباشر بين البرمجيات و بروتوكول (IP) كما يتيح الاتصال بخدمة أو برنامج معين عبر منفذ محدد على جهاز حاسب آلي آخر على ا لشبكة.

الشبكات الوهمية- الشبكات الداخلية والخارجية

VLANs- Intranet - Extranet



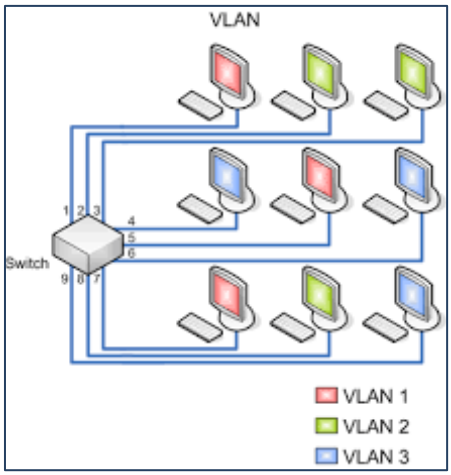
الشبكة الظاهرية VLAN:

VLAN هو اختصار لجملة (Virtual Local Area Network) أي التقسيم التخيلي أو الوهمي للشبكة المحلية (LAN) بحيث تصبح الشبكة المحلية الواحدة عبارة عن عدة شبكات محلية افتراضية. حيث تستخدم في الشبكات المحلية LAN لعزل المستخدمين عن بعضهم بهدف الحماية والأمن بالإضافة إلى رفع أداء الشبكة من خلال عزل مجال البث (Broadcast Domain) في المبدلات (Switches).

سميت بهذا الاسم لأنه في الواقع عندما ننظر الى بنيتها يظهر لنا وكأنها شبكة واحدة (ظاهرياً)، ولكنها في الواقع تكون أكثر من شبكة واحدة، حيث أن الـ Switch هنا يقوم بتقسيم الشبكة الواحدة الى عدة شبكات كل منها منفصل عن الآخر أي لا يمكن لأجهزة "شبكة تخيلية" الاتصال بأجهزة "شبكة تخيلية" أخرى مع أنهم مرتبطين مادياً بجهاز Switch واحد .

مجال البث (Broadcast Domain):

من مزايا الشبكات المحلية (LAN) إمكانيـــة ارسال البيانات مـــن المَصدر (Source) لجميع الأجهزة دفعـة واحدة حيث تسمى هـذه العمليـة بالبث (Broadcast)، حيث يكون عنوان المرَسل إليه (Destination Address) داخل الـ(Frame) المُرسل هو عنوان جميع الأجهزة و عند وصول الـ (Frame) لجهاز الـ (Switch) فإنه يقوم بإعادة إرساله من جميع منافذ جهاز الـ (Switch). وهنا يعتبر جهاز الـ (Switch)مجالا واحدا للبث (Broadcast Domain).
أي أن (Broadcast Frame) المُرسل من طرف سيصل لجميع الأطراف المرتبطة بجهاز الـ (Switch).



شبكة VLAN

الفرق بين Subnetting و VLAN:

التقسيم (Subnetting) هو مفهوم تقسيم عنوان الشبكة (Network Address) الواحد بغض النظر عن فئته (Class A، Class B أو Class C) إلى مجموعة من الشبكات الفرعية (Sub Networks) و لكلٍ منها استقلالها الخاص.

وهنا نستنتج بأن تقسيم الشبكة إلى شبكات فرعية (Subnetting) هو مفهوم و ليس بروتوكولاً أي أنه ليس خاص بالموجهات (Router) أو المبدلات (Switch) .

اذا الـ VLAN تستخدم لتقسيم منافذ جهاز الـ (Switch) إلى مجموعة من مجالات البث (Broadcast Domains) وكل مجال بث يحمل عنوان شبكة (Network Address) أو قناع شبكة فرعية (Subnet Mask) مختلف.

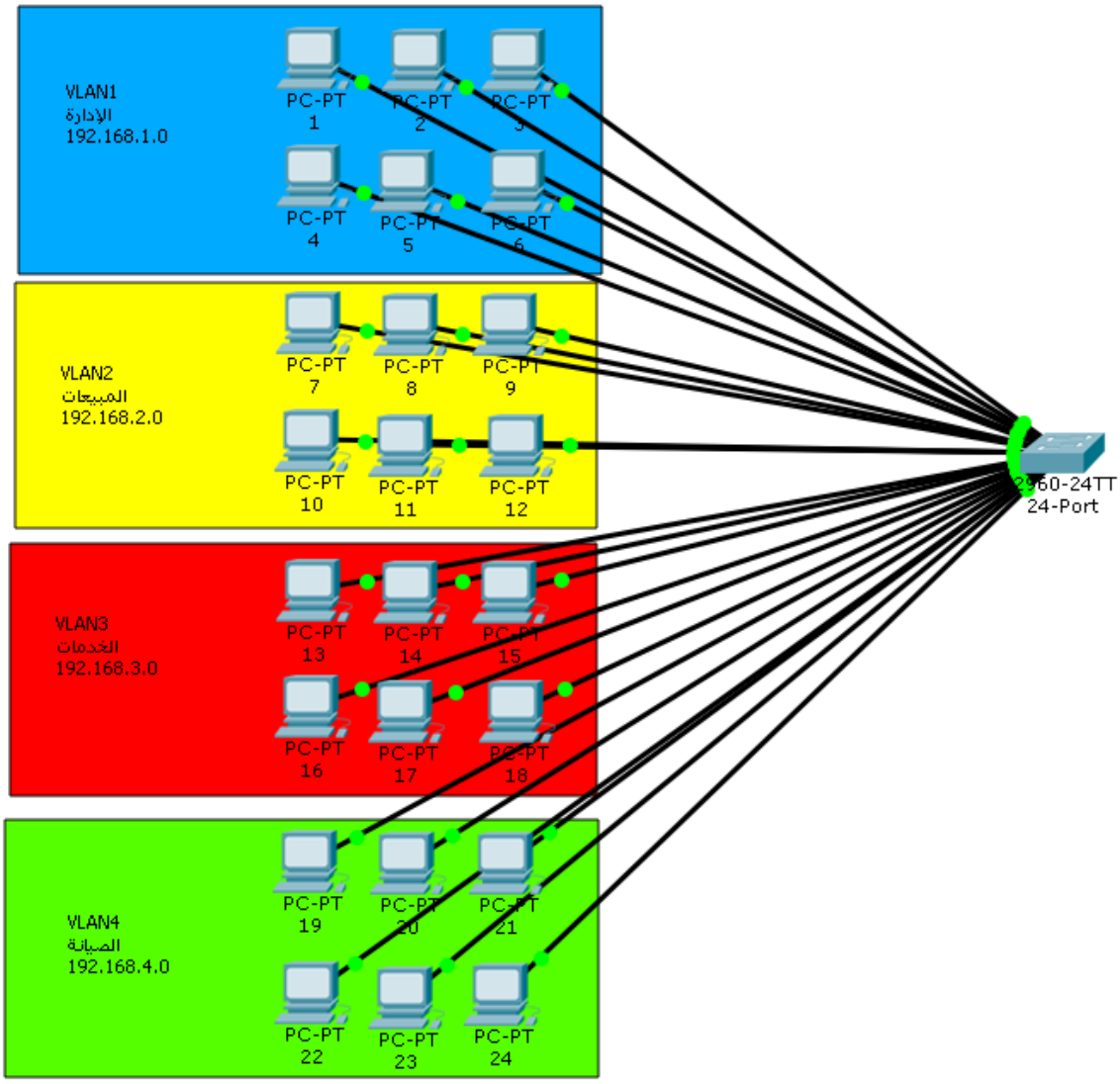
مثال:

شركة تتكون من الأقسام التالية (المبيعات، الصيانة، الخدمات، الإدارة) وأجهزة هذه الأقسام متصلة جميعها بجهاز (Switch) واحد يتكون من (٢٤ منفذ). فإن الوضع الافتراضي (بدون استخدام VLAN) لهذه الأجهزة أن تكون جميعها تحمل نفس عنوان الشبكة ولكن باستخدام تقنية (VALN) فإننا سنقوم بتقسيم منافذ الـ (Switch) كالتالي:

١. المنافذ من (١-٦) تخصص لأجهزة قسم الإدارة (VLAN1).
٢. المنافذ من (٧-١٢) تخصص لأجهزة قسم المبيعات (VLAN2).
٣. المنافذ من (١٣-١٨) تخصص لأجهزة قسم الخدمات (VLAN3).
٤. المنافذ من (١٩-٢٤) تخصص لأجهزة قسم الصيانة (VLAN4).

ولكل شبكة وهمية عنوانها الخاص كما في الجدول:

رقم المنفذ	القسم	اسم الشبكة	عنوان الشبكة
١،٢،٣،٤،٥،٦	الإدارة	VALN1	192.168.1.0
٧،٨،٩،١٠،١١،١٢	المبيعات	VALN2	192.168.2.0
١٣،١٤،١٥،١٦،١٧،١٨	الخدمات	VALN3	192.168.3.0
١٩،٢٠،٢١،٢٢،٢٣،٢٤	الصيانة	VALN4	192.168.4.0



ملاحظة:

لكي تتحدث VLANs مختلفة مع بعضها بعض في أكثر من جهاز (Switch) فإنه لابد من وجود جهاز موجه (Router) يربط هذه الـ (Switches) ببعض.

فوائد الشبكات الوهمية (VALNs):

تقسيم الشبكة ل VLANs مهم جدا عند بناء الشبكات المحلية، فمن الضروري عزل الخوادم بـ VLANs، وذلك لكي لا تتأثر هذه الخوادم بوضعية أجهزة المستخدمين من ناحية وجود ملفات ضارة أو تخريبية (warms, Trojans, Viruses) تتنشر عبر الشبكة ذاتيا، وهذا يعني رفع درجة الحماية على الخوادم، بالإضافة إلى المحافظة على أداء الخوادم. على سبيل المثال يفضل استخدام VLAN للخوادم التي لا تعمل من خلال الانترنت، واستخدام VLAN أخرى للخوادم التي تقتضي طبيعة عملها الاتصال بشبكات الانترنت. وكذلك يتم تقسيم الأجهزة الطرفية (Workstations) في عدة شبكات افتراضية (VLANs) حسب طبيعة عملها ، فمثلا توضع أجهزة المستخدمين (PCs) في أكثر من VLAN، وال (IP Cameras) في VLAN، Network Printers في VLAN، وأيضا (IP phones) في VLAN، وهكذا. مما يسهل التحكم في الشبكة والصلاحيات الممنوحة للمستخدمين، وتطبيق الأولويات وجودة الخدمة (QoS) على أنواع معينة من الخدمات والبروتوكولات.

وعليه فإن فوائد استخدام شبكات VLAN تتلخص في:

١. الـ VLAN يجزئ مجال البث (Broadcast Domain) إلى أجزاء لأن كل VLAN تعتبر Broadcast Domain مستقل بذاته.
٢. يقلل من Broadcast في الشبكة. و هذا يقلل من ال Congestion أو الاختناق الذي يحصل في الشبكة نتيجة تدفق البيانات Data إلى كل جهاز (Hosts).
٣. توفر حماية وأمن عالي للشبكة.
٤. سهولة في إدارة الشبكة.
٥. يسهل انتقال أجهزة الكمبيوتر في الشبكة.
٦. يسهل إضافة أجهزة في الشبكة.

الشبكة الداخلية Intranet:

الإنترانت عبارة عن شبكة كمبيوتر خاصة بمؤسسة ما تستعمل البروتوكولات والقواعد التي بني عليها الإنترنت وذلك كي تُمَكّن الأفراد والعاملين في تلك المؤسسة من الاتصال ببعضهم البعض والوصول إلى المعلومات بطريقة أسرع وأفضل وأكثر كفاءة وأقل كلفة من الأساليب التقليدية المعتادة. فهي (Intranet) تقوم بتسهيل الأعمال العديدة التي يتطلبها المكتب والتي يمكن أن تأخذ وقتا وجهدا ومالا كبيرا لإنجازها. من هذه الأعمال على سبيل المثال لا الحصر الاجتماعات والتحدث على الهاتف وتحضير الرسائل والمذكرات وإرسال الرسائل بالبريد أو الفاكس وغيرها.

الإنترانت في الواقع هي نسخة مصغرة من الإنترنت تعمل داخل المؤسسة. بحيث يكون العاملون بها هم الوحيدين القادرون على الوصول إليها. ولا تحتوي الإنترانت من المعلومات إلا تلك التي توافق عليها إدارة المؤسسة. كما تسمح الإنترانت للمؤسسة أن تكون على اتصال بالإنترنت (لأشخاص محددين وليس للجميع) بدون أن تتأثر بالمشاكل التي يسببها المستخدمون من الخارج بسبب الوصول إلى المعلومات الخاصة داخل شبكة كمبيوتر المؤسسة حيث أن من أهم المساوئ التي تترتب بسبب اتصال المؤسسات بشبكة الإنترنت العالمية واستخدامهم لها هو إمكانية استخدام الإنترنت في أعمال وتطبيقات غير مفيدة للشركة أو المؤسسة بواسطة موظفيها.

لهذه الأسباب وغيرها فإن العديد من المؤسسات قد ابتعدت عن استخدام شبكة الإنترنت العالمية الواسعة واقتصرت على إنشاء الإنترانت، فالإنترانت الخاص بمؤسسة ما عبارة عن إنترنت داخلي تم تفصيله ليكون ملائما لهذه المؤسسة ولكنه غير متصل بالعالم الخارجي إلا في نطاق محدد وذلك لإمكانية القيام بتحديد درجة اتصاله بالعالم الخارجي. كما يمكن للإنترانت أن يصل للإنترنت بدون أن يكون العكس أي من الإنترنت إلى الإنترانت و من هذا يتبين لنا المزايا العديدة للإنترانت. أن الفرق بين الإنترانت و الإنترنت يمكن تلخيصها فيما يلي:

الإنترنت:

١. غير مملوك لأحد.

٢. أي شخص يمكنه الوصول إليه.

٣. يمكن الوصول إليه من أي مكان أو موقع.

٤. يحتوي على العديد من المواقع أو الصفحات المتضمنة معلومات غير لائقة أو سخيفة.

الإنترانت:

١. هو ملك المؤسسة التي تستضيفه.

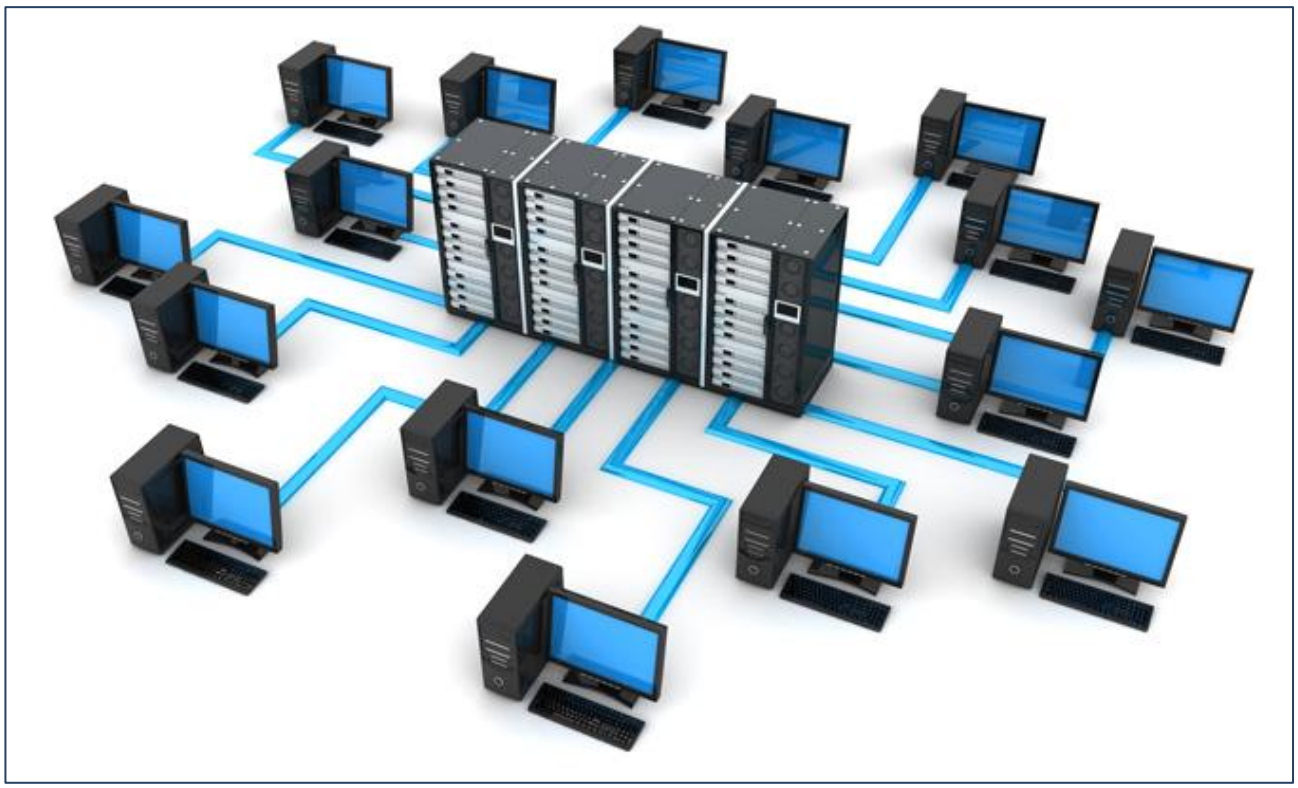
٢. لا يمكن لأي شخص الوصول إليه إلا الذين سمح لهم بذلك.

٣. يعمل فقط في موقع واحد.

٤. يحتوي على المواضيع والمعلومات التي توافق عليها المؤسسة.

أوجه الشبه بين الإنترانت والإنترنت فهي:

١. كل من النظامين يستخدمان صفحات كتبت بلغةHTML .
٢. يستعمل كل منها برنامج التصفح لمشاهدة الصفحات.
٣. كل منهما يستعمل نفس المعايير أو البروتوكولات في أسلوب استقبال وإرسال المعلومات وحركتها عموما عبر خطوط أو وسائل الاتصال بين أجهزة الكمبيوتر.



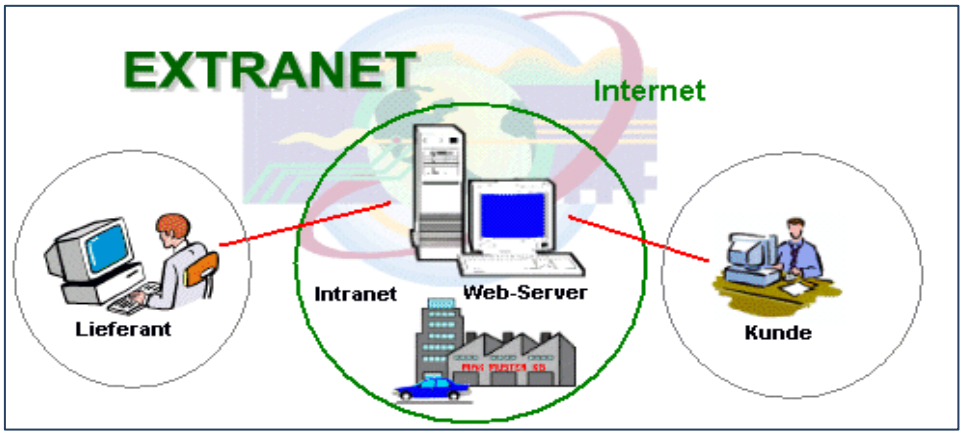
شبكة Intranet

الشبكة الخارجية Extranet:

شبكة الإكسترانت هي الشبكة المكوّنة من مجموعة شبكات إنترانت ترتبط ببعضها عن طريق الإنترنت، وتحافظ على خصوصية كل شبكة إنترانت مع منح أحقية الشراكة على بعض الخدمات والملفات فيما بينها .أي إن شبكة الإكسترانت هي الشبكة التي تربط شبكات الإنترانت الخاصة بالمتعاملين والشركاء والمزودين ومراكز الأبحاث الذين تجمعهم شراكة العمل في مشروع واحد، أو تجمعهم مركزية التخطيط أو الشراكة وتؤمن لهم تبادل المعلومات والتشارك فيها دون المساس بخصوصية الإنترانت المحلية لكل شركة.

استخدام شبكة الإكسترانت:

١. نظم تدريب وتعليم العملاء.
٢. نظم التشارك على قواعد البيانات بين الجامعات ومراكز الأبحاث التابعة لحكومة ما أو لإدارة معينة.
٣. شبكات مؤسسات الخدمات المالي و المصرفية.
٤. نظم إدارة شؤون الموظفين والموارد للشركات العالمية المتعددة المراكز و الفروع .



شبكة Intranet

التغلب على كوارث الشبكات

Network Disaster Recovery

قد تتعرض الشبكات في كثير من الحالات لكوارث أو هجمات منها ما هو مقصود ومنها ما هو وغير ذلك، وعليه فأن من مهام مدير الشبكة حماية البيانات والمعلومات من الضياع أو تلفها أو فقدها، حيث تكون من مسؤولياته تحديد نوع النظام الذي يعمل عليه وما هي المدة التي لن تضرر منها الشبكة إذا توقف النظام عن العمل وما هي المدة التي تتطلب أن يكون النظام يعمل بكفاءة عالية دون أخطاء أو مشاكل.

- أنواع الأنظمة:

أولاً- المواقع الساخنة Hot Sites:

هذا النوع من العمل يتطلب أن يكون النظام يعمل بنسبة ١٠٠% بدون أخطاء أو مشاكل، ويعتبر هذا النوع من الأعمال لا يخضع لنظرية التغلب على الكوارث (Disaster Recovery) لأنه لا يجب أن يحدث أي من الأشياء المتعلقة بضياع المعلومات، ويعتمد هذا النظام على أكثر من مكان لتخزين البيانات، ويتكلف هذا النظام مبالغ باهظة جدا للمحافظة على المعلومات، على سبيل المثال أجهزة الحواسيب التي تعمل في المطارات، الحكومات، المستشفيات والبنوك.

هذه الأنظمة تعتمد على تقنية التجمع (Clustering Technology) والتي تعتمد على وجود أكثر من جهاز مرتبطين ببعضهما البعض للحصول على أداء عالي ودقة في معالجة البيانات والحفاظ عليها.

بعض المواقع الساخنة Hot Sites

ثانياً- المواقع الدافئة Worm Sites:

يعتمد هذا النظام في العمل كون المعلومات متوفرة بنسبة ٨٥% بمعنى أنها متوفرة في أغلب الأوقات، والمعلومات التي توجد في هذا النظام أقل أهمية من المعلومات التي توجد في الأنظمة الحارة Hot Sites.

يعتمد هذا النظام على وجود ما يسمى الخوادم المكررة Duplicate Servers فهو جاهز ليعمل أو ليحل محل أي جهاز آخر في المنظومة عند حدوث المشكلة، وعندما يتم إصلاح الجهاز الذي حدثت به المشكلة يصبح هو Duplicate Server حتى تحدث مشكلة يحل محل جهاز آخر وهكذا.

يعتبر هذا النظام أقل كلفة من Hot Site إلا أن احتمال ضياع البيانات في هذا النظام محتمل كونه يعتمد على النسخ الاحتياطي Backup فلوم لم تتم عملية النسخ الاحتياطي بشكل دوري ومنظم أو حدث بشكل خاطئ فإن هذا سيؤدي إلى ضياع المعلومات وفقدانها.

ثالثاً- المواقع الباردة Cold Sites:

يعتمد هذا النظام على خبير الدعم الفني أو الصيانة، فهو لا يعدو يعتمد إلا على نظام لاستعادة البيانات عند فقدها فإذا حدثت مشكلة ما فسوف يحاول خبير الدعم الفني حل المشكلة بأي وسيلة حتى يعود النظام إلى العمل ولحين إصلاح المشكلة سوف يظل الخادم Server معطل وهذا يدل على أن نوعية البيانات في النظام ليس كمثيلاتها السابقة وهذا النظام لا يضمن أبدا أداء عالياً في الخوادم.

- عوامل المحافظة على البيانات:

١. إدارة الطاقة Power Management:

من أهم الأشياء التي يجب أن تتبعها للمحافظة على البيانات هي مصادر الطاقة مثل UPS أو Power Surges Protectors والعديد من الأجهزة الأخرى التي تحمي الأجهزة من تذبذب التيار أو انقطاعه أو حتى من الصواعق، وكل هذا يختلف حسب درجة أو أهمية البيانات الموجودة في المنظومة المعلوماتية.

٢. تسامح الأخطاء في أقراص النظام Disk System Fault Tolerance:

من أهم عوامل المحافظة على نظام المعلومات هو القرص الصلب ونظام الملفات عليه وكيفية تخزين البيانات عليه لأن معظم مشاكل ضياع البيانات تكون بسبب الأقراص الصلبة ولهذا فإنه باستخدام تقنيات إدارة الأقراص المختلفة في أنظمة التشغيل مثل (Mirroring، Raid) إمكانية استعادة البيانات من القرص عند حدوث أي مشكلة.

٣. النسخ الاحتياطي Backup System:

من أهم العوامل في المحافظة على المعلومات في المؤسسة هو النسخ الاحتياطي Backup System حيث يمكن استخدام برمجيات مثل System Backup أو استخدام برمجيات منفصلة تدعم إعدادات أكثر احترافية في التعامل مع البيانات، كما يمكن استخدام أكثر من وسط تخزين لنقل البيانات مثل الأقراص الصلبة، الأشرطة الممغنطة وغيرها من وسائط التخزين المختلفة.

٤. الحماية من البرمجيات الخبيثة Virus Protection:

إن الحماية من الفايروسات أو البرمجيات الخبيثة المختلفة تعتبر أحد أهم العوامل في المحافظة على البيانات من التلف، وعليه فإنه يجب اتخاذ الحيطة بتثبيت برنامج فعال في مكافحة الفايروسات مثل برنامج Symantec Norton والقيام بعمل التحديثات المستمرة له لضمان عدم وجود أي فايروس على النظام.

٥. برامج التصحيح Software Patches:

وهي مجموعة من الملفات التي يتم تحميلها من الشركة المصنعة لنظام التشغيل لسد بعض الثغرات في النظام والتي تعتبر ذات خطورة على أمن المعلومات والتي يتمكن الهاكرز Hackers عن طريقها من اختراق النظام.

الجانب العملي

المستخدمون المحليون والمجموعات

Local Users and Groups

المستخدمون المحليون

كانت عملية مشاركة الحاسب بين مستخدمين متعددين فيما مضى تعني أن بإمكان المستخدمين الآخرين المشتركين في نفس الحاسب رؤية ملفاتك الخاصة، أو تثبيت ألعاب أو برامج لا تريدها، أو تغيير إعدادات الحاسب. يمكن لميزة "حسابات المستخدمين" في Windows XP أن تخزن الإعدادات الشخصية لعدة مستخدمين مما يجعل الحاسب أكثر أماناً ومتعةً في الاستخدام.

ويمكن تعريف حساب المستخدم بأنه سجل يتكون من كافة المعلومات التي تعرّف المستخدم بالنسبة لنظام التشغيل Windows. وتتضمن معلومات الحساب اسم المستخدم وكلمة المرور المطلوبين ليقوم المستخدم بتسجيل الدخول، والمجموعة التي يتمتع المستخدم بعضويتها، والحقوق والأذونات التي يملكها المستخدم لاستخدام الحاسب وشبكة الاتصال، والوصول إلى مواردهما. ويتم إدارة حسابات المستخدمين في نظام التشغيل Windows XP Professional عن طريق "المستخدمون المحليون والمجموعات المحلية". ويمكن تعريف المستخدم المحلي بأنه على الأغلب شخص يستخدم حاسب في المنزل وليس موصولاً إلى شبكة.

أولاً: التعرف على حسابات المستخدمين المعدّة مسبقاً

أ- سجل الدخول بحساب المدير Administrator أو أي حساب عضو في مجموعة المدراء Administrators.

ب- انقر بزر الفأرة الأيمن فوق أيقونة "جهاز الكمبيوتر"، ثم اختر "إدارة" من القائمة الفرعية.

ج-ستظهر نافذة "Computer Management"، انقر فوق إشارة (+) المحاذية لأيقونة "المستخدمون المحليون والمجموعات المحلية"، كما في الشكل ٦-١.

شكل ٦-١

د-افتح مجلد "المستخدمون".

س- ما هي أسماء الحسابات المتوفرة على الحاسب لديك؟

س: هل تتشابه حسابات المستخدمين المحليين الموجودة على الجهاز لديك مع ما هو موجود في حاسب آخر؟

س: ما هي الحسابات المبنية مسبقاً في نظام التشغيل .Windows XP Prof؟

ثانياً: إنشاء حساب مستخدم محلي جديد

أ. في شجرة وحدة التحكم، انقر فوق "المستخدمون المحليون والمجموعات المحلية"، انقر فوق مجلد "المستخدمون".

ب. من شريط القوائم حدد قائمة "إجراء"، ثم "مستخدم جديد".

ج. ستظهر نافذة "مستخدم جديد"، وطبّق الإعدادات الموضحة في الشكل ٦-٢.

د. انقر فوق زر "إنشاء"، ثم انقر فوق زر "إغلاق".

س: هل أضيف المستخدم User1 إلى قائمة المستخدمين المحليين؟

شكل ٦-٢

أ- سجل خروج من الحساب الحالي، وسجل دخول باستخدام الحساب User1.

ب- سجل خروج من حساب User1، وسجل دخول بالحساب الذي بدأت به[1].

[1]: حساب المدير Administrator أو أي حساب عضو في مجموعة المدراء

ثالثاً: إدارة حسابات المستخدمين المحليين

- تعيين كلمة المرور

أ. انقر بزر الفأرة الأيمن فوق أيقونة حساب المستخدم User1، واختر أمر "تعيين كلمة مرور..."، ستظهر نافذة "تعيين كلمة مرور إلى User1"، كما في الشكل ٦-٣، ثم انقر فوق زر "متابعة".

شكل ٦-٣

ب. ستظهر نافذة "تعيين كلمة مرور إلى User1"، كما في الشكل ٦-٤، اكتب كلمة المرور الجديدة في السطر الأول، ثم أعد كتابتها في السطر الثاني، ثم انقر فوق زر "موافق".

شكل ٦-٤

ج. ستظهر رسالة تفيد نجاح تعيين كلمة المرور، كما في الشكل ٦-٥.

شكل ٦-٥

د. سجل خروج من الحساب الحالي، وسجل دخول باستخدام الحساب User1.

ه. سجل خروج من حساب User1، وسجل دخول بالحساب الذي بدأت به.

- إعادة تسمية حساب المستخدم

أ- انقر بزر الفـأرة الأيمن فـوق أيقونة حساب المستخـدم User1، واختر "إعادة تسمية" من القائمة الفرعية.

ب- اكتب الاسم الجديد للحساب في المربع الخاص بذلك وليكن User20.

ج-سجل خروج من الحساب الحالي، وسجل دخول باستخدام الحساب User20.

د-سجل خروج من حساب User20، وسجل دخول باستخدام حساب المدير.

ه- أعد تسمية حساب المستخدم User20 إلى User1.

- تعطيل حساب مستخدم موجود

أ- انقر بزر الفـأرة الأيمن فـوق أيقونة حساب المستخـدم User1، واختر "خصائص" من القائمة الفرعية.

ب- ستظهر نافذة "خصائص User1"، ومنها حدد خيار "الحساب معطّل"، انظر الشكل ٦-٦.

س: ما التغيير الذي حصل على أيقونة حساب المستخدم User1؟

سجل خروج من الحساب الحالي، وحاول تسجيل دخول باستخدام الحساب User1.

شكل٦-٦

س: ما الرسالة التي ظهرت عند محاولة تسجيل الدخول؟ وماذا تعني؟

- حذف حساب مستخدم موجود

و- انقر بزر الفـأرة الأيمن فـوق أيقونة حساب المستخـدم User1، واختر "حذف" من القائمة الفرعية.

ز- ستظهر رسالة تحذير كما في الشكل ٦-٧، انقر فوق زر "نعم".

شكل٦-٧

المجموعات المحلية

تعرف المجموعة (Group) بأنها مجموعة من حسابات المستخدمين، تستخدم لتبسيط عمليات إدارة الحسابات لأنها تسمح بتعيين الصلاحيات والأذونات والحقوق لعدد من المستخدمين في وقت واحد بدلاً من تعيينها لحساب كل مستخدم لوحده.

أما المجموعة المحلية (Local Group) فيمكن تعريفها بأنها مجموعة من حسابات المستخدمين على حاسب آلي واحد، تستخدم لتعيين الصلاحيات والأذونات على الموارد الموجودة على نفس الحاسب. ويتم إنشاء المجموعات المحلية في نظام التشغيل Windows XP Prof. في قاعدة بيانات الأمان المحلي، وبالتالي يمكن استخدام المجموعات المحلية فقط على الحاسب الذي تم إنشاؤها عليه. والمجموعات المحلية يمكن أن تتضمن حسابات المستخدمين المحليين في نفس الحاسب الذي أنشأت عليه هذه المجموعة.

يحتوي نظام التشغيل Windows XP Prof. ثلاث مستويات أمان أساسية يتم منحها للمستخدمين من خلال العضوية في مجموعات Users، أو Power Users، أو Administrators.

– مجموعة المدراء Administrators

يستطيع أعضاء هذه المجموعة تنفيذ كل المهام الإدارية على الحاسب، ويعد حساب المدير (Administrator) عضواً افتراضياً في هذه المجموعة.

– مجموعة المستخدمين الأقوياء Power Users

يستطيع أعضاء هذه المجموعة إنشاء أو تعديل حسابات المستخدمين المحليين والموارد المشتركة على الحاسب. كما تسمح الأذونات الافتراضية المخصصة لهذه المجموعة لأعضائها تعديل إعدادات الحاسب عموماً. ويتوفر لدى أعضاء المجموعة Power Users أذونات أكثر من الأذونات المتوفرة لأعضاء المجموعة Users وأقل من الأذونات المتوفرة لأعضاء مجموعة المدراء (Administrators).

– مجموعة المستخدمين Users

إن مجموعة Users هي المجموعة الأكثر أماناً، لأن الأذونات الافتراضية المخصصة لها لا تسمح للأعضاء بتعديل إعدادات نظام التشغيل أو بتعديل بيانات أخرى للمستخدم. توفر مجموعة Users بيئة أكثر أماناً يتم فيها تشغيل البرامج. فلا يمكن للمستخدمين تعديل إعدادات التسجيل على النظام، أو ملفات نظام التشغيل، أو ملفات البرامج. يمكن للمستخدمين إيقاف تشغيل محطات العمل. ويمكنهم إنشاء مجموعات محلية، ولكن يمكنهم فقط إدارة المجموعات المحلية التي قاموا بإنشائها.

- **حقوق (صلاحيات) المستخدمين والمجموعات**

لتسهيل مهمة إدارة حساب المستخدم، يجب أولاً تعيين الصلاحيات لحسابات المجموعة، بدلاً من تعيينها لحسابات المستخدم الفردية. عند تعيين الصلاحيات لحساب مجموعة، يتم تعيين هذه الصلاحيات تلقائياً للمستخدمين عندما يصبحون أعضاء في تلك المجموعة. هذه الطريقة لإدارة الصلاحيات أسهل بكثير من تعيين صلاحيات فردية لكل حساب مستخدم عندما يتم إنشاء الحساب. يوضح الجدول التالي بعض الصلاحيات التي يمكن منحها للمستخدمين.

الصلاحيـــة	الوصـــف
نسخ احتياطي للملفات والمجلدات	يسمح للمستخدم بتجاوز أذونات الملفات والمجلدات لإجراء نسخ احتياطي للنظام.
تغيير وقت النظام	يسمح للمستخدم بتعيين الوقت لساعة الحاسب الداخلية.
تحميل برامج تشغيل الأجهزة وإلغاء تحميلها	يسمح لمستخدم بتثبيت برامج تشغيل أجهزة التوصيل والتشغيل وإلغاء تثبيتها. لا يؤثر هذا الامتياز على قابلية تثبيت برامج التشغيل للأجهزة التي ليست أجهزة توصيل وتشغيل. يمكن أن يتم تثبيت برامج تشغيل الأجهزة التي ليست أجهزة توصيل وتشغيل

□

أولاً: التعرف على المجموعات المحلية المعدّة مسبقاً وصلاحياتها

أ- سجل الدخول بحساب المدير Administrator أو أي حساب عضو في مجموعة المدراء Administrators.

ب- انقر بزر الفأرة الأيمن فوق أيقونة "جهاز الكمبيوتر"، ثم اختر "إدارة" من القائمة الفرعية.

ج-ستظهر نافذة "Computer Management"، انقر فوق إشارة (+) المحاذية لأيقونة "المستخدمون المحليون والمجموعات المحلية"، كما في الشكل ٧-١.

شكل ٧-١

د-افتح مجلد "المجموعات".

س- ما هي أسماء المجموعات المحلية المضمنة على الحاسب؟ وما هي وظيفة كل منها؟ (تلميح: في فهرس التعليمات اكتب "مجموعة"، سيقوم النظام بإظهار اسم إحدى المجموعات، انقر نقراً مزدوجاً فوق عبارة "نظرة عامة" عندها ستظهر أسماء المجموعات المحلية المضمنة في نظام التشغيل).

م	اسم المجموعة	وظيفتها

ثانياً: إنشاء مجموعة محلية جديدة

أ- في شجرة وحدة التحكم، انقر فوق "المستخدمون المحليون والمجموعات المحلية"، انقر فوق مجلد "المجموعات".

ب- من شريط القوائم حدد قائمة "إجراء"، ثم "مجموعة جديدة...".

ج-ستظهر نافذة "مجموعة جديدة"، وطبّق الإعدادات الموضحة في الشكل ٧-٢.

د-انقر فوق زر "إنشاء"، ثم انقر فوق زر "إغلاق".

شكل ٧-٢

ثالثاً: إضافة حسابات مستخدمين محليين إلى مجموعة محلية

- الطريقة الأولى

أ- أنشئ ثلاثة حسابات مستخدمين محليين هي على التوالي User1، User2، User3، كما تعلمت في التجربة السابقة.

ب- انقر بزر الفأرة الأيمن فوق أيقونة حساب المستخدم User2، واختر أمر "خصائص".

ج- ستظهر نافذة "خصائص User2"، حدد منها التبويب "عضو في"، كما في الشكل ٧-٣.

شكل ٧-٣

س- إلى أي مجموعة محلية يتم ضم حساب المستخدم المحلي عند إنشائه؟

د- انقر فوق زر "إضافة..."، ستظهر نافذة "حدد مجموعات" كما في الشكل ٧-٤.

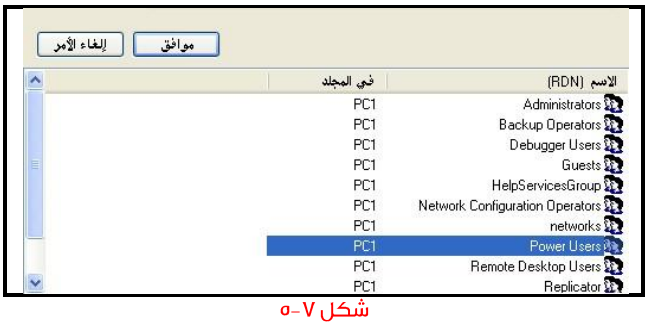
ه- انقر فوق زر "خيارات متقدمة..."، ثم انقر فوق زر "البحث الآن".

و- حدد مجموعة "Power Users"، كما في الشكل ٧-٥، ثم انقر فوق زر "موافق"، ثم "موافق"، ثم "موافق".

س- هل يمكن ضم حساب مستخدم محلي إلى أكثر من مجموعة؟

س- هل تمكن المستخدم User1 من تغيير الوقت والتاريخ؟ لماذا؟

شكل ٧-٤



شكل ٧-٥

- الطريقة الثانية

أ- انقر بزر الفأرة الأيمن فوق أيقونة مجموعة "Administrators"، واختر "إضافة إلى المجموعة...".

ب- ستظهر نافذة "خصائص Administrators"، كما في الشكل ٧-٦، ثم انقر فوق زر إضافة.

ج-ستظهر نافذة "حدد مستخدمين"، ثم انقر فوق زر "خيارات متقدمة..."، ثم انقر فوق زر "البحث الآن".

د- حدد حساب المستخدم User3، كما في الشكل ٧-٧، ثم انقر فوق زر "موافق"، ثم "موافق"، ثم "موافق".

شكل ٧-٦

شكل ٧-٧

رابعاً: تعيين حقوق المستخدمين من خلال المجموعات

أ- سجل دخول باستخدام حساب المستخدم User1، وحاول تغيير الوقت والتاريخ.

س- هل تمكن المستخدم User1 من تغيير الوقت والتاريخ؟ لماذا؟

ب- سجل خروج من حساب User1، وسجل دخول بحساب المدير أو أي حساب عضو في مجموعة المدراء.

ج- ضم حساب المستخدم User1 إلى مجموعة Networks.

د- انقر نقراً مزدوجاً فوق أيقونة "أدوات إدارية" في لوحة التحكم، ثم انقر فوق أيقونة اختصار "نهج الأمان المحلي".

ه- انقر فوق إشارة (+) المحاذية لأيقونة "النهج المحلية"، ثم انقر فوق أيقونة "تعيين حقوق المستخدم".

و- ستظهر نافذة "Local Security Settings"، كما في الشكل ٧-٨، انقر نقراً مزدوجاً فوق النهج "تغيير وقت النظام".

شكل ٧-٨

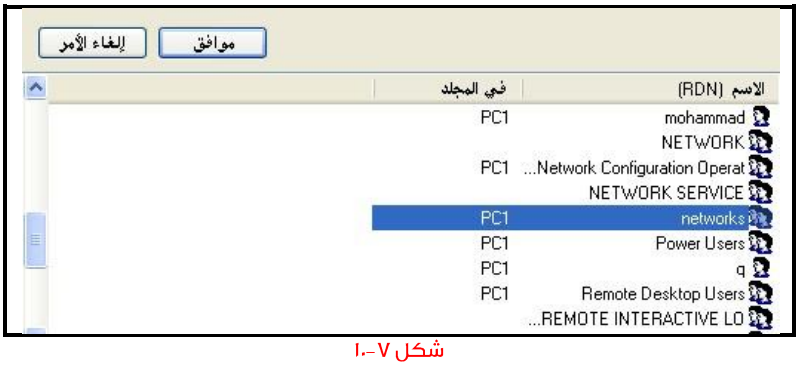
ز- ستظهر نافذة "خصائص تغيير وقت النظام"، كما في الشكل ٧-٩.

شكل ٧-٩

س- ما هي المجموعات المحلية التي يحق للحسابات الأعضاء فيها تغيير الوقت والتاريخ؟

ح-انقر فوق زر "إضافة مستخدم أو مجموعة..."، ثم انقر فوق زر "خيارات متقدمة..."، ثم انقر فوق زر "أنواع الكائنات"، ثم حدد خيار "مجموعات".

ط- انقر فوق زر "البحث الآن"، ثم حدد مجموعة "Networks"، كما في الشكل ٧-١٠، ثم انقر فوق زر "موافق"، ثم "موافق"، ثم "موافق".



شكل ٧-١٠

ي-سجل دخول باستخدام حساب المستخدم User1، وحاول تغيير الوقت والتاريخ.

س- هل تمكن المستخدم User1 من تغيير الوقت والتاريخ؟ علل إجابتك؟

خامساً: إعادة تسمية وحذف مجموعة محلية

- إعادة تسمية مجموعة محلية

أ- انقر بزر الفـأرة الأيمن فـوق أيقونة مجموعة Networks، واختر "إعادة تسمية" من القائمة الفرعية.

ب- اكتب الاسم الجديد للحساب في المربع الخاص بذلك وليكن Networks2.

س: هل يمكن تعيين حقوق المستخدم لحساب المستخدم مباشرة بدلاً من المجموعة؟

س: هل يؤدي إعادة تسمية مجموعة محلية إلى التخلص من حسابات المستخدمين الأعضاء في هذه المجموعة؟

- حذف مجموعة محلية

أ- انقر بزر الفـأرة الأيمن فـوق أيقونة مجموعة Networks2، واختر "حذف" من القائمة الفرعية.

ب- ستظهر رسالة تحذير كما في الشكل ٧-١١، انقر فوق زر "نعم".

شكل ٧-١١

س: هل يؤدي حذف مجموعة محلية إلى حذف حسابات المستخدمين الأعضاء في هذه المجموعة؟

س: باستخدام النهج "إيقاف تشغيل النظام"، كيف يمكن منع حسابات المستخدمين المحليين الأعضاء فـي مجموعة (Users) من إيقاف تشغيل النظام؟

الجانب العملي

نهج الأمان المحلي

Local Security Policy

إن نهج الأمان عبارة عن تركيبة من إعدادات الأمان التي تؤثر على جهاز الحاسب الآلي بحيث يمكنك استخدام نهج الأمان المحلي لتحرير نُهج الحساب والنُهج المحلية على الكمبيوتر المحلي. باستخدام نهج الأمان المحلي، يمكنك التحكم بمن يصل إلى الكمبيوتر الخاص بك والموارد المخوّلة للاستخدام على جهاز الحاسب الخاص بك من قبل المستخدمين. يحتوي الجدول التالي على بعض وظائف النهج المحلية:

- نهج كلمة المرور:

نهج الأمان	الوصف
الحد الأقصى لمدة كلمة المرور	تحديد المدة الزمنية (بالأيام) التي يمكن خلالها استخدام كلمة المرور قبل أن يطلب النظام من المستخدم تغييرها. يمكنك تعيين كلمات المرور لتنتهي صلاحيتها بعد انقضاء عدد من الأيام ما بين ١ و٩٩٩ يوماً، أو يمكنك تحديد عدم انتهاء صلاحية كلمات المرور أبداً بتعيين عدد الأيام إلى ٠. عدد الأيام الافتراضي لصلاحية كلمة المرور: ٤٢.
الحد الأدنى لمدة كلمة المرور	تحديد المدة الزمنية (بالأيام) التي يجب أن تُستخدم خلالها كلمة المرور قبل أن يتمكن المستخدم من تغييرها. يمكنك تعيين قيمة ما بين ١ و ٩٩٩ يوم، أو يمكنك السماح بالتغييرات مباشرة وذلك بتعيين عدد الأيام إلى ٠.
الحد الأدنى لطول كلمة المرور	تحديد أقل عدد من الأحرف يمكن أن تتضمنها كلمة مرور المستخدم. يمكنك تعيين قيمة ما بين ١ و ١٤ حرف، أو يمكنك تأسيس حالة عدم طلب كلمة مرور بإعداد عدد الأحرف إلى ٠.

- نهج تأمين الحسابات:

نهج الأمان	الوصف
حد تأمين الحساب	تحديد عدد محاولات تسجيل الدخول الفاشلة التي تسببت بتأمين حساب المستخدم. لا يمكن لحساب تم تأمينه أن يُستخدم حتى يتم إعادة تعيينه من قبل المسؤول أو حتى تنتهي مدة صلاحية فترة التأمين له. يمكنك تعيين قيمة ما بين ١ و ٩٩٩ لمحاولات تسجيل الدخول الفاشلة، أو يمكنك تحديد ألاّ يتم تأمين الحساب أبداً بإعداد القيمة إلى ٠.
تأمين الحساب لمدة	تحديد عدد الدقائق التي يبقى فيها الحساب مؤمناً قبل أن يصبح غير مؤمن تلقائياً. إن المجال المتوفر هو من ١ إلى ٩٩،٩٩٩ دقيقة. يمكنك تحديد أن يكون الحساب مؤمناً حتى يقوم المسؤول بإلغاء تأمينه بشكل صريح بإعداد القيمة إلى ٠.
إعادة تعيين عداد تأمين الحساب بعد	تحديد عدد الدقائق التي يجب انقضاؤها بعد محاولة تسجيل الدخول الفاشلة، قبل إعادة تعيين حساب محاولات تسجيل الدخول الفاشلة إلى ٠ محاولة تسجيل دخول فاشلة. إن المجال المتوفر هو من ١ إلى ٩٩،٩٩٩ دقيقة.

- نهج خيارات الأمان:

نهج الأمان	الوصـــف
عدم المطالبة بالضغط على CTRL+ALT+DEL	تحديـد وجـوب ضـغط CTRL+ALT+DEL ليـتمكن المستخدم من تسجيل الدخول. إذا تم تمكين هذا النهج على الكمبيوتر، فإن المستخدم غير مطالب بضغط CTRL+ALT+DEL لتسجيل الدخول. إن عدم وجوب ضغط CTRL+ALT+DEL يترك المستخدمين عرضةً لعمليات الاقتحام التي تحاول التصدي لكلمات مرور المستخدم. إن طلب ضغط CTRL+ALT+DEL قبل تسجيل دخول المستخدمين يؤكد أن المستخدمين يتصلون بواسطة مسار موثوق عند إدخالهم لكلمات المرور الخاصة بهم. في حال تعطيل هذا النهج، تتم مطالبة أي مستخدم بضغط CTRL+ALT+DEL لتسجيل الدخول إلى Windows.
عنوان الرسالة للمستخدمين الذين يحاولون تسجيل الدخول	السماح لتحديدات العنوان بالظهور في شريط العنوان لإطار يتضمن تسجيل دخول تبادلي: نص الرسالة للمستخدمين الذين يحاولون تسجيل الدخول.
نص الرسالة للمستخدمين الذين يحاولون تسجيل الدخول	تحديد الرسالة النصية التي يتم عرضها للمستخدمين عند تسجيل الدخول. يُستخدم هذا النص غالباً لأسبابٍ قانونية، على سبيل المثال، لتحذير المستخدمين حول المبالغة في سوء استخدام معلومات الشركة أو لتحذيرهم من أن إجراءاتهم قد يتم تدوينها.
عدم عرض اسم المستخدم الأخير	تحديد وجوب عرض اسم المستخدم الأخير الذي تم تسجيل دخوله إلى الكمبيوتر في شاشة تسجيل دخول Windows.إذا تم تمكين هذا النهج، لا يتم عرض اسم المستخدم الأخير الذي تم تسجيل دخوله بنجاح في مربع الحوار تسجيل الدخول إلى Windows.

- **أولاً: دراسة نهج كلمة المرور**

ه- سجل الدخول بحساب المدير Administrator أو أي حساب عضو في مجموعة المدراء Administrators.

و- انقر نقرا مزدوجاً فوق أيقونة "أدوات إدارية" من نافذة لوحة التحكم.

ز- انقر نقرا مزدوجاً فوق أيقونة "نهج الأمان المحلي".

م- ستظهر نافذة "Local Security Settings"، أنقر فوق إشارة (+) المحاذية لأيقونة "نهج الحساب"، ثم انقر فوق أيقونة "نهج كلمة المرور".

ط- عند الجزء الأيسر من النافذة أنقر بزر الفأرة الأيمن فوق "الحد الأقصى لمدة كلمة المرور"، ثم اختر "خصائص من القائمة الفرعية.

ي- ستظهر نافذة "خصائص الحد الأقصى لمدة كلمة المرور"، حدد يومين كما في الشكل (١٢-١)، ثم اضغط فوق زر "موافق".

شكل ١٢-١

ك- أنقر بزر الفأرة الأيمن فوق "الحد الأدنى لمدة كلمة المرور"، ثم اختر "خصائص من القائمة الفرعية.

ل- ستظهر نافذة "خصائص الحد الأقصى لمدة كلمة المرور"، حدد السماح بتغير كلمة المرور بعد يومين كما في الشكل (١٢-٢)، ثم اضغط فوق زر "موافق".

شكل ١٢-٢

م- أنقر بزر الفأرة الأيمن فوق "الحد الأدنى لطول كلمة المرور"، ثم اختر "خصائص من القائمة الفرعية.

ن- ستظهر نافذة "خصائص الحد الأدنى لطول كلمة المرور "، ثم حدد "عدد الكلمات غير مطلوبة" بستة (٦) أحرف كما في الشكل (١٢-٣) ثم اضغط فوق الزر "موافق".

شكل ١٢-٣

س- أنشئ مستخدم جديد باسم (LSS) وحدد له كلمة مرور (Link)، هل استطعت إنشاء المستخدم (LSS)؟علل؟

س- عدل على السؤال السابق بحيث تحدد كلمة المرور (Fast Link)، هل استطعت إنشاء المستخدم (LSS)؟علل؟

- ثانياً: دراسة نهج تأمين الحسابات

أ- سجل الدخول بحساب المدير Administrator أو أي حساب عضو في مجموعة المدراء Administrators.

ب- انقر نقرا مزدوجاً فوق أيقونة "أدوات إدارية" من نافذة لوحة التحكم.

ج-انقر نقرا مزدوجاً فوق أيقونة "نهج الأمان المحلي".

د-ستظهر نافذة "Local Security Settings"، أنقر فوق إشارة (+) المحاذية لأيقونة "نهج الحساب"، ثم انقر فوق أيقونة "نهج تأمين الحسابات".

ه-عند الجزء الأيسر من النافذة أنقر بزر الفأرة الأيمن فوق "حد تأمين الحساب"، ثم اختر "خصائص من القائمة الفرعية.

و-ستظهر نافذة "خصائص حد تأمين الحساب"، حدد محاولات تسجيل الدخول غير صالحة بمرتين، كما في الشكل (١٢-٤)، ثم اضغط فوق زر "موافق".

شكل ١٢-٤

س- حاول أن تسجل دخول بحساب المستخدم (LSS) باستخدام كلمة مرور خاطئة مرتين متتاليتين؟ ماذا تلاحظ بعد المرة الثانية؟

س- سجل دخول بحساب المستخدم Administrator أو أي حساب عضو في مجموعة Administrators، ثم استعرض خصائص حساب المستخدم (LSS) ماذا تلاحظ؟

س- أنقر بزر الفأرة الأيمن فوق "تأمين الحساب لمدة"، ثم اختر "خصائص من القائمة الفرعية.

ع- ستظهر نافذة "خصائص تأمين الحساب لمدة"، ثم حدد مدة تأمين الحساب لدقيقة واحدة كما في الشكل ١٢-٥، ثم اضغط فوق زر "موافق".

شكل ١٢-٥

س- حاول أن تسجل دخول بحساب المستخدم (LSS) باستخدام كلمة مرور خاطئة مرتين متتاليتين؟ وانتظر مدة دقيقة واحدة ثم حاول تسجيل الدخول مرة أخرى باستخدام كلمة المرور الصحيحة، هل استطعت تسجيل الدخول هذه المرة؟ علل؟

س- أنقر بزر الفأرة الأيمن فوق نهج "إعادة تأمين عداد تأمين الحساب بعد" ماذا تلاحظ؟ هل توجد علاقة بين نهج "تأمين الحساب لمدة" و نهج" إعادة تأمين عداد تأمين الحساب بعد"؟؟

- ## ثالثاً: دراسة خيارات الأمان

أ- سجل الدخول بحساب المدير Administrator أو أي حساب عضو في مجموعة المدراء Administrators.

ب- انقر نقرا مزدوجاً فوق أيقونة "أدوات إدارية" من نافذة لوحة التحكم.

ج-انقر نقرا مزدوجاً فوق أيقونة "نهج الأمان المحلي".

د-ستظهر نافذة "Local Security Settings"، أنقر فوق إشارة (+) المحاذية لأيقونة "النهج المحلية"، ثم انقر فوق أيقونة "خيارات الأمان".

ه-عند الجزء الأيسر من النافذة أنقر بزر الفأرة الأيمن فوق " Interactive Logon: Do not require CTRL+ALT+DEL"، ثم اختر "خصائص من القائمة الفرعية.

و-ستظهر نافذة "خصائص Interactive Logon: Do not require CTRL+ALT+DEL "، أنقر فوق الخيار "تمكين"، كما في الشكل (١٢-٦) ثم اضغط فوق زر "موافق".

شكل ١٢-٦

س- سجل خروج من حساب المستخدم الذي تعمل به حالياً وحاول تسجيل الدخول مرة أخرى ماذا تلاحظ؟

ز- أنقر بزر الفأرة الأيمن فوق " Interactive Logon: Message Title for users attempting to log on"، ثم اختر "خصائص من القائمة الفرعية.

ح-ستظهر نافذة خصائص "Interactive Logon: Message Title for users attempting to log on "، أكتب عنوان النافذة كما في الشكل (١٢-٧). ثم انقر فوق زر "موافق".

شكل ١٢-٧

ط- أنقـر بـزر الفـأرة الأيمـن فـوق " Interactive Logon: Message text for users attempting to log on"، ثم اختر "خصائص من القائمة الفرعية.

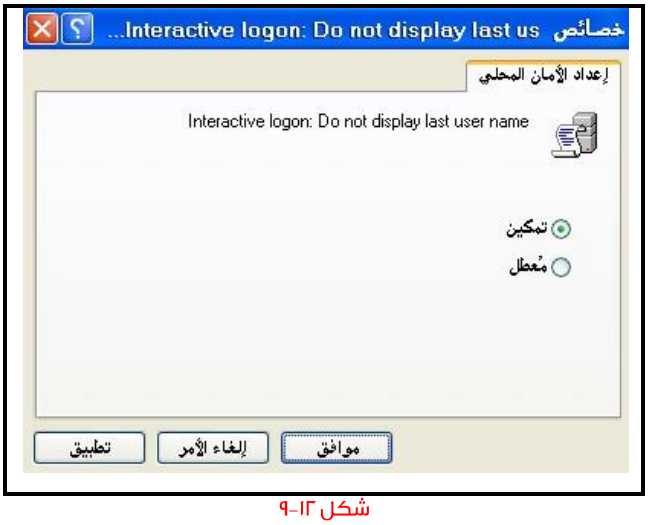
ي- ستظهر نافذة " خصائص Interactive Logon: Message text for users attempting to log on "، أكتب عنوان النافذة كما في الشكل (١٢-٨)، ثم اضغط فوق زر "موافق".

شكل ١٢-٨

س- سجل خروج من حساب المستخدم الذي تعمل به حالياً وحاول تسجيل الدخول مرة أخرى ماذا تلاحظ؟

أنقـر بـزر الفـأرة الأيمـن فـوق "Interactive Logon: Do not Display last user name"، ثم اختر "خصائص من القائمة الفرعية.

ك- ستظهر نافذة "خصائص Interactive Logon: Do not Display last user name "، أنقر فوق الخيار "تمكين"، كما في الشكل (١٢-٩)، ثم انقر فوق زر "موافق".



شكل ١٢-٩

س- سجل خروج من حساب المستخدم الذي تعمل به حالياً وحاول تسجيل الدخول مرة أخرى ماذا تلاحظ؟

الجانب العملي

الحصص النسبية

Quota

توفر شركة مايكروسوفت أكثر من نظام ملفات للعمل مع أنظمة التشغيل المختلفة الخاصة بها. ويعرف يعرف نظام الملفات بأنه البنية المستخدمة في تسمية الملفات، وتخزينها، وتنظيمها. ومن الأمثلة على أنظمة نظام الملفات NTFS (وهو نظام ملفات متقدّم يوفر الأداء، والأمان، والثقة، وميزات متقدمة لا يمكن العثور عليها في الإصدارات القديمة من أنظمة الملفات الأخرى)، ونظام ملفات FAT (وهو نظام ملفات مستخدم من قبل MS-DOS وبرامج التشغيل الأخرى المستندة إلى Windows لتنظيم وإدارة الملفات)، ونظام ملفات FAT32 (وهو مشتق من نظام ملفات "جدول تخصيص الملفات FAT). والجدول التالي يوضح الفروق الشاسعة بين النظامين.

وجه المقارنة	نظام ملفات FAT	نظام ملفات NTFS
أنظمة التشغيل التي يدعمها	DOS, Windows 95, 98, Me, XP, Windows 2000.	Windows 2000, XP.
حجم القرص المنطقي	Windows 9x= 2GB Windows NT= 4GB	16 EB (1EB=1073741824 GB)
نسخة احتياطية عن جدول التوطين	لا توجد نسخة احتياطية عن جدول توطين الملفات FAT	توجد نسخة احتياطية عن جدول الملفات السيد MFT
الأمن وسرية الملفات والمجلدات	لا أمن ولا سرية	أمن وسرية على مستوى الملفات والمجلدات
ضغط الملفات	لا يمكن الضغط إلا باستخدام برامج خاصة	يمكن ضغط البيانات مباشرة دون الحاجة لبرامج خاصة

تتحكم الحصص النسبية للقرص باستخدام مساحة أقراص وحدات تخزين NTFS[1]، بحيث يتمكن مدير النظام من منع الاستخدام الزائد لمساحة القرص وتسجيل حدث عند تجاوز المستخدم حداً معيناً من مساحة قرص، هذا الحد هو الكمية من مساحة القرص المسموم للمستخدم باستخدامها. ويسمح بتسجيل حدث عند تجاوز المستخدم مستوى تحذير معيّن لمساحة القرص، وتلك هي النقطة التي يكون فيها المستخدم على وشك استنفاد حد حصته النسبية.

عند تمكين الحصص النسبية للقرص، يمكن تعيين قيمتين: حد الحصة النسبية للقرص ومستوى التحذير للحصة النسبية للقرص. على سبيل المثال، يمكنك تعيين حد الحصة النسبية من القرص لمستخدم إلى ٥٠٠ ميغا بايت، ومستوى التحذير للحصة النسبية من القرص إلى ٤٥٠ ميغا بايت. في هذه الحالة، يمكن للمستخدم تخزين ملفات بحجم ٥٠٠ ميغا بايت على الأكثر على وحدة التخزين. إذا خزّن المستخدم أكثر من ٤٥٠ ميغا بايت من

[1] : نظام ملفات لتقنية الحديثة New Technology File System.

الملفات على وحدة التخزين، يمكنك تكوين نظام الحصص النسبية للقرص ليسجل حدث نظام. يجب أن تكون عضواً في المجموعة Administrators لإدارة الحصص النسبية على وحدة تخزين، ويجب أن يكون نوع نظام الملفات للقرص المستخدم في إنشاء الحصص النسبية لحسابات المستخدمين المحلية NTFS، مع ملاحظة أن الحصص النسبية لا تطبق على أي حساب عضو في مجموعة المدراء.

إنشاء حصص نسبية لحسابات المستخدمين المحليين

أ- سجل الدخول بحساب المدير Administrator أو أي حساب عضو في مجموعة المدراء Administrators.

ب- انقر نقراً مزدوجاً فوق أيقونة "جهاز الكمبيوتر"، ثم انقر بزر الفأرة الأيمن فوق أيقونة "القرص المحلي C:" مثلاً.

ج-لاحظ كلاً من نوع نظام الملفات لهذا القرص (تأكد أن يكون NTFS)، وسعة القرص، كما في الشكل ٩-١.

شكل ٩-١

د-أنقر فوق تبويب "الحصة النسبية".

ه-ستظهر نافذة تبويب الحصة النسبية، حدد الخيارات كما هي موضحة في الشكل ٩-٢ تماماً، ثم انقر فوق زر "إدخالات الحصة النسبية".

شكل ٩-٢

و- ستظهر نافذة "إدخالات الحصة النسبية للقرص المحلي :C"، ثم من شريط الأوامر أنقر فوق الأمر "الحصة النسبية"، ثم اختر "إدخال جديد للحصة النسبية..." من القائمة الفرعية كما في الشكل ٩-٣.

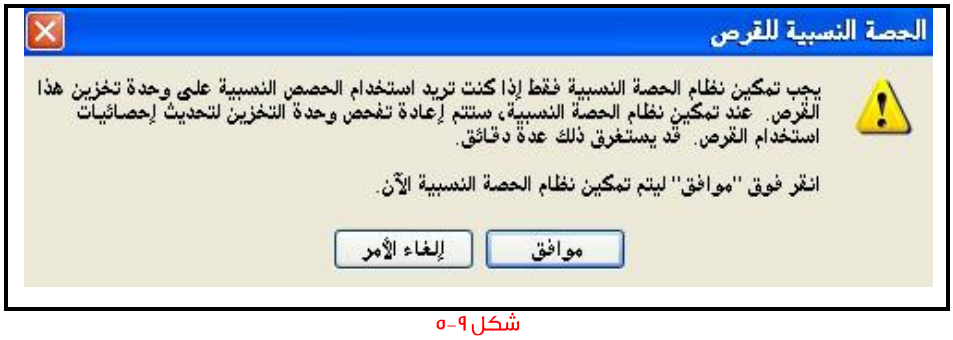
شكل ٩-٣

ز- ستظهر نافذة "إضافة إدخال جديد للحصة النسبية"، أنقر فوق الخيار "الحد من مساحة القرص إلى"، وأعط القيم كما في الشكل ٨-٤، ثم أنقر فوق زر "موافق".

شكل ٩-٤

م-ستظهر نافذة "إدخالات الحصة النسبية للقرص المحلي :C" مرة أخرى، أغلق هذه النافذة لتعود إلى نافذة تبويب " الحصة النسبية" ثم أنقر فوق زر "موافق".

ط- ستظهر نافذة تأكيد تفعيل خدمة الحصة النسبية على القرص المحلي :C كما في الشكل ٩-٥، أنقر فوق زر "موافق".



شكل ٩-٥

ي- سجل خروج من حساب المستخدم الذي أنشأت من خلاله الحصة النسبية لحساب المستخدم User1.

ك- سجل دخول بحساب المستخدم User1، ثم استعرض خصائص القرص المحلي :C (الذي أنشأت عليه الحصة النسبية)، لاحظ سعة القرص. كما في الشكل ٩-٦.

شكل ٩-٦

س- لماذا ظهر محرك الأقراص :C وكأنه فارغ تماماً، علماً بأنه يحتوي على العديد من الملفات والمجلدات؟

حاول نسخ مجلد حجمه أكبر من سعـة محرك الأقراصC، ولاحظ رسالة الخطأ كما في الشكل ٩-٧.

شكل ٩-٧

س١- غير المجموعة التي ينتمي إليها حساب المستخدم User1 وضعه ضمن مجموعة المدراء ؟ ثم استعرض خصائص القرص المحلي :C، ماذا تلاحظ؟

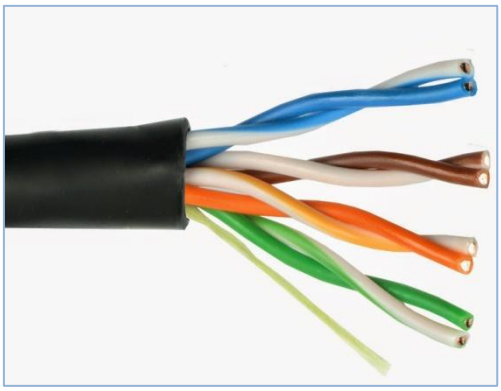
س٢- هل يمكن تطبيق الحصص النسبية على محرك أقراص يعمل بنظام ملفات FAT؟ إذا كان الجواب بلا، كيف يمكن تحويل نظام الملفات من Fat إلى NTFS؟

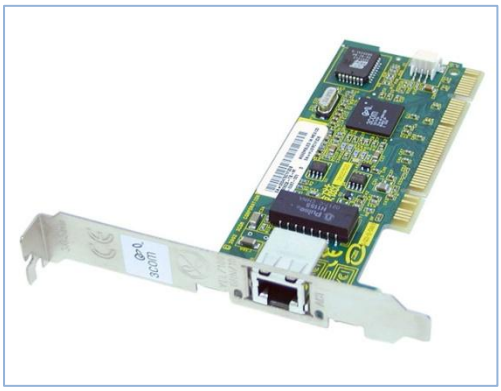
س٣- عدل مساحة الحصة النسبية المخصصة لحساب المستخدم User1 لتكون ٢٠ ميجابايت، ومستوى التحذير عند ١٩ ميجابايت.

الجانب العملي

بطاقة الشبكة وكابلات UTP

NIC and UTP Cables





بطاقة الربط مع الشبكة (NIC) أو محول الشبكة عبارة عن بطاقة تستخدم لربط محطة العمل مع خادم الملفات أو محطات العمل الأخرى. وتقوم بطاقة الربط مع الشبكة على تحويل الإشارات الرقمية المتوازية الصادرة من الحاسب إلى إشارة تماثلية ونقلها إلى وسط ناقل (سلكي أو لاسلكي). كما تعمل بطاقة مواجهة الشبكة على تحويل الإشارات التماثلية الواصلة عبر الوسط الناقل (سلكي أو لاسلكي) إلى مجموعة من الإشارات الرقمية المتوازية في الجهاز المستقبل. وبهذا تقوم بطاقة الشبكة بتنظيم حركة مرور البيانات من وإلى الوسط الناقل.

تتطلب بطاقة ربط الشبكة نوعاً معيناً من الكابلات؛ وتعرف الكابلات المستخدمة مع بطاقات Ethernet لإنشاء الشبكة النجمية بالكابلات المجدولة، وغالباً ما تستخدم الكابلات المجدولة غير المغلفة.

لربط حاسبين في شبكة محلية سلكية فيجب تجهيز كابل UTP نوع Cross Over Cable، وتركيب الطرف الأول من الكابل في بطاقة الشبكة للجهاز الأول والطرف الثاني من الكابل في بطاقة الشبكة للجهاز الثاني.

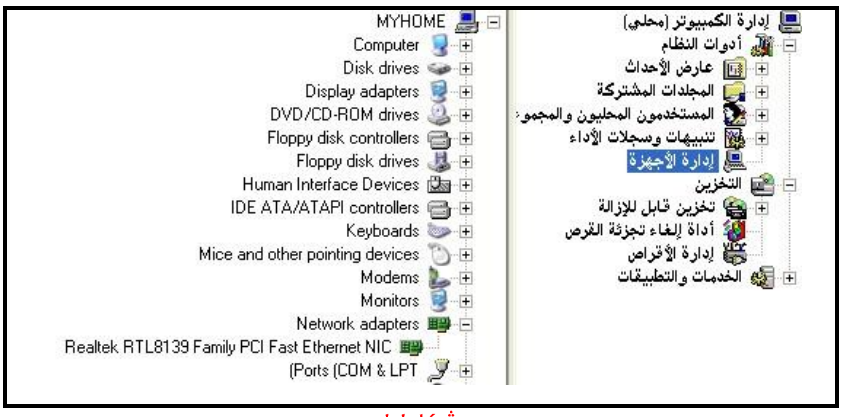
يعد استخدام كابلات UTP هو الأكثر استخداماً في إنشاء وتركيب الشبكات النجميـة المكونة من أكثر من حاسبين. ونحتاج في هذه الحالـة إلى استخدام جهاز اتصال لربط الأجهزة ببعضها بعض، وتعرف كابلات UTP المستخدمـة في هذه الحالة باسم Drop Cables.

أولاً: التعرف على نوع بطاقة الشبكة

أ- شغل جهاز الحاسب، وسجل دخول باستخدام حساب المدير[1]، أو أي حساب عضو في مجموعة المدراء.

ب- انقر بزر الفارة الأيمن فوق أيقونة "جهـاز الكمبيوتر"، ثم اختـر "إدارة" من القائمة الفرعية.

ج-ستظهر نافذة شكل ١-١، حدد خيار "إدارة الأجهزة"، ثم انقر بالفأرة فوق إشارة (+) المحاذية لأيقونة "Network Adapter".



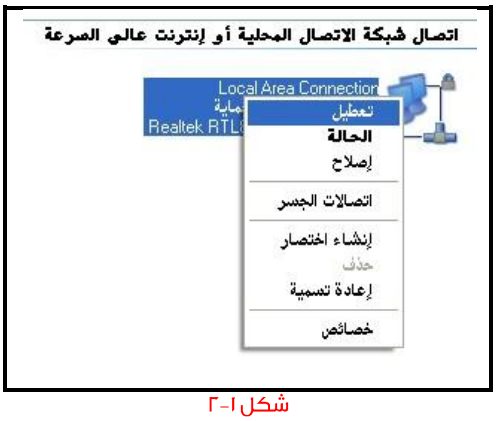
شكل ١-١

س: ما هو نوع بطاقة مواجهة الشبكة المثبتة على الحاسب لديك؟

ثانياً: تعطيل/تمكين بطاقة الشبكة

أ- انقر بزر الفارة الأيمن فوق أيقونة "مواضع شبكة الاتصال"، ثم اختـر "خصائص" من القائمة الفرعية.

ب- اضغط بزر الفأرة الأيمن فوق أيقونة "Local Area Connection" من القائمة الفرعية اختر الأمر "تعطيل"، انظر شكل ١-٢.



شكل ١-٢

[1] حساب المدير Administrator: هو حساب مستخدم محلي يمتلك أعلى صلاحيات إدارية على الحاسب.

ج-اضغط بزر الفأرة الأيمن فوق أيقونة "Local Area Connection" مرة أخرى، ومن القائمة الفرعية اختر الأمر "تمكين"، انظر شكل١-٣.

شكل١-٣

س: ما هي التغيرات التي حدثت على أيقونة "Local Area Connection" في كل من ب و ج؟

ثالثاً: إظهار رمز الاتصال على شريط المهام

أ- انقر بزر الفارة الأيمن فوق أيقونة "مواضع شبكة الاتصال"، ثم اختر خصائص من القائمة الفرعية.

ب- انقر بزر الفارة الأيمن فوق أيقونة (Local Area Connection)، ثم اختر خصائص من القائمة الفرعية.

ج- فعل الخيار "إظهار الرمز في منطقة الإعلام عند الاتصال"، عندها ستظهر الرسالة التالية في شريط الإعلام، انظر شكل ١-٤.

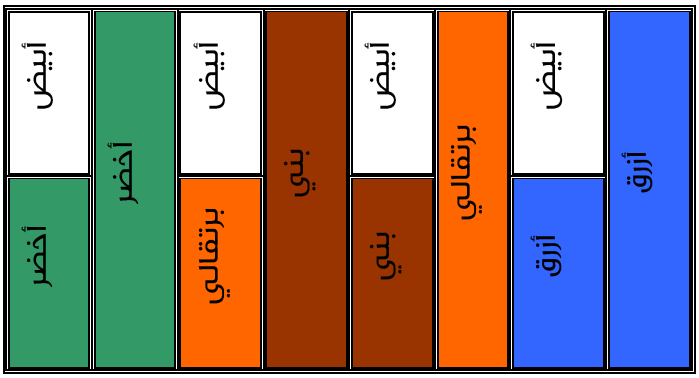
شكل ١-٤

رابعاً: تركيب وفحص كابل نوع Cross Over Cable

أ- اقطع سلكاً بطول مترين من لفـة كابلات UTP المتوفرة لديك.

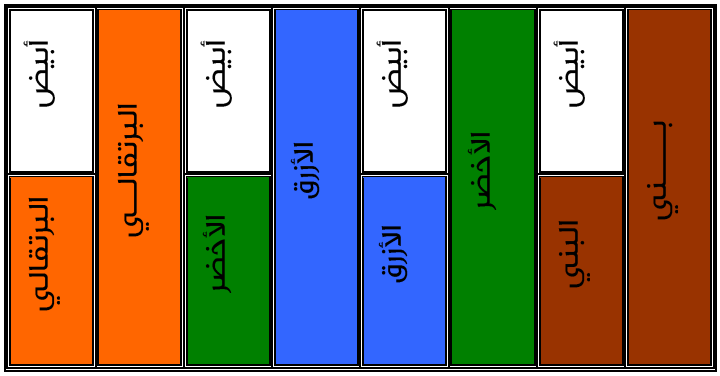
ب- انزع –باستخدام المشرط حوالي ٥،١ سم- من الغطاء الخارجي الواقي للأسلاك من كلا الطرفين.

ج- رتب الأسـلاك – في الطرف الأول- وفـق جدول ١-١، وتأكد من الترتيب بكل دقة.



جدول ١-١

د- رتب الأسلاك – في الطرف الثاني- من الكابل وفق جدول ١-٢، وتأكد من الترتيب بكل دقة.



جدول ١-٢

ه- ركب وصلة RJ-45 إلى الطرف الأول – سيقوم المدرس بإرشادك إلى الطريقة- ثم استخدم أداة الـربط (Crimping Tool) لتثبيت الوصلة إلى الكابل.

و- أعد تطبيق الخطوة السابقة على الطرف الثاني من الكابل.

ز- استخدم أداة الفحص للتأكد من سلامة توصيل الكابل.

خامساً: تركيب وفحص كابل نوع Drop Cable

أ- اقطع سلكاً بطول خمسة أمتار من لفـة كابلات UTP المتوفرة لديك.

ب- انزع –باستخدام المشرط حوالي ٥،١ سم- من الغطاء الخارجي الواقي للأسلاك من كلا الطرفين.

ج- رتب الأسـلاك – في الطرفين- وفـق جدول ١-٣، وتأكد من الترتيب بكل دقة.

أبيض	برتقالي	أبيض	أزرق	أبيض	أخضر	أبيض	بني
برتقالي	برتقالي	أخضر	أزرق	أزرق	أخضر	بني	بني

جدول ١-٣

د- ركب وصلة RJ-45 إلى الطرفين، ثم استخدم أداة الربط (Crimping Tool) لتثبيت الوصلة إلى الكابل.

٥- استخدم أداة الفحص للتأكد من سلامة توصيل الكابل.

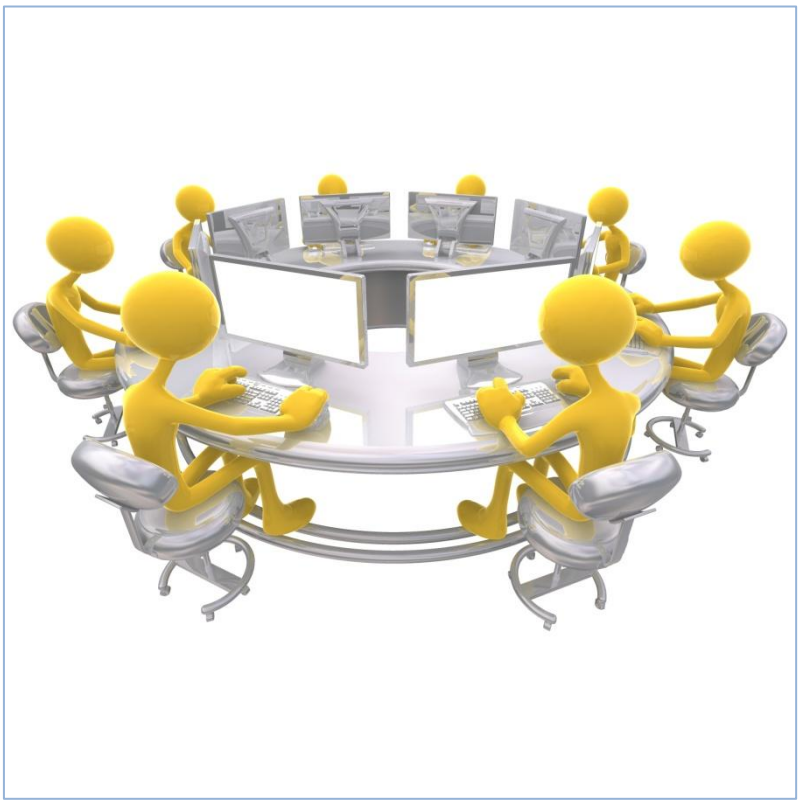
١- بفرض أن سرعة أحدى بطاقات مواجهة الشبكة هي ١٠٠ميجابت/ثانية، وسرعة بطاقة مواجهة الشبكة الثانية هي ١٠ ميجابت / ثانية، ما هي سرعة نقل البيانات بين الجهازين؟ ولماذا؟

٢- هل يمكن بناء شبكة بين جهازين كل منهما يعمل بنظام تشغيل مختلف؟

الجانب العملي

بناء شبكة مجموعة عمل

Building a Workgroup



كل جهاز حاسب يتصل بشبكة لابد أن يمتلك عنواناً خاصاً به يتكون من ٣٢ خانة من الأعداد الثنائية هذا العنوان يطلق عليه اسم "عنوان IP". وهذا العنوان على معلومتين اثنتين، أحداهما يطلق عليها اسم معرف الشبكة Net ID والأخرى يطلق عليها اسم معرف الجهاز Client ID. والذي يحدد Net ID من Host ID في كل رقم هو قناع الشبكة الفرعية Subnet Mask، وهناك ثلاث فئات من أقنعة الشبكة الفرعية وهي Class A؛ وفيها يكون رقم قناع الشبكة الفرعية (255.0.0.0)، و Class B؛ وفيها يكون رقم قناع الشبكة الفرعية (255.255.0.0)، أما Class C؛ فإن قناع الشبكة الفرعية يكون (255.255.255.0).

والسؤال هو كيف يمكن استخلاص معرف الشبكة Net ID ومعرف الجهاز Host ID من أي عنوان IP؟. توضح الأمثلة القادمة الطريقة.

مثال ١:

يمتلك جهاز حاسب معلومات عنوان IP التالي:

عنوان IP	100.20.50.90
قناع الشبكة	255. 0. 0. 0

هنا يقابل كل رقم من عنوان IP الرقم 255 الموجود في قناع الشبكة، هو معرف الشبكة Net ID، وباقي الأرقام هي معرف الجهاز Host ID، لاحظ بأن قناع الشبكة هو من الفئة Class A، إذاً معرف الشبكة Net ID حسب هذا المثال هو (100) ومعرف الجهاز Host ID هو (20.50.90)، وهذا يعني أن جميع الأجهزة في الشبكة الواحدة، يجب أن يبدأ أول رقم من أرقام IP فيها بالرقم (100) وباقي الأرقام متاحة يمكن فيها وضع أي رقم وبشرط أن لا يملك جهازين عنوان IP ذاته.

مثال ٢:

يمتلك جهاز حاسب معلومات عنوان IP التالي:

عنوان IP	130. 20. 50. 90
قناع الشبكة	255. 255. 0 . 0

هنا يقابل كل رقم من عنوان IP الرقم 255 الموجود في قناع الشبكة، هو معرف الشبكة Net ID، وباقي الأرقام هي معرف الجهاز Host ID، لاحظ بأن قناع الشبكة هو من Class B، إذاً معرف الشبكة Net ID حسب هذا المثال هو (130.20) ومعرف الجهاز Host ID هو (50.90)، هذا يعني أن جميع عناوين IP التي تمتلكها الأجهزة في الشبكة الواحدة يجب أن تبدأ بالرقمين (130.20) وباقي الأرقام متاحة الأرقام متاحة.

مثـال ٣:

يمتلك جهاز حاسب معلومات عنوان IP التالي:

عنوان IP	200. 60. 30. 50
قناع الشبكـة	255. 255.255. 0

هنا يقابل كل رقم من عنوان IP الرقم 255 الموجود فـي قنـاع الشبكـة، هـو معـرف الشبكـة Net ID، وبـاقي الأرقـام هي معرف الجهـاز Host ID، إذاً معـرف الشـبكة Net ID حسـب هـذا المثـال هـو (200.60.30) ومعـرف الجهـاز Host ID هو (50)، لاحظ أن قناع الشبكة هـو من Class C، وهذا يعني أن جميع عناوين IP التـي تمتلكهـا الأجهـزة في الشبكـة الواحـدة يجب أن تبـدأ بالأرقام (200.60.30) وباقي الأرقام متاحـة الأرقام متاحـة.

في الأمثلة السابقة، لكل عنوان IP هناك عنوان قناع الشبكة مرافق له، فكان من السهل اسـتخراج معـرف الجهاز ومعرف الشبكة، ولكن ماذا لو أعطيت رقم IP مـن دون أن تعطـى عنـوان قنـاع الشـبكة؟، هـل تسـتطيع استخراج معرف الشبكة Net ID ومعرف الجهاز Host ID؟ الجواب نعم. فبالنظر إلى أول خانة من خانات عنـوان IP، إذا كانت القيمة تتراوح بين 126-1 فهذا يعني أن عنوان IP من الفئـة A، أما إذا كانـت القيمة تتراوح بين 191-128 فهذا يعني بأن عنوان IP من الفئة B، وفي حال كانـت القيمة تتراوح بين 223-192 فهذا يعني بأن عنـوان IP مـن الفئة C، انظر الجدول التالي.

عنوان IP	أول خانة من IP	المجال	الفئة
50. 66. 40. 11	50	1 – 126	Class A
185. 10. 11. 12	185	128 - 191	Class B
200. 1. 2. 3	200	192 -223	Class C

بطاقة الربط مع الشبكة (NIC) أو محول الشبكة عبارة عن بطاقة تستخدم لربط محطة العمل مع خادم الملفات أو محطات العمل الأخرى. وتقوم بطاقة الربط مع الشبكة على تحويل الإشارات الرقمية المتوازية الصادرة من الحاسب إلى إشارة تماثلية ونقلها إلى وسط ناقل (سلكي أو لاسلكي). كما تعمل بطاقة مواجهة الشبكة على تحويل الإشارات التماثلية الواصلة عبر الوسط الناقل (سلكي أو لاسلكي) إلى مجموعة من الإشارات الرقمية المتوازية في الجهاز المستقبل. وبهذا تقوم بطاقة الشبكة بتنظيم حركة مرور البيانات من وإلى الوسط الناقل.

تتطلب بطاقة ربط الشبكة نوعاً معيناً من الكابلات؛ وتعرف الكابلات المستخدمة مع بطاقات Ethernet لإنشاء الشبكة النجمية بالكابلات المجدولة، وغالباً ما تستخدم الكابلات المجدولة غير المغلفة.

لربط حاسبين في شبكة محلية سلكية فيجب تجهيز كابل UTP نوع Cross Over Cable، وتركيب الطرف الأول من الكابل في بطاقة الشبكة للجهاز الأول والطرف الثاني من الكابل في بطاقة الشبكة للجهاز الثاني.

يعد استخدام كابلات UTP هو الأكثر استخداماً في إنشاء وتركيب الشبكات النجمية المكونة من أكثر من حاسبين. ونحتاج في هذه الحالة إلى استخدام جهاز اتصال لربط الأجهزة ببعضها بعض، وتعرف كابلات UTP المستخدمة في هذه الحالة باسم Drop Cables أو Straight Through.

أولاً: إنشاء الاتصال الفيزيائي بين الجهازين

د- صل الطرف الأول من كابل UTP نوع Cross Over في بطاقة مواجهة الشبكة (NIC) للجهاز الأول، والطرف الثاني من الكابل في بطاقة مواجهة الشبكة (NIC) للجهاز الثاني.

o- شغل جهاز الحاسب، وسجل دخول باستخدام حساب المدير، أو أي حساب عضو في مجموعة المدراء.

و- لاحظ الإضاءة الموجودة إلى جانب منفذ RJ-45 في بطاقة الشبكة لكلا الجهازين.

ز- أظهر رمز الاتصال في منطقة الإعلام.

س- كم عدد الإضاءات الموجودة في بطاقة الشبكة وما هي وظيفة كل منها؟

س- من خلال الإضاءات الموجودة في بطاقة الشبكة، كيف يمكن معرفة ما إذا كان الاتصال قائماً أم لا؟

ثانياً: بناء شبكة بين جهازين من نوع مجموعة عمل وعناوين IP التلقائية

أ- انقر بزر الفارة الأيمن فوق أيقونة "مواضع شبكة الاتصال"، ومن القائمة الفرعية اختر "خصائص".

ب- انقر بزر الفارة الأيمن فوق أيقونة "Local Area Connection"، ومن القائمة الفرعية اختر "خصائص".

ج- تأكد من تحديد الخيارات في مربع الحوار "خصائص Local Area Connection" بحيث تتطابق مع الإعدادات الموضحة في شكل ٢-١.

د- الآن، حدد بروتوكول "Internet Protocol (TCP/IP)"، ثم اضغط فوق زر "خصائص".

ه- ستظهر نافذة "خصائص Internet Protocol(TCP/IP)"، كما في شكل ٢-٢، ثم حدد خيار "الحصول على عنوان IP تلقائياً"، وخيار "الحصول على عنوان ملقم DNS تلقائياً".

شكل ٢-١

شكل ٢-٢

و- اضغط فوق زر "موافق"، ثم اضغط زر "موافق" مرة أخرى.

ز- انقر بزر الفأرة الأيمن فوق أيقونة "جهاز الكمبيوتر"، ومن القائمة الفرعية اختر "خصائص".

ح- ستظهر نافذة "خصائص النظام"، شكل ٢-٣، ومنها اختر تبويب "اسم الكمبيوتر"، ثم انقر فوق زر "تغيير...".

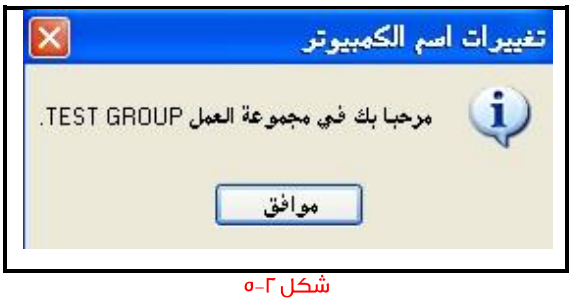
شكل ٢-٣

ط- ستظهر نافذة "تغييرات اسم الكمبيوتر"، أعط اسماً للجهاز وليكن "Pc1" مثلاً في مربع نص "اسم الكمبيوتر"، كما في شكل ٢-٤.

ي- أعط اسماً لمجموعة العمل وليكن "TEST GROUP" مثلاً، كما في شكل ٢-٤.

شكل ٢-٤

ك- انقر فوق "موافق"، وبعد عدة ثوان ستظهر شاشة ترحيب تدل على انضمامك إلى مجموعة العمل التي اخترتها، وهي "TEST GROUP" في مثالنا هذا، كما في شكل ٢-٥.



شكل ٢-٥

ل- بعدها، ستظهر نافذة جديدة تطلب إعادة تشغيل الكمبيوتر، كما في شكل ٢-٦، انقر فوق زر "موافق".

شكل ٢-٦

م- اضغط فوق زر "موافق"، ثم اضغط زر "موافق" مرة أخرى.

ن- أعد تشغيل الكمبيوتر حتى تصبح التغيرات نافذة المفعول.

س- كرر نفس الخطوات السابقة على جهاز الحاسب الثاني مع التأكد من تسمية الحاسب باسم مختلف وليكن "Pc2" مثلاً.

ملاحظة:

في مجموعة العمل الواحدة، لا يجوز تسمية جهازين بنفس الاسم، وبالنسبة لاسم مجموعة العمل، فإنه يجب أن يكون موحداً لجميع الأجهزة المتصلة معاً.

ثالثاً: استعراض أجهزة الحاسب المرتبطة بمجموعة العمل

أ- انقر نقراً مزدوجاً فوق أيقونة مواضع شبكة الاتصال على سطح المكتب.

ب- ستظهر نافذة "مواضع شبكة الاتصال"، كما في شكل ٢-٧، انقر فوق خيار "عرض أجهزة مجموعة العمل".

شكل ٢-٧

ج- ستظهر نافذة "Test Group"، التي تبين الجهازين المتصلين في مجموعة العمل "TEST GROUP"، كما في شكل ٢-٨.

شكل ٢-٨

رابعاً: بناء شبكة بين جهازين من نوع مجموعة عمل وعناوين IP الثابتة

أ- كرر الخطوات من أ إلى هـ في ثانياً.

ب- ستظهر نافذة "خصائص Internet Protocol(TCP/IP)"، ومنها حدد خيار "استخدام عنوان IP تلقائياً التالي".

ج- أعط "عنوان IP" و "قناع الشبكة الفرعية" كما في شكل ٢-٩.

شكل ٢-٩

د- اضغط فوق زر "موافق"، ثم اضغط زر "موافق" مرة أخرى.

س- إلى أي فئة يتبع عنوان IP المستخدم في شكل ٢-٩؟

ملاحظة:

في مجموعة العمل الواحدة، لا يجوز إعطاء جهازين نفس عنوان IP.

١- هل يمكن استخدام كابل UTP نوع Cross Over لربط جهازين معاً؟ لماذا؟

٢- ما هي الرسالة التي يظهرها نظام التشغيل في الحالات التالية:

أ. تسمية جهازين في مجموعة عمل واحدة باسمين متشابهين

ب. إعطاء عنوان IP واحد لجهازين متصلين في مجموعة عمل واحدة

٣- قام شخص بإعداد شبكة من جهازين على النحو التالي:

اسم الجهاز	اسم مجموعة العمل	عنوان IP	قناع الشبكة الفرعية
Comp1	Fast link	100.10.20.15	255.0.0.0
Comp15	Fast link	192.168.123.48	255.255.255.0

- هل يتم الاتصال بين الجهازين؟ لماذا؟

- ما هي التعديلات التي يمكن القيام بها لضمان اتصال الجهازين معاً؟

الجانب العملي

مشاركة الوسائط والمجلدات

Media and Folders Sharing

تـؤمن شـبكة الحاسـبات إمكانيـة تشـارك المسـتثمرين فـي مـوارد الشـبكة المختلفـة مثـل الطابعـات والماسحات الضوئية ومحركات الأقراص بما تحتويه من مجلدات وملفـات وغيرهـا مـن مـوارد الشـبكة المختلفـة. ويمكن للمستخدم في الشبكة تحديد الأجهزة المحيطية والملفات التي يريد بقية مستخدمي الشبكة فيها، كما يمكن تحديد المجموعات أو الأشخاص الذين يستطيعون التعامل مع مورد معيّن، وكـذلك تخصـيص كلمـة مـرور للوصول إليها. تكون الموارد في شبكة الند للند موزعة على حاسبات عديدة في الشبكة مما يتطلب لإبقاء هـذه الحاسبات في حالة العمل والارتباط مع الشـبكة طالمـا أن مسـتخدمي الشـبكة الآخـرين يحتـاجون المعلومـات المخزنة على تلك الحاسبات.

خصائص المشاركة

- تعمل المشاركات فقط مع عناصر المجلد ولكنها لا تعمل مع الملفات التي توجد في المجلـدات. يمكنـك أن تشارك المجلد وتسمح للمستخدمين بالوصول إلى الملفات الموجودة في المجلد.
- يمكن أن تنشأ المشاركات باستخدام نظام الملفات FAT ونظام الملفات NTFS.
- تعد المشاركات مرئية بالنسبة للمستخدمين المتصلين عن طريق شبكة الاتصال.
- المجلد المشترك الموجود على الحاسب تظهر على شكل أيقونة لديها يد تمسك بالمجلد. ولكنهـا تظهـر من خلال شبكة الاتصال، ولا تحتوي الأيقونة على اليد.
- من الممكن تجميع تصاريح المشاركة. فإذا كان المستخدم عضواً في مجموعة واحدة لديها ميـزة الوصـول Read وكان عضواً كذلك في مجموعة أخرى لـديها ميـزة Change علـى نفـس المشـاركة فـإن التصـاريح المجمعة الخاصة بالمستخدم الموجودة في المشاركة تعتبر Read و Change في ذات الوقت.
- عندما نقل مجلد يتم حذف المشاركات المخصصـة لـــه، وعنـد نسـخ مجلـد فـإن النسـخة الجديـدة لا تعتبـر مشتركة ويبقى المجلد المصدر مشتركاً.

من الذي يستطيع تقديم المشاركة في المجلدات؟

من خلال جهاز الكمبيوتر المستقل يسـتطيع حسـاب المـدير Administrator وأعضـاء مجمـوعتي Power Users و Administrators الداخليتين من المشاركة في المجلدات.

المشاركات المخفية

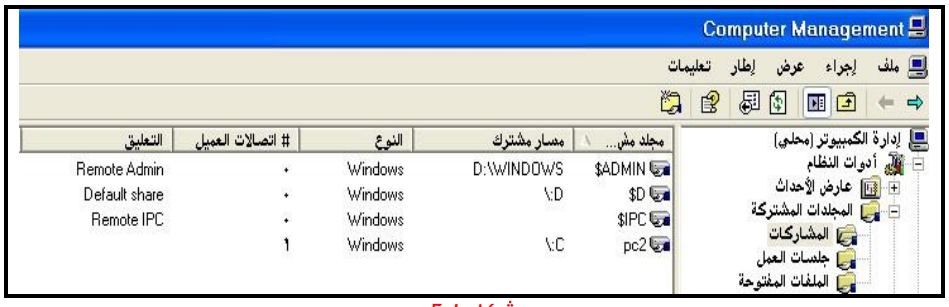
تعد سمة المشاركة المخبأة مفيدة جداً في حل مشكلة كون المشاركات مرئية بالنسبة لأي شخص موجود على شبكة الاتصال. من الممكن إخفاء المشاركات عن طريق إنهاء اسم المشاركة بعلامة الدولار ($). ويمكن الاتصال بالمشاركة المخفية باستخدام Run، وأمر NET SHARE.

أولاً: إنشاء مشاركات على الأقراص المحلية والمجلدات باستخدام المعالج

أ- أنقر بزر الفأرة الأيمن فوق أيقونة "جهاز الكمبيوتر"، ومن القائمة الفرعية اختر " إدارة ". كما في الشكل ١٠-١.

شكل ١٠-١

ب- ستظهر لك نافذة "Computer Management"، انقر على إشارة "+" المحاذية لمجلد "المجلدات المشتركة"، ثم انقر فوق مجلد "المشاركات"، كما في الشكل ١٠-٢.



شكل ١٠-٢

س- كم عدد المشاركات الموجودة على الحاسب الذي تعمل عليه؟

أنقر بزر الفأرة الأيمن فوق "المشاركات" ثم اختر "مشاركة ملف جديدة ..." من القائمة الفرعية، كما في الشكل ١٠-٣.

شكل ١٠-٣

ج- ستظهر شاشة ترحيبية أنقر فوق زر "التالي" للبدء في تشغيل "معالج إنشاء مشاركة جديدة".

د- ستظهر نافذة كما في الشكل ١٠-٤، أنقر فوق زر "استعراض".

شكل ١٠-٤

ه- ستظهر نافذة "الاستعراض بحثاً عن مجلد" كما في الشكل ١٠-٥ ، حدد من خلالها "محرك أقراص مضغوطة :E" (وهو محرك الأقراص المراد مشاركته).

شكل ١٠-٥

و- أنقر فوق زر "موافق" للعودة إلى نافذة شكل ١٠-٤، تأكد من ملئ مربعات النص كما في الشكل ١٠-٦، ثم اضغط فوق زر "التالي".

شكل ١٠-٦

ز- ستظهر نافذة "أذونات المجلد المشتركة"، حدد الخيار "كافة المستخدمين لديهم حق القراءة فقط"، كما في الشكل ١٠-٧.

شكل ١٠-٧

م-أنقر فوق زر "التالي" ثم فوق زر "إنهاء". لاحظ وجود مشاركة جديدة على القرص المضغوط E: باسم CD Drive كما في الشكل ١٠-٨.

شكل ١٠-٨

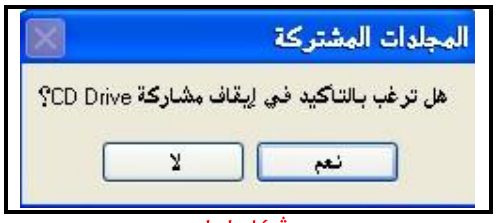
ثانياً : إلغاء المشاركات عن الأقراص المحلية والمجلدات باستخدام المعالج

أ- أعد الخطوات (أ ، ب) التي قمت بها في أولاً.

ب- أنقر بزر الفأرة الأيمن فوق المشاركة الخاصة بالقرص المضغوط E: ثم اختر "قطع المشاركة" من القائمة الفرعية كما في الشكل ١٠-٩.

شكل ١٠-٩

ج-ستظهر نافذة تأكيد إلغاء المشاركة كما في شكل ١٠-١٠، أنقر فوق زر "نعم".



شكل ١٠-١٠

ثالثاً : طريقة أخرى لإنشاء المشاركات على الأقراص المحلية والمجلدات

أ- أنقر نقراً مزدوجاً فوق أيقونة "جهاز الكمبيوتر" ثم أنقر بزر الفأرة الأيمن فوق أيقونة "محرك أقراص مضغوطة E:".

ب- من القائمة الفرعية اختر "مشاركة وأمان..."، كما في الشكل ١٠-١١.

شكل ١٠-١١

ج-ستظهر نافذة "خصائص محرك أقراص مضغوطة (E:)"، تبويب "المشاركة"، تأكد من ملئ النافذة بالمعلومات كما في الشكل ١٠-١٢.

شكل ١٠-١٢

رابعاً: طريقة أخرى لإلغاء المشاركات على الأقراص المحلية والمجلدات

أ- أنقر نقراً مزدوجاً فوق أيقونة "جهاز الكمبيوتر" ثم أنقر بزر الفأرة الأيمن فوق أيقونة "محرك أقراص مضغوطة E:"، سبق إنشاء مشاركة عليها في ثالثاً.

ب- من القائمة الفرعية اختر "مشاركة وأمان...".

ج-ستظهر نافذة كما في شكل ١٠-١٣، ومن تبويب "مشاركة"، حدد خيار "عدم مشاركة هذا المجلد".

د- انقر فوق زر موافق.

شكل ١٠-١٣

خامساً: الوصول إلى المشاركات على حاسبات مجموعة العمل

أ- استعرض أجهزة مجموعة العمل المتصل بها حاسبك.

ب- أنقر نقراً مزدوجاً فوق أيقونة أحد الحاسبات المتوفرة في مجموعة العمل.

س- ما هو عدد المشاركات الموجودة على الجهاز الذي قمت بالدخول إليه؟ وما هي أسماء هذه المشاركات؟

س- ما الفرق بين اسم القرص (المجلد) واسم المشاركة على القرص (المجلد)؟

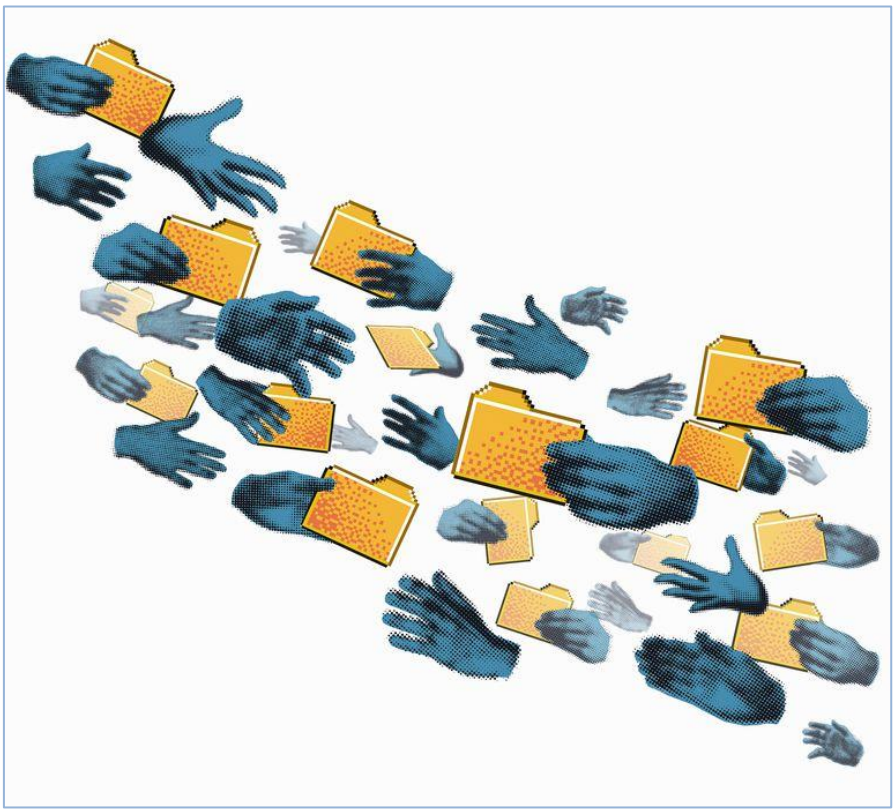
س- ما الفرق بين إلغاء المشاركة عن محرك أقراص، وإزالة المشاركة عن محرك أقراص.

س- أنشئ مجلد على القرص المحلي C: باسم (My Folder)، ثم أنشئ مشاركة عليه باسم (مجلد التدريبات) باستخدام طريقتين مختلفتين.

الجانب العملي

المشاركة المخفية

Hidden Sharing



تعد سمة إخفاء المشاركات مفيدة جداً في أنظمة تشغيل Windows. فقد تم إنشاؤها من أجل مشكلة كون المشاركات مرئية بالنسبة لأي شخص موجود على شبكة الاتصال، وينطبق ذلك حتى على المستخدمين الذين لا يستطيعون الوصول إلى المشاركات. أما إخفاء المشاركات فيعد صعباً جداً ويحتاج لتكنولوجيا متقدمة لتقديمها في نظام التشغيل. ولكنها تمثل شيئاً هاماً بالنسبة للمستخدمين الذين يستطيعون الوصول إليها. وبالنسبة للمستخدمين الآخرين فإن المشاركات ينبغي أن تكون مرئية فقط في حالة الحاجة إلى التعرف عليها. وعلى ذلك فإنه من الممكن إخفاء المشاركات عن طريق وضع علامة ($) في نهاية اسم المشاركة. ويمكنك أن تظل متصلاً بالمشاركة إذا كنت قد وصلت إليه ولكنه لن يظهر على قائمة التصفح (حيث أنه لا يظهر شيئاً ينتهي بعلامة الدولار على قائمة التصفح). ويمكنك أن تتصل بالمشاركة باستخدام Run، كما سيتم توضيح ذلك لاحقاً.

أولاً: إنشاء مشاركة مخفية على الأقراص المحلية والمجلدات

ط- من نافذة "Computer Management"، انقر على إشارة "+" المحاذية لمجلد "المجلدات المشتركة"، ثم انقر فوق مجلد "المشاركات"، كما في الشكل ١١-١، ثم أغلق النافذة.

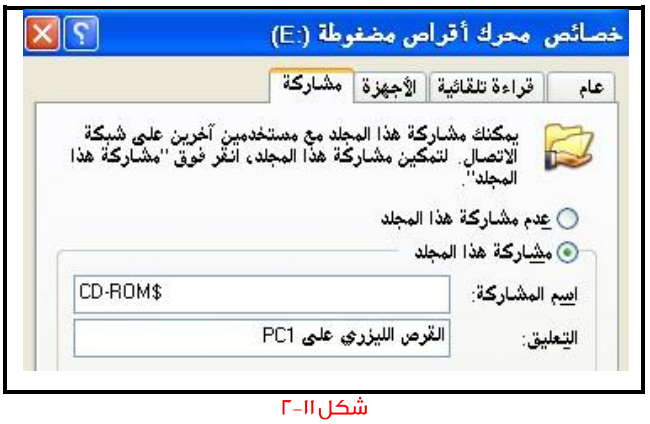
شكل ١١-١

س- كم عدد المشاركات المنشأة على جهاز الحاسب لديك؟

س- ماذا تعني علامة ($) الظاهرة بعد بعض أسماء المشاركات؟

أنقر نقراً مزدوجاً فوق أيقونة "جهاز الكمبيوتر" ثم أنقر بزر الفأرة الأيمن فوق أيقونة "محرك أقراص مضغوطة E:"، ومن القائمة الفرعية اختر "مشاركة وأمان...".

ي- ستظهر نافذة "خصائص محرك أقراص مضغوطة (E:)"، تبويب "المشاركة"، تأكد من ملئ النافذة بالمعلومات كما في الشكل ١١-٢. ثم انقر فوق زر موافق.



شكل ١١-٢

ك- انتقل إلى جهاز حاسب آخر من أجهزة مجموعة العمل المتصل بها حاسبك.

ل- من مواضع شبكة الاتصال استعرض أجهزة مجموعة العمل.

م- أنقر نقراً مزدوجاً فوق أيقونة الحاسب الذي أنشأت فيه المشاركة المخفية.

ثانياً: الوصول إلى المشاركات المخفية باستخدام أمر تشغيل

أ- انتقل إلى جهاز حاسب آخر من أجهزة مجموعة العمل المتصل بها حاسبك.

ب- انقر فوق زر قائمة ابدأ، ثم الأمر "تشغيل".

ج- اكتب الأمر كما هو موضح في الشكل ١١-٣.

شكل ١١-٣

د- ستظهر نافذة تظهر محتوى القرص المضغوط على الحاسب الذي أنشأت فيه المشاركة المخفية، انظر الشكل ١١-٤.

شكل ١١-٤

ثالثاً: تعيين محرك أقراص شبكة اتصال لمحرك أقراص أو مجلد مشترك

ل- انقر بزر الفأرة الأيمن فوق أيقونة "جهاز الكمبيوتر"، ثم اختر "تعيين محرك أقراص شبكة اتصال..."، كما في الشكل ١١-٥.

شكل ١١-٥

م- ستظهر نافذة "تعيين حرف لمحرك أقراص شبكة الاتصال"، انظر الشكل ١١-٦، انقر فوق زر "استعراض".

شكل ١١-٦

ن- انقر فوق إشارة (+) المحاذية لاسم مجموعة العمل، ثم انقر فوق إشارة (+) المحاذية لاسم الحاسب الذي تتوفر عليه المشاركة.

س- حدد اسم محرك الأقراص أو المجلد الهدف، ثم انقر فوق زر "موافق"، ثم انقر فوق زر "إنهاء" للخروج من المعالج.

ع- مباشرة ستظهر نافذة تظهر محتويات القرص أو المجلد الهدف، الشكل ١١-٧.

ف- أغلق النافذة، ثم انقر نقراً مزدوجاً فوق أيقونة "جهاز الكمبيوتر.

رابعاً: قطع الاتصال بمحرك أقراص شبكة اتصال

أ- انقر بزر الفأرة الأيمن فوق أيقونة "جهاز الكمبيوتر"، ثم اختر "قطع الاتصال بمحرك أقراص شبكة اتصال...".

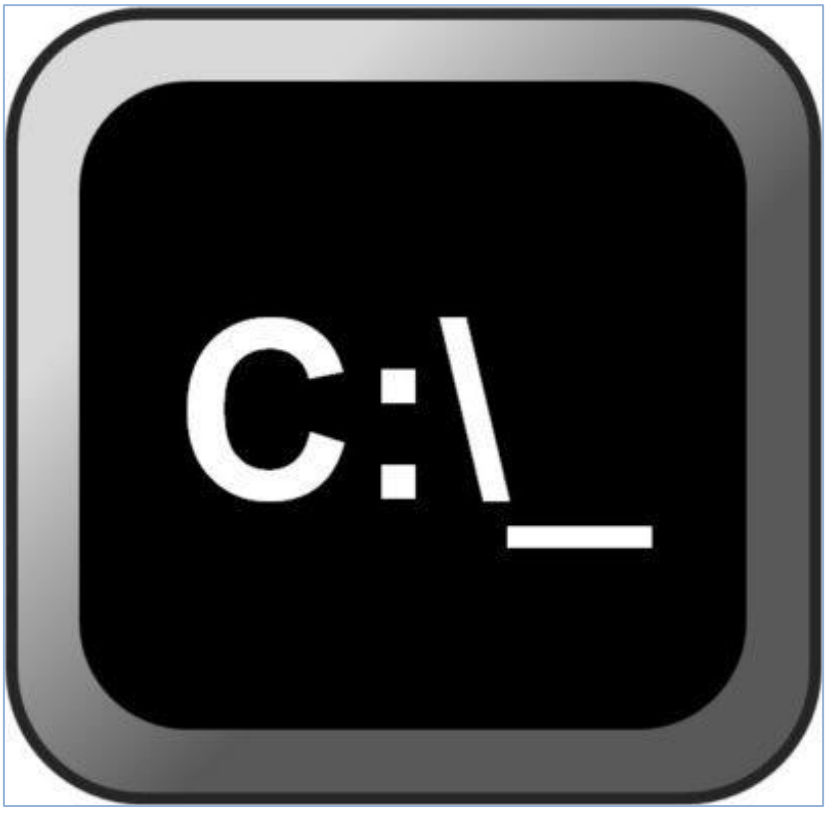
ب- ستظهر نافذة "قطع اتصال محركات أقراص شبكة الاتصال"، انظر الشكل ١١-٧.

ج-حدد محرك أقراص المشاركة المراد قطعها، ثم انقر فوق زر "موافق".

شكل ١١-٧

موجه الأوامر في إدارة الشبكة

Network Management using Command Prompt

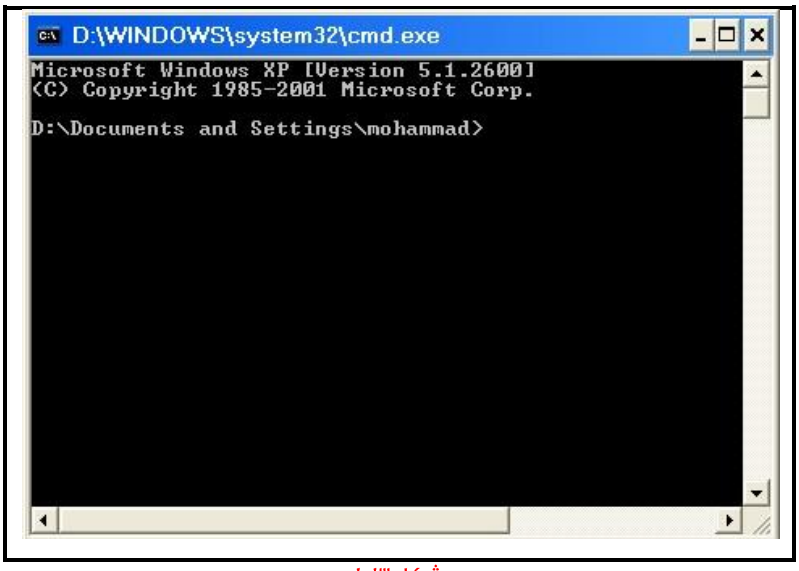


أولاً: التدرب على أهم أوامر بيئة التشغيل الخطية DOS المستخدمة في إدارة الاتصال وعنوان IP

أ- سجل الدخول بحساب المدير Administrator أو أي حساب عضو في مجموعة المدراء Administrators.

ب- انقر فوق زر قائمة "ابدأ"، اختر تشغيل "RUN"، ثم اكتب CMD، ثم انقر فوق زر "موافق".

ج- ستظهر نافذة مواجهة بيئة التشغيل الخطية DOS، كما في الشكل(١٣-١).



شكل ١٣-١

- لمعرفة إعدادات بروتوكول TCP/IP اكتب الأمر:

```
C:\>ipconfig
```

ستظهر نتائج تنفيذ الأمر كما في الشكل (١٣-٢).

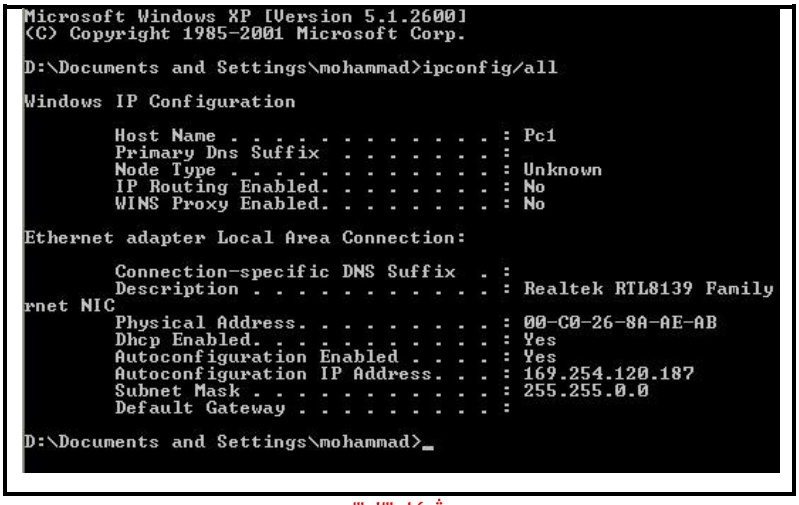
شكل ١٣-٢

س- ما هو عنوان IP للجهاز، وعنوان قناع الشبكة الفرعي (Subnet Mask)؟

- لمعرفة إعدادات بروتوكول TCP/IP كاملة اكتب الأمر:

```
C:\>ipconfig/all
```

د- ستظهر نتائج تنفيذ الأمر كما في الشكل (١٣-٣).

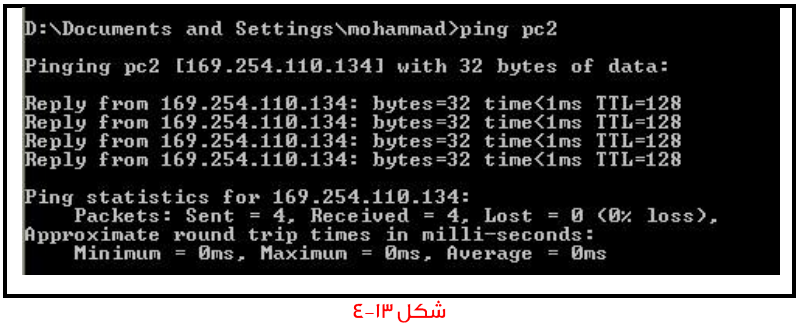


شكل ١٣-٣

- للتأكد من اتصال الجهاز Pc2 على شبكة الاتصال أكتب الأمر:

```
C:\>Ping Pc2
```

ستظهر نتائج تنفيذ الأمـر كما في الشكـل (١٣-٤).



شكل ١٣-٤

س- ما هو عنوان IP الخاص بالجهاز Pc2؟

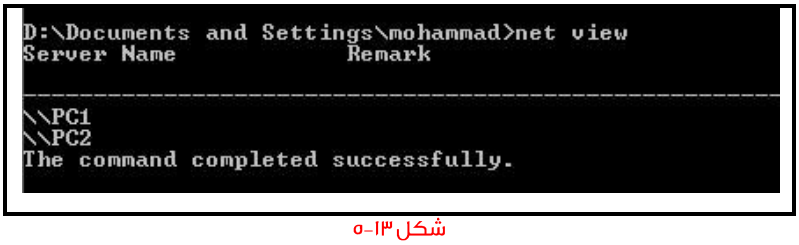
س- هل تستطيع التأكد من اتصال الجهاز Pc2 من خلال عنوان IP الخاص به؟ وضح؟

س- ماذا يحدث لو حاولت التأكد من اتصال جهاز مغلق أو مفصول عن الشبكة؟

- لاستعراض جميع أجهزة الحاسب المتصلة بالشبكة أكتب الأمر:

```
C:\>net view
```

o- ستظهر نتائج تنفيذ الأمـر كما في الشكـل (١٣-٥).



شكل ١٣-٥

ثانياً: التدرب على أهم أوامر بيئة التشغيل الخطية DOS المستخدمة في إدارة الحسابات والمجموعات على محطات العمل المحلية

- لاستعراض جميع المستخدمين المحليين، أكتب الأمر:

```
C:\>net users
```

ستظهر نتائج تنفيذ الأمر كما في الشكل (١٣-٦).

```
D:\Documents and Settings\mohammad>net user

User accounts for \\PC1

-------------------------------------------------------------------------------
Administrator            Guest                    HelpAssistant
lss                      mohammad                 q
SUPPORT_388945a0         user1                    user2
user3
The command completed successfully.
```

شكل ١٣-٦

س- كم عدد المستخدمين المحليين الذين تم إنشاؤهم على جهازك؟

_____

_____

- لاستعراض بعض خصائص نهج الأمان المحلي (نهج كلمة المرور)، أكتب الأمر:

```
C:\>net accounts
```

ستظهر نتائج تنفيذ الأمر كما في الشكل (١٣-٧).

```
D:\Documents and Settings\mohammad>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    2
Lockout duration (minutes):                           1
Lockout observation window (minutes):                 1
Computer role:                                        WORKSTATION
The command completed successfully.
```

شكل ١٣-٧

س- ماذا تعني جميع النتائج التي ظهرت على جهازك عند تطبيق الأمر؟

_____

_____

- لإنشاء مستخدم محلي باسم "FastLink" بكلمـة مرور "١٢٣"، أكتب الأمر:

```
C:\>net user FastLink 123 /add
```

- لتغير كلمة المرور للمستخدم FastLink من ١٢٣ إلى ٤٥٦ أكتب الأمر:

```
C:\>net user FastLink 456 /passwordchg:yes
```

- لاستعراض خصائص المستخدم FastLink، أكتب الأمر:

```
C:\>net user FastLink | more
```

- لحذف المستخدم FastLink، أكتب الأمر:

```
C:\>net user FastLink /del
```

ثالثاً: التدرب على أهم أوامر بيئة التشغيل الخطية DOS المستخدمة في إدارة المشاركات

- لعرض المجلدات أو محركات الأقراص المشتركة، أكتب الأمر:

```
C:\>net share
```

- لعرض خصائص اسم المشاركة C$، أكتب الأمر:

```
C:\>net share c$
```

- لإنشاء مشاركة باسم "Pictures" على المجلد "MyPhoto" الموجود على محرك الأقراص d:، أكتب الأمر:

```
C:\>net share Pictures="D:\MyPhoto"
```

- لحذف المشاركة "Pictures"، أكتب الأمر:

```
C:\>net share Pictures /del
```