كتاب فهم وتنصيب الشبكات السلكية واللاسلكية المحلية LAN مع امن الشبكات

تاليف

مهندس نظم

ماجستير هندسة نظم المملكة المتحدة

بدون اسم المؤلف لتجنب الرياء ولا تنسونا من الدعاء

بسم الله الرحمن الرحيم

ا لحمدلله والصلاة والسلام على رسول الله وعلى آله وصحبه أجمعين ..... أما بعد.

اهداء

اهدي هذا الكتاب الى كافة افراد عائلتي الاعزاء اولا ومن ثم اهديه الى ابنتي المغتربة مع ابنتيها في المانيا واهديه الى كل من يستفاد من هذا الكتاب ويعمل به . واهديه الى كل من ينشره بنية نشر المعرفة والعلم مع الحفاظ على حقوق المؤلف واهديه الى كل المصادر التي تم الاستعانة بها من معلومات ووسائل ايضاح ورسومات وانه حق من حقوقهم..... ومن الله التوفيق

المقدمة

في الواقع الذي نعيشه، و مع تقدم عجلة الزمن والحياة ، تطورت العلوم والتقنية في شتى المجلات لا سيما في تقنية الاتصالات والمعلومات ، فنتج عن ذلك الأمر ثورات هائلة في مجال التقنيات، ومنها الشبكات .هذه التقنية تعطي مرونة أكثر لمجرى العمل في القطاعات و المؤسسات التي تحل بها.

وقد ظهرت الشبكات نظراً للحاجة إلى الاتصال بين الأفراد في الأماكن المتباعدة وتبادل الخدمات المختلفة، وساعد في ذلك التطور العلمي والتقني . لذلك دعت الحاجة الى اِنشاء نظام يمكن للمستخدم الشاركة في مصادر المعلومات مثل ربط فروع الشركة المنتشرة في عدة مناطق بنظام واحد و كذلك المشاركة في الأجهزة و البرامج مثل ربط آلة الطباعة بعدة أجهزة بدلا من أن يكون لكل جهاز طابعة خاصة. لذلك فان الشبكات سوف توفر بيئة عمل مشتركة و التي سوف تمكن مسؤلي الشركة من الادارة والدعم المركزي

ازدهرت اعمال الشبكات خلال السنوات القليلة الماضية واصبح من النادر ان يوجد جهاز كومبيوتر في احد الشركات الكبير غير متصل بشبكة كومبيوتر واصبح الامر لا يتوقف على الشبكات الكبيرة فقط بل حتى الشركات الصغيرة والسبب هو ما وجد هذه الشركات من فوائد كبيرةتعود عليها من هذه الشبكات وهذه الفوائد لا تشكل جانب واحد بل عدة جوانب بما في ذلك المشاركة بالاجهزة والمشاركة في المعلومات التي تعتبر عنصر الحياة الاول لاي شركو ووسبب نجاحها

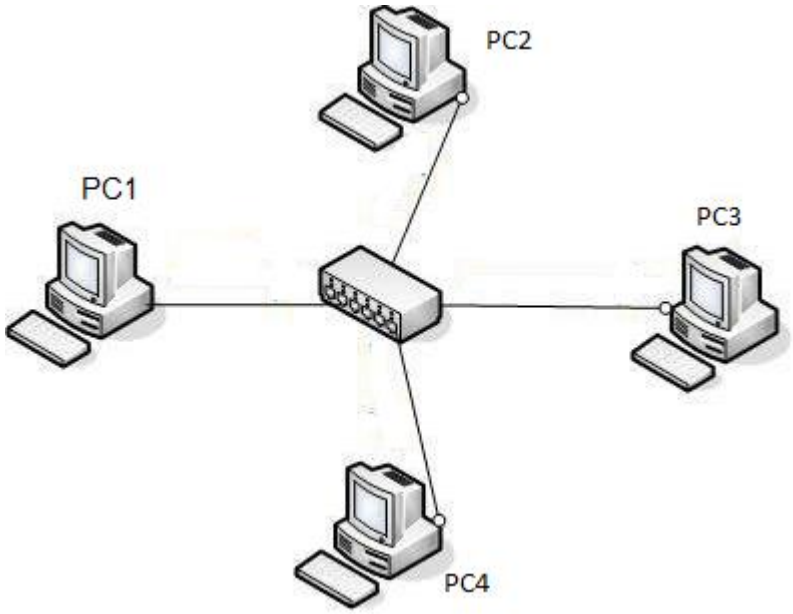
وقد ساعد انتشار الاجهزة والمعدات والبرامج والانخفاض المستمر في التكاليف بعمل الشبادكات والميل الى استخدامها بكثرة بالاضافة الى انها سهلة التركيب بحيث لا تحتاج الى خبير مختص بنصب الشبكات وهذا يتم من خلال ما لديك من فهم واسع حول الشبكات وهذا ما اريد ان اصل اليه في هذا الكتاب ان شاء الله من خلال ما ساقدمه من شرح واسع بحيث فعلا سوف لا نحتاج الى خبير او تقني مختص في الشبكات ولكي لا نبالغ هذا يخص الشبكات الصغير طبعا وكل ما كبر او توسع حجم الشبكة كلما زاد التعقيد

تعريف الشبكة

نقصد بالشبكة مجموعة من الحواسيب المتصلة فيما بينها فيزيائياً بحيث يمكن لأي منها الوصول إلى الآخر واستخدام موارده من تطبيقات وقواعد بيانات ومعطيات وغيرها من المصادر.

في أبسط أشكالها تتكون الشبكة من جهازين كمبيوتر متصلين ببعضهما بواسطة سلك cable، و يقومان بتبادل البيانات. تُوصل الحواسيب بواسطة أسلاك تختلف من شبكة إلى أخرى تبعاً للتقنية المعتمدة والبنية المستخدمة. أما عن وصل السلك cable بالحاسوب فيتم عن طريق مأخذ في بطاقة خاصة موجودة في الحاسوب ويوصل بها السلك

عند وصل مجموعة متقاربة من الحواسيب مع بعضها فإننا ندعوها شبكة محلية (**Local Area Network**) أو اختصاراً **LAN** وتكون هذه الشبكة صغيرة نسبياً وتتباعد عناصرها لمسافات قصيرة تتعلّق بنوع الأسلاك المستعملة، وهي غالباً شبكة في بناء أو مجموعة متقاربة من الأبنية كأبنية المعاهد والجامعات, .والشركات الصغيرة أما عندما تكبر المسافات فإننا نقوم بإنشاء مجموعات من الشبكات المحلية ثم نربطها ببعضها عن طريق عناصر خاصة وأسلاك من نوع خاص كالخطوط الهاتفية، وذلك لأن المسافات الطويلة تحتاج إلى وسائط نقل أكثر سرعة وفعالية. نسمي هذا النمط بالشبكات الموسعة wide area networ واختصارها WAN وهذا رسم لشبكة محلية بسيطة جدا



الهدف من استعمال الشبكة

مع إزدياد حجم المؤسسات والشركات والتطور في أساليب العمل والكم الهائل من البيانات والمعلومات التي تتعامل فيها هذه الشركات، كان هناك حاجة ملحة للتمكن من تسيير إنتقال هذه البيانات والمعلومات بالسرعة التي لا تعطل سير العمل وبالتالي كان من الضروري ربط أجهزة الحاسب فيما بينها بما يعرف بالشبكات ، إن الهدف الدائم من الشبكة هو التشارك في المصادر اي كل ما يُمكِن للمستخدم أن يصل إليه على حاسوب آخر كالملفات وقواعد البيانات و البرامج و الطابعات وكافةالأجهزة محيطية و تسمح للمستخدمين بالتواصل مع البعض بشكل فوري.

بدايةً لنتخيل وضع الكمبيوتر بدون وجود شبكات ، في هذه الحالة كيف سنتبادل البيانات ، سنحتاج الى مئات الأقراص او الفلاش روم وغيرها من وسائل النقل لنقل المعلومات من جهاز الى آخر مما يسبب هدراً كبيرا للوقت و الجهد. و مثال آخر إذا كان لدينا طابعة واحدة و عدة حواسب في هذه الحال إذا أردنا الطباعة فإما سنقوم بالوقف في طابور

انتظار على الجهاز الموصل بالطابعة ، أو سنقوم بنقل الطابعة إلى كل مستخدم ليوصلها إلى جهازه ليطبع ما يريد و في كلا الأمرين عناءاً كبير ، و من هنا نرى أن تقنية التشبيك قد تطورت لسد الحاجة المتنامية لتبادل المعلومات و الموارد بشكل فعال

في الشبكات الحديثة من المهم استخدام لغة مشتركة أو بروتوكول Protocol متوافق عليه لكي تستطيع الأجهزة المختلفة الاتصال مع بعضها البعض و فهم كل منها الآخر. والبروتوكول هو مجموعة من المعايير أو المقاييس المستخدمة لتبادل المعلومات بين جهازي كمبيوتر.

المتطلبات العامة لعمل الشبكات

1-لكي تشكل الحواسب شبكة، تحتاج إلى وسط ناقل للبيانات و في هذه الحالة يكون إما أسلاك أو وسط لاسلكي.

2-كما تحتاج هذه الحواسب إلى موائم أو أداة ربط ، Adapterلتقوم بوصل هذه الأجهزة بالأسلاك المكونة للشبكة و تسمى هذه الموائمات بطاقة واجهة الشبكة Network Interface Card وحاليا الـ Adapterموجود ضمن الـ mother board والذي يسمى build in

٣-حاسبة تقدم البيانات أو الموارد في الشبكات الحالية يطلق عليها اسم مزودات ، Servers وحواسب التي تستفيد من هذه البيانات أو الموارد والتي تسمى زبائن Clients

٤-تحتاج الشبكة إلى برنامج شبكات مثبته على الأجهزة المتصلة بالشبكة سواء كانت مزودات أو زبائن ، و هذا البرنامج إما يكون نظام تشغيل شبكات ، NOS (Network Operating System)أو يكون نظام تشغيل بمختلف انواعه (Windows)يقوم هذا النظام بالتحكم بمكونات الشبكة و صيانة الاتصال بين الزبون و المزود

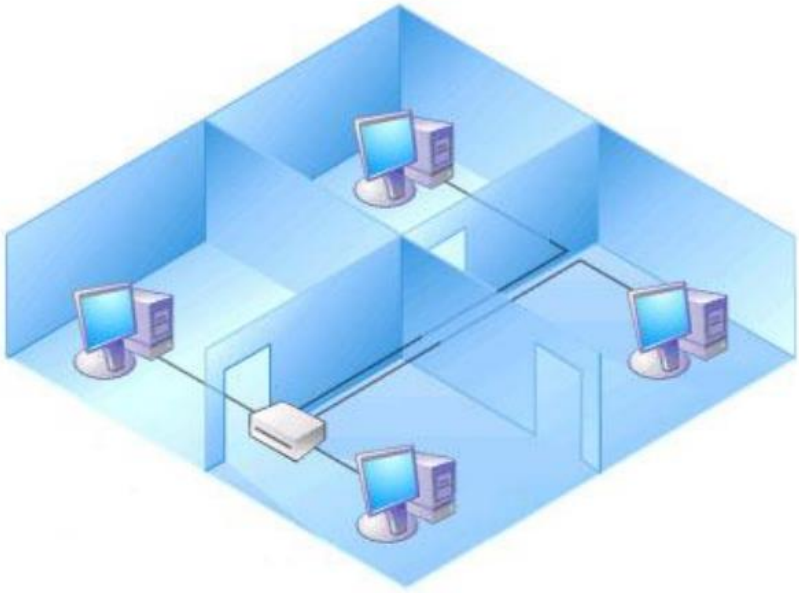
٥- وسائط سلكية او لاسلكية لربط الحاسبات فيما بينها وتكون على عدة انواع ونذكر منها :

- أسلاك مزدوجة مجدولة Twisted pair cableو تكون هذه الأسلاك إما مغطاة أو غير مغطاة بطبقة واقية. (Shielded or Unshielded)
- السلك المحوري Coaxial cable
- أسلاك الألياف البصريه Optic Cable .
- وسط اتصال لاسلكي Wireless transmission media

طرق توصيل الشبكات الحديثة...

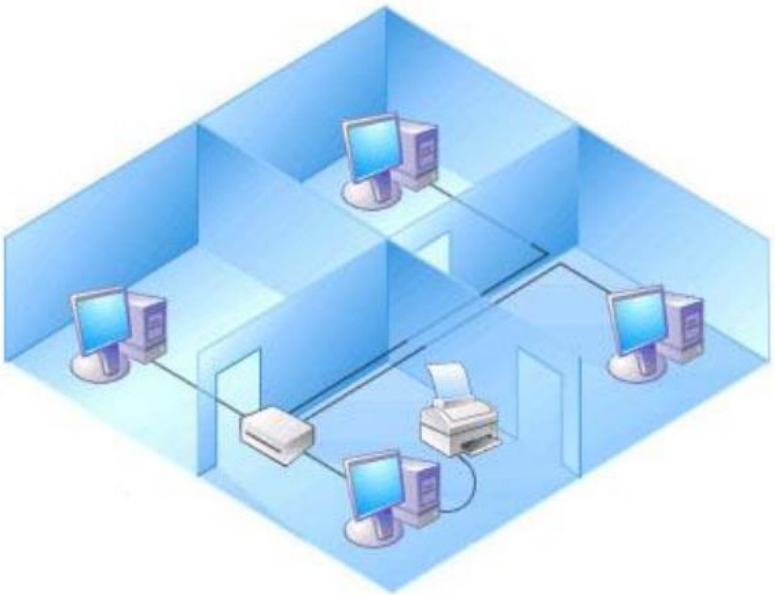
- **شبكة الند للند Peer to Peer networks:**

تتكون هذه الشبكة من أجهزة وأنظمة لها الإمكانيات والوظائف نفسها. وتسمح هذه الشبكة للحواسيب المكتبية والحواسيب المحمولة بالتصرف كما لو أنها أجهزة خادم، كما تسمح لها بالتشارك في ملفاتها مع الأجهزة الأخرى الموجودة في الشبكة، ومن الأمثلة على هذه الشبكة، شبكة المنزل، وشبكة المكاتب التي لا تحتاج إلى وجود جهاز خادم ذي قدرات تخزينية عالية, ويمكن لأي جهاز على الشبكة أن يكون خادم أو زبون.



- **شبكة الخادم/ الزبون Client-Server networks:**

تتكون هذه الشبكة من حاسوب قوي يسمى الخادم Server، وهي الأجهزة التي تقدم الخدمة من حيث التخزين والبرامج وموارد الشبكة للأجهزة التي تطلبها وهي أجهزة الزبون Client, ويكون عمل أجهزة الزبائن Clients مرتبط بعمل الجهاز الخادم Server.



لنلق الآن نظرة على مميزات شبكات الزبون / المزود و التي تتفوق فيها على شبكة الند للند :

1- النسخ الاحتياطي للبيانات وفقا لجدول زمني محدد.

2- حماية البيانات من الفقد أو التلف.

3- تدعم آلاف المستخدمين .

4- تزيل الحاجة لجعل أجهزة الزبائن قوية وبالتالي من الممكن أن تكون أجهزة رخيصة بمواصفات متواضعة.

5- في هذا النوع من الشبكات تكون موارد الشبكة متمركزة في جهاز واحد هو المزود مما يجعل الوصول إلى المعلومة أو المورد المطلوب أسهل بكثير مما لو كان موزعا على أجهزة مختلفة ، كما يسهل إدارة البيانات و التحكم فيها بشكل أفضل .

6- يعتبر أمن الشبكة Security من أهم الأسباب لاستخدام شبكات الزبون / المزود ، نظرا للدرجة العالية من الحماية التي يوفرها المزود من خلال السماح لشخص واحد (أو أكثر عند الحاجة) هو مدير الشبكة Administrator بالتحكم في إدارة موارد الشبكة و إصدار أذونات (Permission) للمستخدمين للاستفادة من الموارد التي يحتاجونها فقط و يسمح لهم بالقراءة دون الكتابة إن كان هذا الأمر ليس من تخصصهم .

أصناف الشبكات

يمكن تصنيف الشبكات الحاسوبية بشكل عام إلى أربعة أنواع رئيسة حسب المساحة الجغرافية التي تغطيها وسرعة نقل المعطيات التي تسمح بها، إضافةً إلى عدد المستخدمين القابل للربط إلى الشبكةوهذه الانواع هي.

1.الشبكات المحلية LANs

2.شبكات إقليمية MANs

3.شبكات المناطق الواسعة WANs

4. الانترنيت Internet

يوضح الجدول التالي التصنيف المتبع مع العلم بأن الشبكات تخضع للتطور المستمر الذي يمكن أن يؤثر على المعلومات الموجودة فيه

ذ . وع الشبكة	قطر الشبكة	السرعة (bps)	عدد المستخدمين
المحلية LAN	2,000–10m	4M - 2 G	1000 – 2
الإقليمية MAN	100–5Km	56K - 622 M	5000 – 2
الواسعة WAN	1,000–100Km	2.4K - 45 M	عشرات الآلاف
الانترنت	الكرة الأرضية	_____	مئات الملايين

وكل نوع من هذه الأنواع الأربعة له ميزة خاصة ولا يصلح أن يحل نوع مكان آخر.

الشبكات المحلية(Local Area Network (LAN

فشبكة LANالمحلية تتقيد بمكان واحد مثل بناية أو بنايات متجاورة وتتميز برخص وتوفر المعدات اللازمة لها. وهي شبكة صغيرة عادة توجد ضمن طابق واحد في مبنى أو تشمل كامل المبنى أو تشمل مجموعة من المباني المتقاربة. الشبكة المحلية هي شبكة محدودة المسافة.

*الشبكات المناطقية أو MAN (Metropolitan Area Network)

شبكات MANالإقليمية صممت لنقل البيانات عبر مناطق جغرافية شاسعة ولكنها ما تزال تقع تحت مسمى المحلية وهي تصلح لربط مدينة او مدينتين متجاورة ويستخدم في ربط هذا النوع من الشبكات الألياف البصرية او الوسائل

الرقمية فهذه التقنية تقدم سرعات فائقة و شبكات MANيمكن أن تحتوي على عدد من شبكات LANsوتتميز بالسرعة و الفاعلية ومن عيوبها أنها مكلفة وصيانتها صعبة.

* :الشبكات الواسعة Wide Area Networks (WAN)

اما شبكات المناطق الواسعة WANsفهي تغطي مساحات كبيرة جدا مثل ربط الدول مع بعضها البعض ومن مميزات هذه النوع انها تربط آلاف الأجهزة وتنقل كميات كبيرة من البينات لا تنقل إلا بها ومن عيوبها أنها تحتاج إلى برامج وأجهزة غالية جدا صعبة التشغيل والصيانة.

*شبكة الانترنت Internet :

الانترنت شبكة الشبكات ، تعتبر الشبكة العالمية فلقد توسعت وانتشرت وضمت في داخلها كل انواع الشبكات.WAN / MAN / LAN

طبولوجيات الشبكة :

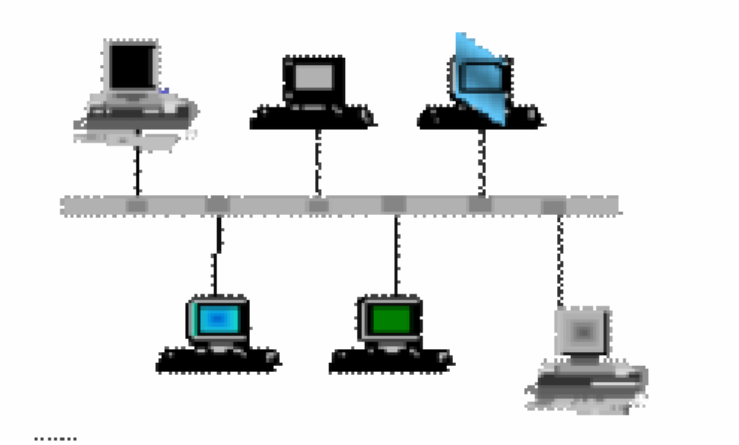
طبولوجيات الشبكة يطلق على الشكل الذي سيكون عليه توصيل الحواسب مع بعضها البعض وتندرج هذه الاشكال تحت ثلاث مسميات رئيسية وهي:

*الشبكة الخطية .

*الشبكة الحلقية

* الشبكة النجمية

*الشبكة الخطية

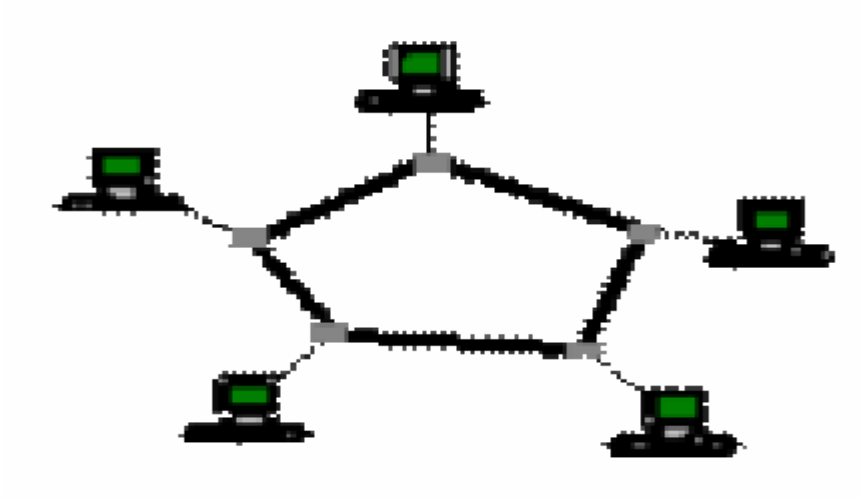


.....

يعتبر هذا النوع أبسط تصميم للشبكات حيث يتم تبادل البيانات عن طريق ناقل رئيسي وتتفرع منه الأجهزة الأخرى. كما تسمى أيضا شبكة الناقل الخطي وبنيتها أسهل وأبسط بنية فهي تتألف من كابل وحيد على الشبكة تتصل به كل الأجهزة ويستطيع أي جهاز أن يرسل إلى أي عقدة)جهاز(وتنتقل هذه الرسالة إلى كافة العقد الموجودة على الشبكة ولكن لا يستطيع قرائتها إلا المرسله له ويكون المرسل في هذه اللحظة هو المسيطر على الشبكة حتى ينتهي من عملية الإرسال.

من المحاسن في شبكة الناقل الخطي أنها سهلة التركيب ورخيصة من حيث التكلفة ومن السلبيات صعوبة تحدد المشكلة على الشبكة كما يؤثر عدد العقد الموجودة على الشبكة على سرعة الأداء، من عيوب هذا النوع أيضا أنه إذا تعطل الناقل الرئيسي تتعطل جميع الشبكة كما أنه غير ملائم عند الحاجة إلى توسعة الشبكة بشكل كبير.

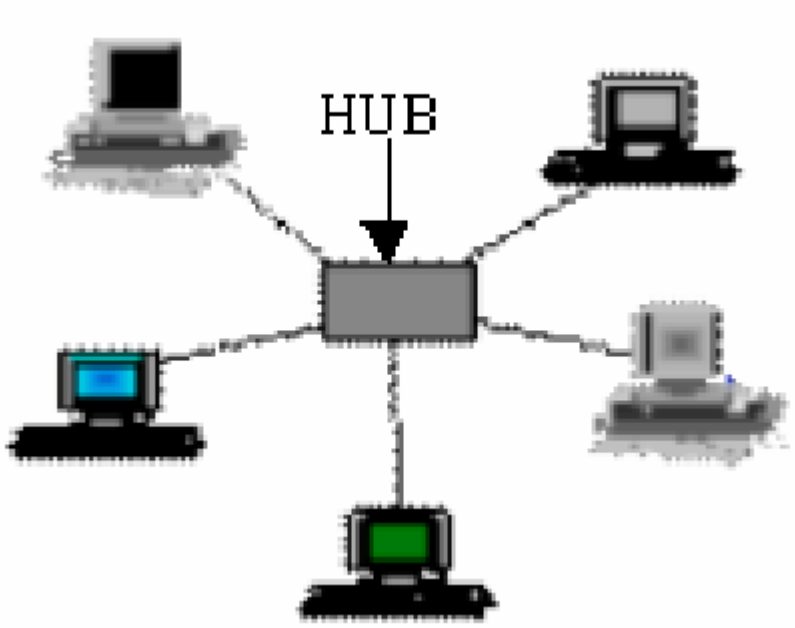
*الشبكة الحلقية



هذا النوع من التصميمات مختلف عن التصميمات الأخرى إذ أنه لا يحتوي على وسط ناقل رئيسي أو جهاز **HUB**بل إنّ كل جهاز في الشبكة يعمل كوسط ناقل للبيانات عن اتصاله بوسطي ناقل أحدهما للجهاز المرسل والاخر للجهاز المستقبل.

وهي شبكة تكون على الشكل الدائري على الأقل من الناحية النظرية حيث تنتقل الإشارات من عقدة إلى عقده أخرى في إتجاه واحد فقط وتتصل كل عقدة مع دتين بشكل مباشر: عقدة ترسل لها وعقدة تسبقبل منها وهي تشارك بشكل فعال في إرسال أي رسالة عبر الشبكة وفي بعض الحالات تقوم بتقوية الإشارة قبل تمريرها إلى العقدة التالية وهي في هذه الحالة عكس شبكة الناقل الخطي. من محاسن هذا النوع انه سهل التركيب ورخيص ومن سلبياته أنه عند حدوث مشكلة يصعب التحديد وإذا انقطع الكابل تتوقف الشبكة بشكل كامل.

* الشبكة النجمية:



هذا النوع من أفضل و أشهر أنواع التصميمات في الشبكات إذ أنه يعتمد بشكل أساسي على جهاز شبكي يسمى المجمع المركزي ال هب(HUB) او السويج (SWITCH) الذي توصل جميع أجهزة الشبكة به بحيث يتم تبادل البيانات عن طريقه.

عند الحاجة إلى زيادة المستخدمين في الشبكة فإننا نستطيع ربط جهازي (HUB) او السويج (SWITCH) مع بعضهما البعض للحصول على عدد أكبر من المنافذ.

ومن اهم حسنات هذا النوع من الشبكات أنه يسهل إضافة أو عزل العقد منه وسهولة تحدد المشكلة اذا حدثت، وعزل أي جزء من الشبكة لا يؤثر على باقي الأجزاء. ومن مساوئ هذا النوع من الشبكات إذاحصل عطل في HUB او السويج (SWITCH) فإن جميع الشبكة سوف تتعطل خلال هذا المقال سوف نستعرض الفرق بين كل من الهب والسويتش واهم المميزات لكل منهم

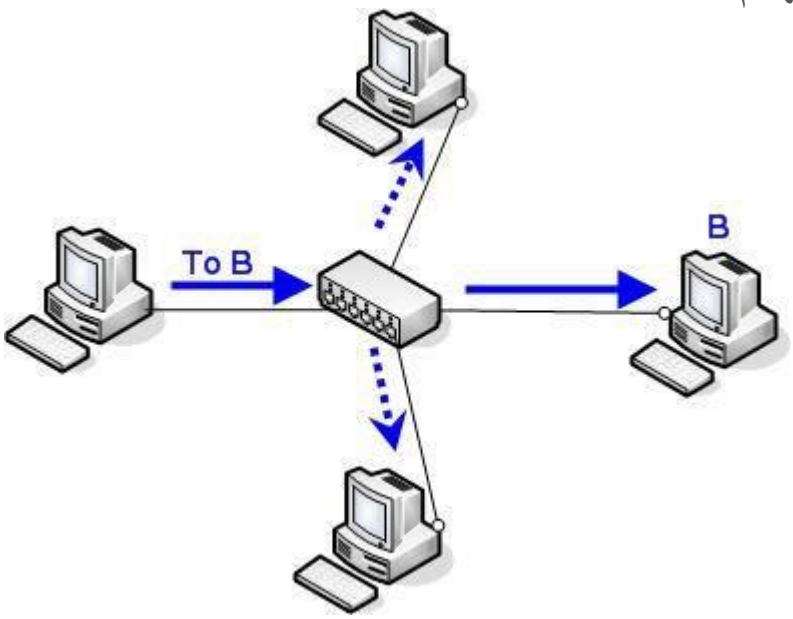
الهب: Hub

هو جهاز شبيه بالسوتش بحيث لا يمكن للمستخدم العادى التفرقة بين الهب والسوتش الا من خلال قراءة المكتوب عليها، وكان يستعمل الهب قديماً لربط الأجهزة مع بعضها فى الشبكة الواحدة وفى الغالب يحتوى على 4او ٨ او ١٦ او ٣٢ فتحة او port ولكن للأسف يعيب الهب أنه جهاز بطىء للغاية ويتعمل مع البيانات وكأنها موجات كهربائية ولا يفهم أى شىء ولا يعرف عنوان IP ويقوم بأرسال البيانات بين الأجهزة فى الشبكة الواحدة بنظام البرو كاست ويسبب فى بطىء الشبكة

كيف يعمل الهب فى الشبكة:

عندما يقوم أى مستخدم بأرسال بيانات داخل الشبكة وليكن من جهاز pc 1 الى الجهاز pc 5 فأن البيانات تمر على كل الأجهزة الأخرى فى نفس الشبكة الى ان تصل الى الجهاز المقصود بدلاً من أرسالها بشكل مباشر كما هو فى السويتش، بالأضافة الى ذلك عندما يقوم الجهاز pc 5 بأستلام البيانات لن يقوم بأرجاعها مرة أخرى الى الهب اما باقى الأجهزة فى الشبكة فى الشبكة تقوم بأرجاع البيانات مرة أخرى الى الهب بهدف أيصالها الى الحهاز المقصود pc 5وذلك لان الهب لا يعرف هل الجهاز أستلم البيانات ام لا وهو عيب أخرى وبهذه الطريقة سوف تستمر عملية ارسال البيانات الى الجهاز المقصود داخل الشبكة بشكل مستمر (أستمرارية مرور البيانات او الداتا داخل الشبكة) ويتسبب فى مشاكل كثيرة فى الشبكة او ما يسمى بأسم loop او موت الشبكة،لهذا يعتبر الهب جهاز غبى جداً مما أدى الى عدم أستمرارة حتى الأن.

هذه صورة تبين طريقة عمل الهب وكيف انه يمرر البيانات الى جميع الاجهزة المتصلة به سواء كانت هذه البيانات تهمها ام لا:



الخط المقطع يبين ان البيانات ذاهبة الى اجهزة لا تهمها البينات وسوف تبدأ بمعالجتها لتكتشف فيما بعد انها ليست موجهة اليها فتهمل الباقي، مما فيه اهدار للوقت ولسعة (Bandwidth) الشبكة.

الخلاصة:
***يوصل ال Hub مجموعة من الاجهزة ببعضها البعض لتكوين شبكة محلية.**
***يقوم بتكرير الاشارة التي تصله عبر منفذ ما ثم يقوم باعادة ارسالها عبر جميع المنافذ الاخرى المتصلة به ما عدا المنفذ الذي اتت منه هذه البيانات، و دون التدقيق في محتواها**
.

الجسر Bridge

يستخدم لتقسيم شبكة محلية كبيرة الى قسمين) يربط بين هبين مثلا ٢ Hubs بحيث كل Hub يربط مجموعة من الاجهزة (وهو اذكى من الهب.. وتم اختراعه لاضافة سعة اضافية للشبكة نأتي لمعرفة كيف ولماذا؟

***معلومة لا بد منها:**

لكل جهاز به كرت شبكة، يوجد عنوان خاص بهذا الكرت يسمى (MAC Address) ويكون هذا العنوان محفوظ بالكرت من المصنع.. وكل كرت له عنوان لا يوجد في اي كرت ثاني (مثل بصمة اليد) لكي يتم تمييز الجهاز عن غيره بعبارة اخرى.. هذا هو عنوان ال Unicast الذي تحدثت عنه سابقا

MAC Address

هو العنوان الفيزيائي أو الثابت أو الحقيقيّ الذي يُعطى للأجزاء الصلبة \ الوسائط المتصلة بالإنترنت أو بالشبكة المحليّة، مثل بطاقة الشبكة، **المودم، الموزّعات والمبدلات الشبكية، بلوتوث، إيثرنت، وايفاي، وغيرها**

وهو اختصار لـ Media Access Control address (عنوان تحكم وصول الوسائط)، ويتكون هذا العنوان من ١٢ خانة ذات أرقام ست عشرية (طولها ٤٨ بت)، ويتم كتابتها في واحد من الصيغتين الآتيتين:

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

ويحتوي النصف الأول من العنوان على رقم تعريفي خاص بالشركة المصنّعة لذلك الوسيط أو الجزء الصلب، وكل شركة لديها رقم تعريفي مخصص في النصف الأول من العنوان يختلف عن الرقم الموجود لدى شركة أخرى، ويتم تنظيم هذه الأرقام التعريفية بواسطة هيئة معايير الإنترنت، وأمّا النصف الثاني من العنوان فيمثّل الرقم التسلسلي الخاص بالوسيط\الجزء الصلب المحوّل\الجهاز، الذي تم تصنيعه.

مثال –:

00:A0:C9:14:C8:29

عنوان ماك أدريس المبيّن أمامك، يوضّح أن هذا الجزء الصلب مصنّع بواسطة شركة إنتل، والدليل هو الرقم التعريفي في Serial الخاص بشركة إنتل، وأما ما تبقى من العنوان فهو رقم تسلسلي A0C9النصف الأول (البادئة) وهو ٠٠ Number لذلك الجزء الصلب.

وبشكل عام، فإن ماك أدريس هو مثل بصمة الـDNA ، إذّ أنه لا يمكن لأي عنوان ماك في العالم أن يتطابق مع عنوان آخر، فمثلا: من المستحيل أن يتطابق عنوان ماك لبطاقة شبكة مع عنوان ماك لبطاقة شبكة أخرى في العالم، فلدى كل واحدة عنوان مختلف

Unicast

(البث فريد الوجهة أو البث الفريد أو البث المنفرد أو البث الأحادي) بالإنجليزية (Unicast) وهوَ مُصطلح مستخدم في شبكات الحاسوب وهو يُشير إلى انتقال واحد لواحد من نقطة مُعينة في الشبكة إلى نقطة أُخرى، وبالتالي هُناك مرسل واحد ومستقبل واحد، وكل مُنهما مُحدد بواسطة عنوان الشبكة

نعود مرة اخرى عندما يرسل اي جهاز اي بيانات خلال الشبكة.. يضع هذا العنوان (Unicast) والخاص بالجهاز المرسلة اليه البيانات، ضمن الفريم المرسل وللاضافة، فهو يضع ال Unicast الخاص به نفسه ايضا حتى يعرف الجهاز الذي سيستلم هذه البيانات الى اي عنوان يرد اذا احتاج ان يرد. (مثلا لماذا عندما تقوم بكتابة www.google.comفي المتصفح مثلا لا تأتي هذه الصفحة لجهاز اخر معك في الشبكة الداخلية؟ لان البيانات العائدة الى الشبكة لديك موجهة لعنوان ال MAC الذي يخص جهازك فقط.. هذا كمثال

هنا يظهر مستوى ذكاء الجسر bridge حيث انه لا يستقبل الاشارة القادمة فقط .. انما يدخل في تفاصيلها حتى يكتشف هذا ال.MAC

و يأتي الجسر بمنفذين فقط غالبا ويستخدم لتقسيم شبكة كبيرة الى قسمين كما اسلفت، ولكن كيف؟

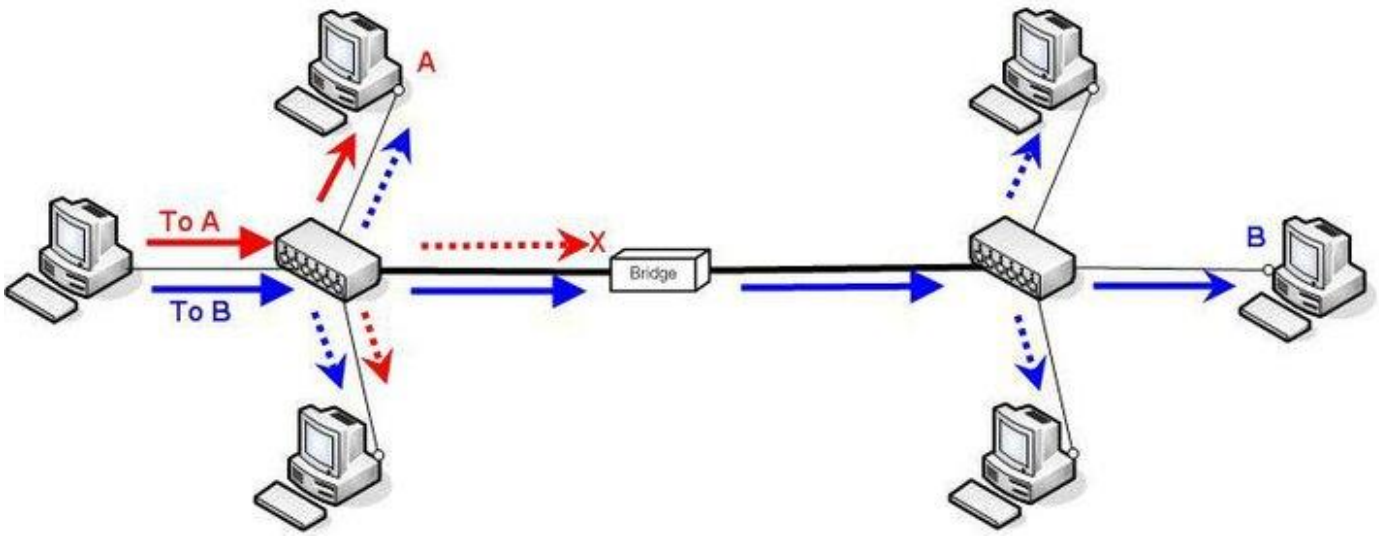
يقوم بعمل جدول يسمى (MAC Table) ثم يقوم بتعبئته قليلا قليلا .. كيف؟

عندما يستقبل بيانت قادمة من خلال المنفذ ١ فيه مثلا، فانه يستخرج عنوان ال MAC للجهاز المرسل (بكسر السين) لهذه البيانات. بهذا يعرف ان هذا الجهاز هو احد الاجهزة الموجودة في الشبكة المتصلة بالمنفذ ١ (ولنسمها الشبكة ١) ويقوم بتخزين هذه المعلومة) الجهاز صاحب ال MAC الفلاني موجود في الشبكة المتصلة بالمنفذ رقم ١ (وبهذا بعد ان تقوم جميع الاجهزة بارسال بيانات يكون الجسر قد عرف تقريبا ماهي جميع الاجهزة الموجودة في الشبكة ١ وجميع الاجهزة الموجودة في الشبكة ٢. وهذه العملية مستمرة ولا تنتهي طبعا، فاحتمال اضافة جهاز جديد بأي شبكة دائما وارد .

الان، وبالنظر الى الصورة ادناه، لنفترض اننا قمنا بارسال بيانات من جهازنا (الجهاز اقصى اليسار) الى الجهازA ، عندما يستقبل الجسر هذه البيانات المرسلة الى عنوان Unicast والذي يخص الجهاز A فانه سوف يستخرج هذا

العنوان من الفريم الذي ارسله جهازنا، ثم يقوم بمقارنته بجدول ال MAC الذي قام بتكوينه، فاذا وجد ان هذا العنوان والذي يخص الجهاز (A موجود مع جهازنا في نفس الشبكة) لان البيانات جائت عن طريق المنفذ ١ وال MAC للجهاز A ايضا في الشبكة المتصلة بالمنفذ ١ (فانه لن يمرر هذه البيانات الى المنفذ ٢ وبالتالي لن تصل الى الشبكة ٢.. لكن عند ارسالنا بيانات الى الجهازB ، فان الجسر سوف يمررها لعلمه ان الجهاز B متصل بالمنفذ ٢ فيه. وهذا هو المنطق الذي يستخدمه الجسر. بسيط لكنه فعال جدا.

عموما، وفي وقتنا الحاضر، فقد انقرض الجسر. وذلك لعدم الحاجة اليه بعد ظهور ال .. Switch فقد كان السبب الرئيسي لاستخدامه هو التقليل من مساوئ ال Hub السابقة الذكر. وبعدم الحاجة لل Hub الان، انعدمت الحاجة للجسر كذلك.
هذه صورة تبين الوظيفة المهمة التي يقوم بها الجسر من اجل تقليل فيضان البيانات الذي لا داعي له بتقسيم الشبكة منطقيا الى قسمين:



لاحظ ان البيانات المرسلة الى الجهاز A تم اعتراضها لان الجسر يعلم ان الجهاز A موجود في نفس الشبكة مع الجهاز الذي ارسل البيانات ولا داعي لتمرير هذه البيانات الى الجزء الاخر من الشبكة.
كذلك لاحظ ان ال Hub في كل شبكة مرر البيانات التي اتته الى جميع الاجهزة الموصولة به سواء همتها هذه البيانات ام لا مما يستهلك Bandwidth لاداعي له.

الخلاصة:

***يقوم الجسر بتقسيم الشبكة منطقيا الى اكثر من قسم لتقليل استهلاك ال bandwidth للشبكة.**

***يقوم الجسر بتمرير البيانات الى المنفذ الاخر فيه في احد الحالات التالية:**

أ- اذا كانت البيانات مرسلة لعنوان ال Broadcast حيث ان هذه البيانات يفترض ان تصل الى جميع الاجهزة.

ب- اذا لم يجد العنوان المرسل اليه في جدول ال MAC الخاص به

ج- اذا وجد العنوان المرسل اليه في جدول ال MAC الخاص به ولكنه في الشبكة الاخرى

-السويتش: switch

عبارة عن جهاز يقوم بربط الأجهزة فى شبكة واحدة lan عن طريق الكابلات ولايمكن لأكثر من جهاز أن يشترك فى بورت واحد،وتتراوح منفذ Port بين ٤ و ٦ و٨ و ١٦و ٣٢ ويقوم بالتعامل مع الأجهزة فى الشبكة عن طريق. MAC address

انواع السويتش:

1 - Ethernet :سرعة الفتحة تصل الى ١٠ mbps

2 - fast Ethernet :بسرعة ١٠٠mbps

3 - gaga Ethernet :بسرعة ١٠٠٠ mbps

كيف يعمل السويتش ؟

على عكس الهب، يعمل السويتش بطريقة ذكية جداً فى نقل البيانات بين الأجهزة داخل الشبكة الواحدة وذلك من خلال انشاء جدول بداخله، وفى أول مرة يتم أرسال بيانات داخل الشبكة ترسل الى جميع الأجهزة فى المرة الاولى فقط الى أن يتعرف السويتش على الأجهزة فى الشبكة وهذا هو أهم فرق بين السويتش والهب.

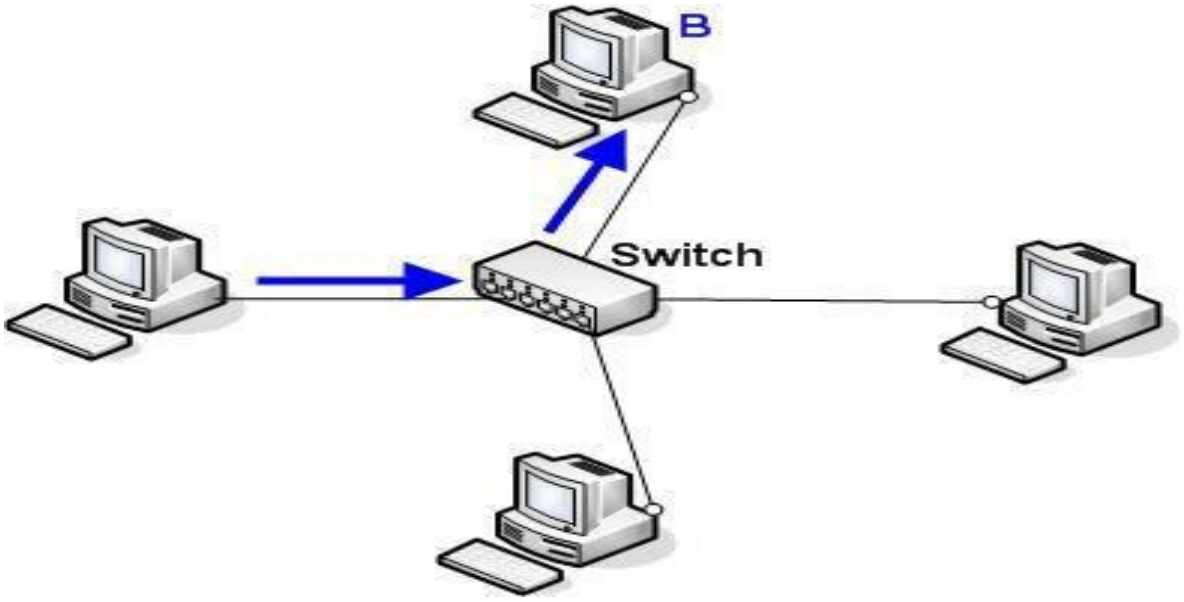
السويتش يستخدم نفس المنطق الذي يستخدمه الجسر. ويكون نفس الجدول (MAC Table) ليحدد بأي عنوان يرتبط كل منفذ.

الفرق بين السويتش والجسر هو عدد المنافذ (Interfaces) حيث يقتصر عددها بمنفذين في حالة الجسر، بينما يزيد عددها عن ذلك بكثير في حالة السويتش ٤ ، ٨ ، ١٦، ٢٤، ٣٢،... .

الان وبما ان السويتش العبقري يعرف تماما باي منفذ يتصل كل جهاز (تعلم ذلك بنفس طريقة الجسر) اصبح الوضع مختلفا، فاذا ارسل جهاز ما بيانت الى جهاز اخر، فان السويتش يوجه هذه البيانات الى الجهاز المعني فقط) بالنظر الى ال Unicast للجهاز المرسل اليه ومقارنته بجدول ال MAC المخزن فيه (دون ازعاج بقية الاجهزة.

طبعا هناك امتيازات اخرى كثيرة جدا للسويتش تتعلق بالامن والسرعة واستخدام الشبكات الافتراضية VLANs وال Full Duplexغيرها لكننا لسنا بصددها هنا) لكنى سأحاول توضيح الفرق بين ال Full Duplex و ال Half Duplex).

هذه صورة تبين كيف ان السويتش لا يبدد اي Bandwidth في الشبكة حيث ان البيانت تذهب الى الجهاز المعني فقط وتكون الشبكة متوفرة لبقية الاجهزة متى ما شائت ارسال اي بيانات.



-الفرق بين hub و switch

الهب يعمل برودكاست، بينما السويتش يعمل بعنوان كارت الشبكة.
الهب ليس له برنامج تشغيل ، اما السويتش فى الغالب له برنامج تشغيل.
الهب يرسل البيانات الى جميع الأجهزة فى الشبكة، السويتش يرسل البيانات الى الجهاز المقصود.
منافذ الـ Hub يتراوح بين ٤ و٣٢ منفذ، بينما عدد منافذ الـ Switch يتراوح بين٨ و٤٨ منفذ.

تكوين شبكة محلية من عدة أجهزة عن طريق السويتش

في المرة السابقة لقد تعلمنا كيف نربط بين جهازين و الإعدادات اللازمة لذلك أما الآن حان الوقت لنتعلم كيف نربط عدت أجهزة ببعض عن طريق السويتش.

المراحل التي سنتبعها في هذا الموضوع:

- كيف نعد كبلات الاتصال
- كيف نربط هذه الأجهزة بالكبلات المعدة
- الإعدادات اللازمة في كل كمبيوتر لنجاح الاتصال

هذا الموضوع يهم كل من لديه اشتراك في الانترنت (ADSL) أو غير ذلك و يود مشاركة أصدقائه أو جيرانه في العمارة ليتقاسموا كلفة الاشتراك و تكون غير مكلفة أيضا. يهم أصحاب مقاهي الانترنت أو من يود فتح مقهى انترنت و كذلك لمن يريد أن يضيف إلى رصيده التعليمي عسى أن ينتفع بها يوما من الأيام

كيف نعد كيبلات الاتصال:

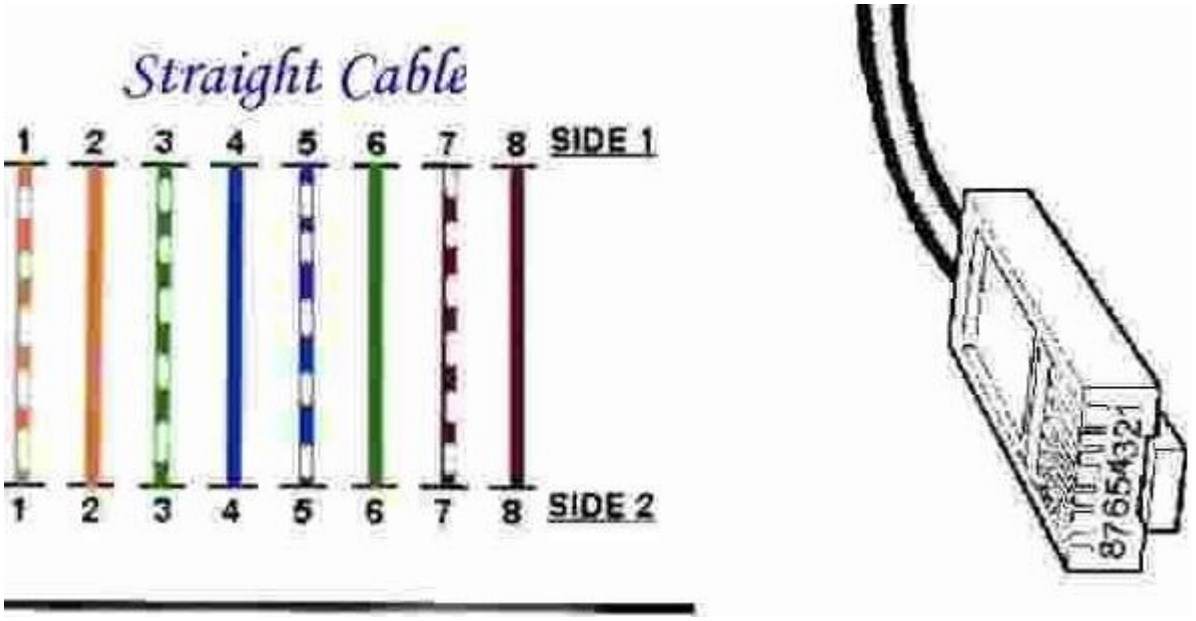
الطريقة سهلة جدا الأشياء اللازمة لذلك كما ذكرنا سابقا:

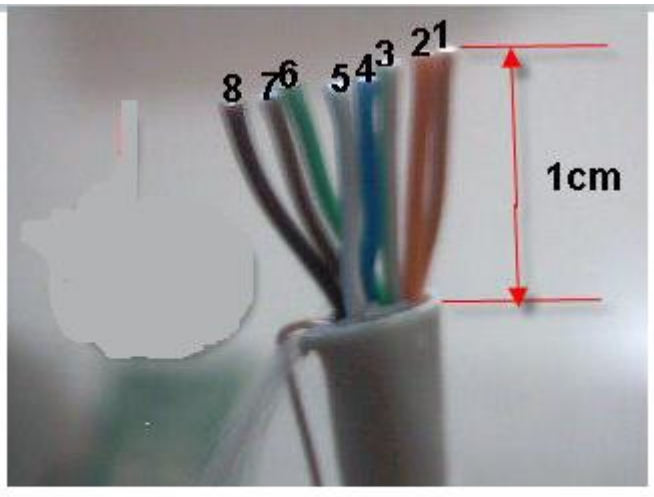
١. كابل من نوع كات ٥ (CATE5)
٢. الأداة (Crimping Tool)
٣. كونك تور (RJ45)

الآن كيفية ترتيب أطراف كابل كآت ٥ يحمل ثمانية أطراف ترتب بطريقة اسمها Straight Cable

1. برتقالي ابيض
2. برتقالي
3. أخضر ابيض
4. ازرق
5. ازرق ابيض
6. اخضر
7. بني ابيض
8. بني

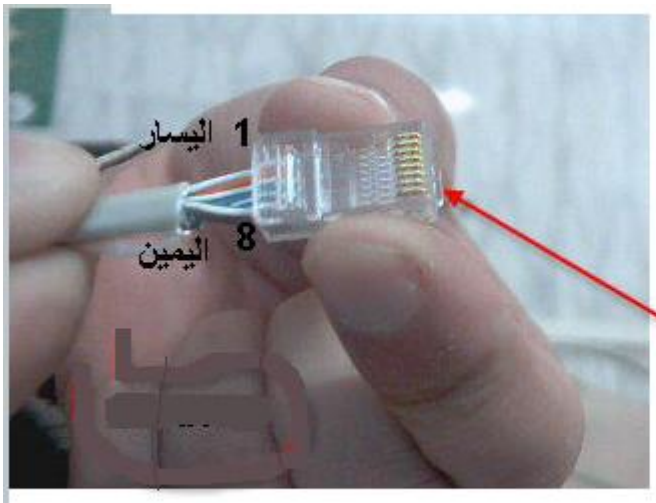
و هذه الصورة التوضيحية لترتيب الأطراف والترتيب يكون من اليسار إلى اليمين:





هذه أطراف الكبل بعد قصها في مستوى واحد و
ظاهرة ب 1 سنتمتر تقريبا
و مرتبة جيدا
يبقى الآن ادخالها في الكونك تور

يجب أن تترك أسلاك الكبل ظاهرة بنحو 1
سنتمتر تقريبا
لقص الأسلاك في مستوى واحد شاهد الصورة



بعد ذلك ندخل الاسلاك في الكونك تور حيث أن داخل الكونك تور توجد لكل سلك مجرى خاص به لذلك ستكون عملية الإدخال سهلة جدا
لكن يجب أن يكون الترتيب من اليسار الى اليمين دائما و يكون رأس الكونك تور الى الاسفل لاحظ الصورة جيدا

اليسار و اليمن بالنسبة اليك

بعد ذلك يأتي دور أداة(كري مبين تول) لقد تعرفنا على هذه الأداة في المرة السابقة لمن فاته قراءة الموضوع نقول له زر هذا الرابـــــــط حتى تستطيع الفهم معنا الآن (في تثبيت الكبل في ألكونك تور تابع الصور جيدا:

بعد ذلك ندخل الكونكتور داخل الفتحة الخاصة به في
Crimping Tool
و نضغط بقوة متوسطة حتى نسمع صوت خفيف يدل على إطباق الكونك تور على الكبل ملا حظة احنا أدخلنا الاسلاك بدون أن نقشرها لماذا لأن التقشير هذه من و ظيفة
Crimping Tool
حيث عند الضغط تقوم شفرات خاصة موجودة في الأداة على تقشير الأسلاك من البلاستيك لتلامس صفائح النحاس في الكونك تور أرجو أنكم فهمتم الشرح

ويكون الطرف الثاني بنفس الطريقة ، ونعمل الكيبلات على عدد الحاسبات التي سوف تربط بالشبكة ، اي لكل حاسبة كيبل

كيف نربط هذه الأجهزة بالكبلات المعدة

نفرض أننا نريد أن نربط ثمانية أجهزة ببعض في هذه الحالة يجب أن يكون لدينا سويتش بثمانية منافذ مرقمة المنفذ الأول رقم واحد نربط به الجهاز الأول الذي سيكون هو السيرفر الذي يزود الانترنت للأجهزة الأخرى و المنفذ الثاني نربط به الجهاز الثاني و هكذا.....
عند الانتهاء بربط جميع الأجهزة بالسويتش نكون مستعدين للمرحلة التالية.

الإعدادات اللازمة في كل كمبيوتر لنجاح عملية الاتصال

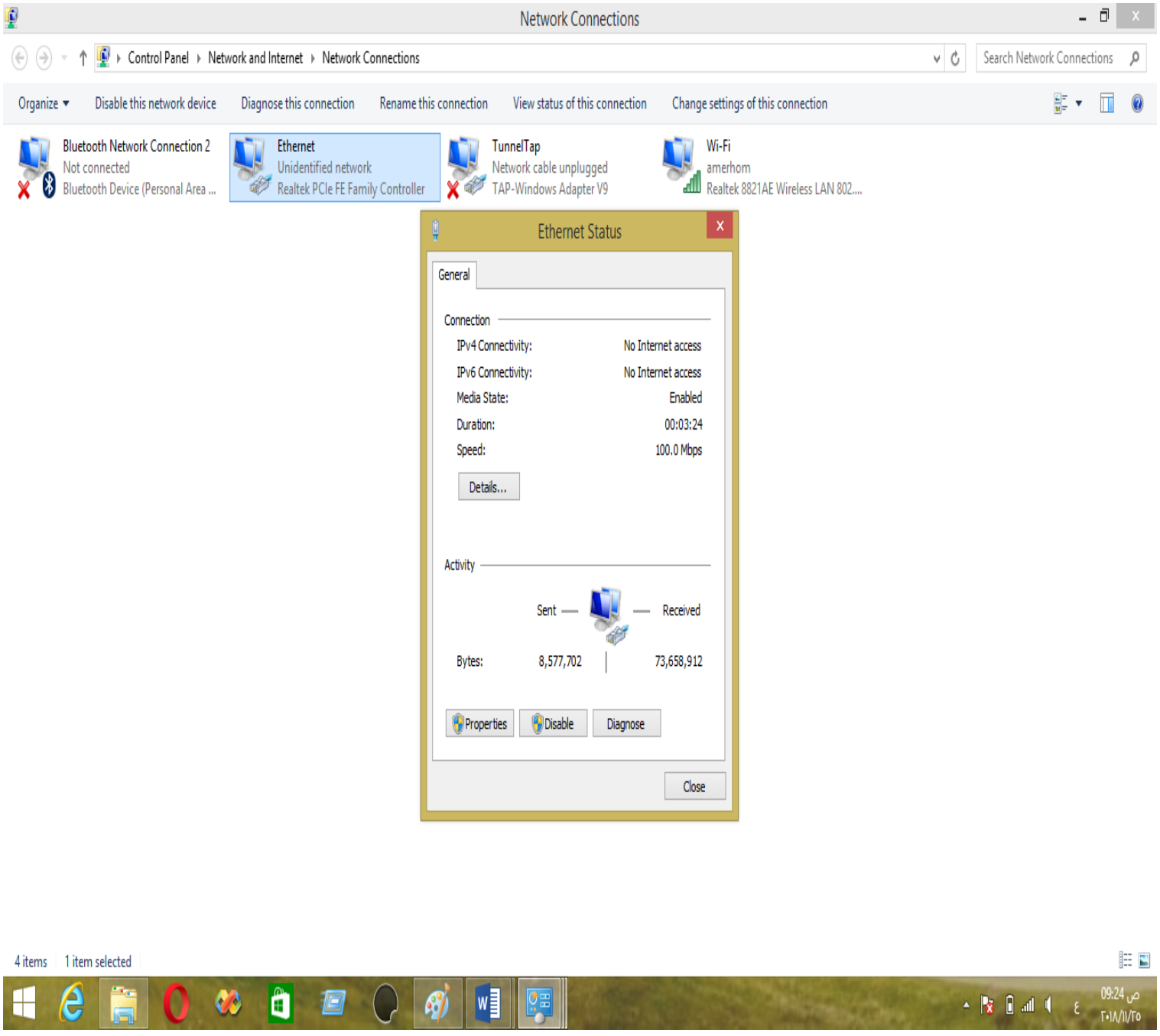
١- نذهب الى ايقونة control panel الموجودة في سطح المكتب ونضغط عليها

٢- فتظهر لنا نافذة نختار منها Network and sharing center

٣- تظهر لنا نافذة نختار منها change adapter setting

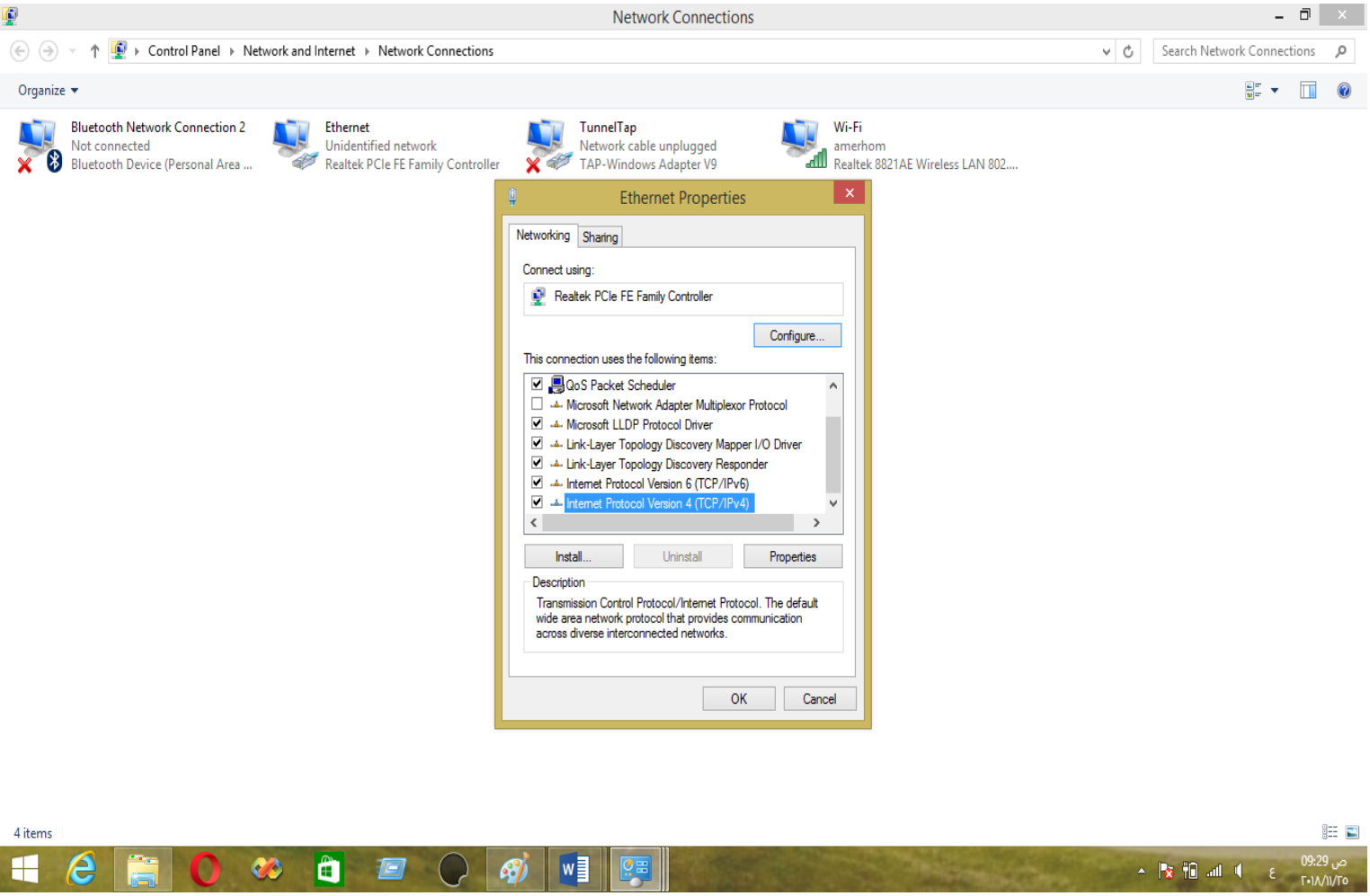
٤- تظهر لنا نافذة نختار منها Ethernet اذا كان الربط بواسطة الكيبلات ، او تختار Wi-Fi اذا كانت الشبكة لاسلكية بواسطة الانترنيت مع الاخذ بنظر الاعتبار اذا توقفت الانترنيت فان الشبكة المحلية سوف تتوقف .

٥- تظهر لنا نافذة بالشكل التالي



٦- نختار منها properties

٧- تظهر لنا النافذة التالية



٨- نؤشر على Internet protocol version 4 (TCP/Pv4) ونظغط على Properties

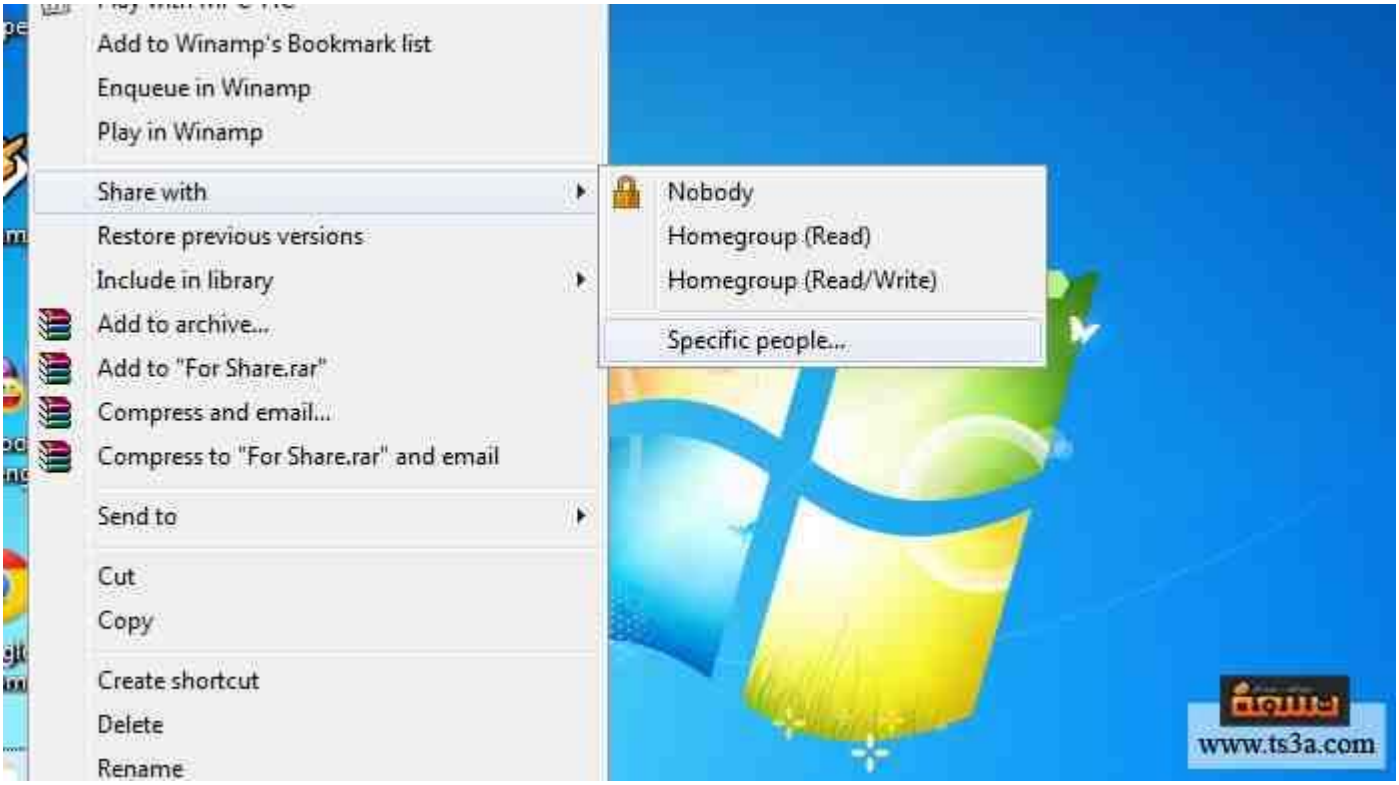
٩- تظهر لنا النافذة التالية ونقوم بادخال المعلومات كما مبين فيهابالنسبة للايبيات ورقم الحاسبة الاولى التي اخذت الرقم ١ في المربع الاخير في اقصى اليمين

١٠- تكرر العملية بالنسبة للجهاز الثاني ونضع ٢ بدلا من ١ وبنفس الايبيات ثم ٣ للجهاز الثالث .....الى اخر جهز وليكن مثلا ٨

١١- نضط على ok تظهر لنا النافذة السابقة ثم نخرج

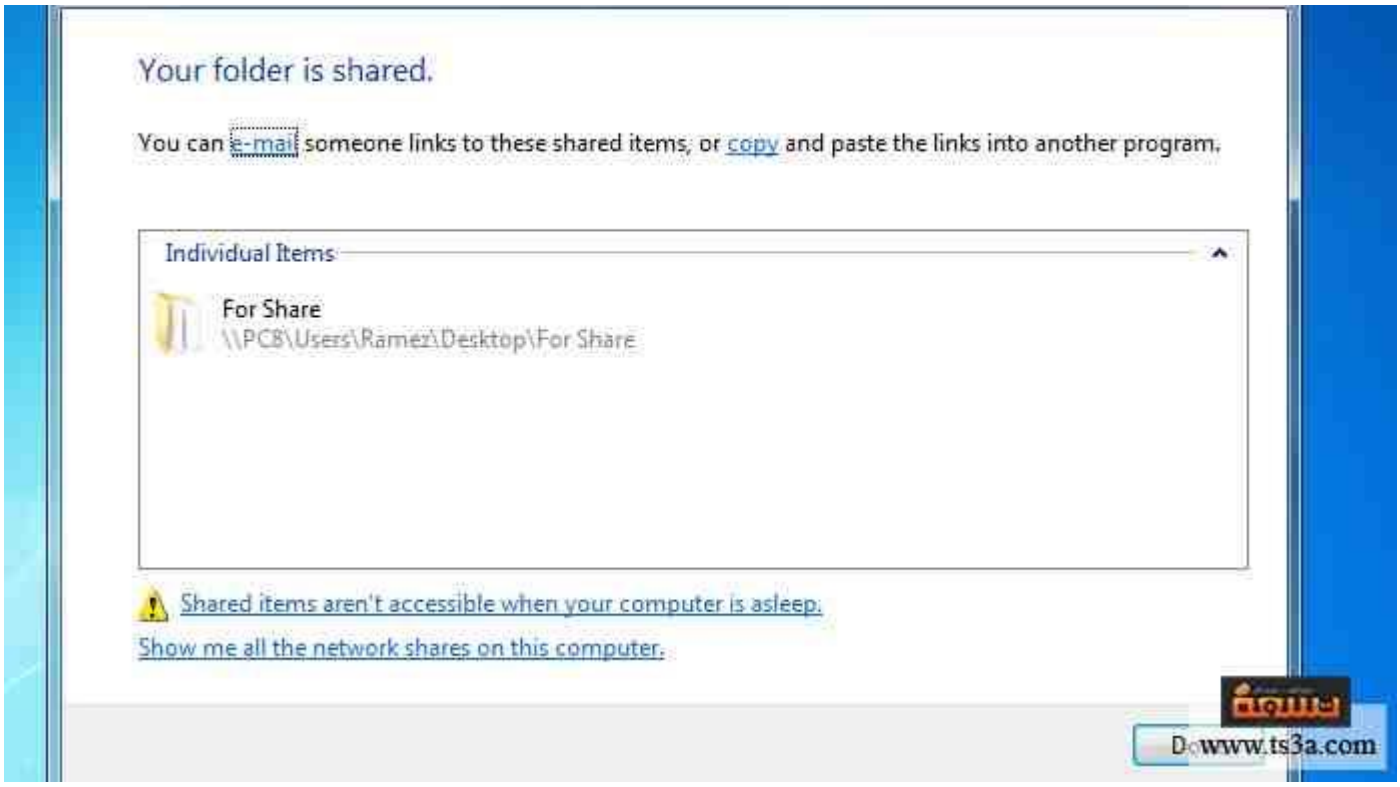
١٢- الان نذهب الى النافذة التي سبقف وان اخترنا منها change adapter setting ونختار من تحتها المدخل change advanced sharing setting فتظهر لنا نافذة نجعل جميع مداخلها on وفي اسفل النافذة نختار الاختيار Turn off password protected sharing ثم نظغط على save changing

١٣- بعد أن قمنا بضبط إعدادات الـ Network نذهب إلى الملف المراد مشاركته وليكن الملف الذي على سطح المكتب نذهب إليه ونضغط على الزر الأيمن للفأرة ونختار Share With ثم Specified People كما هو موضح في الصورة.

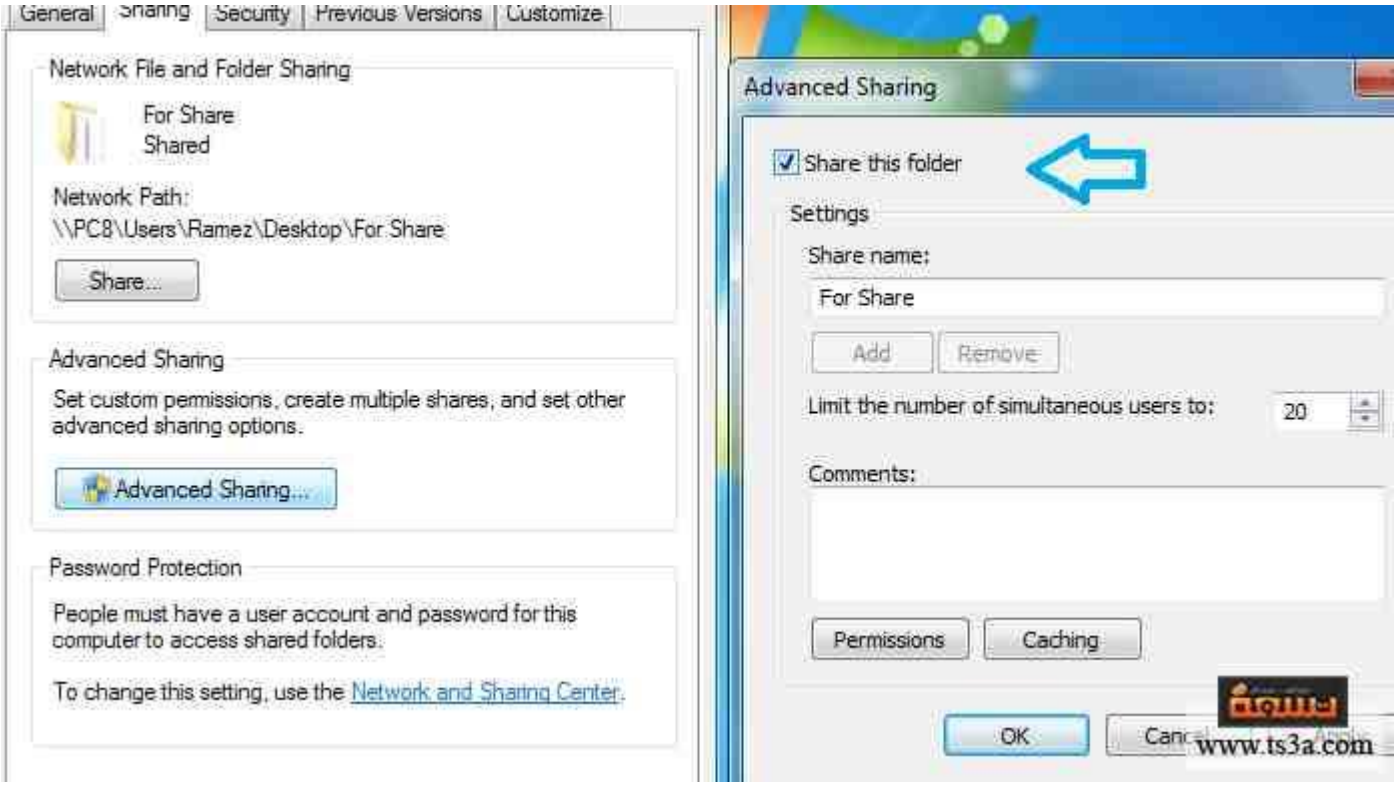


١٤- . سوف تظهر لنا قائمة نختر Everyone ثم Add كما هو موضح بالصورة .

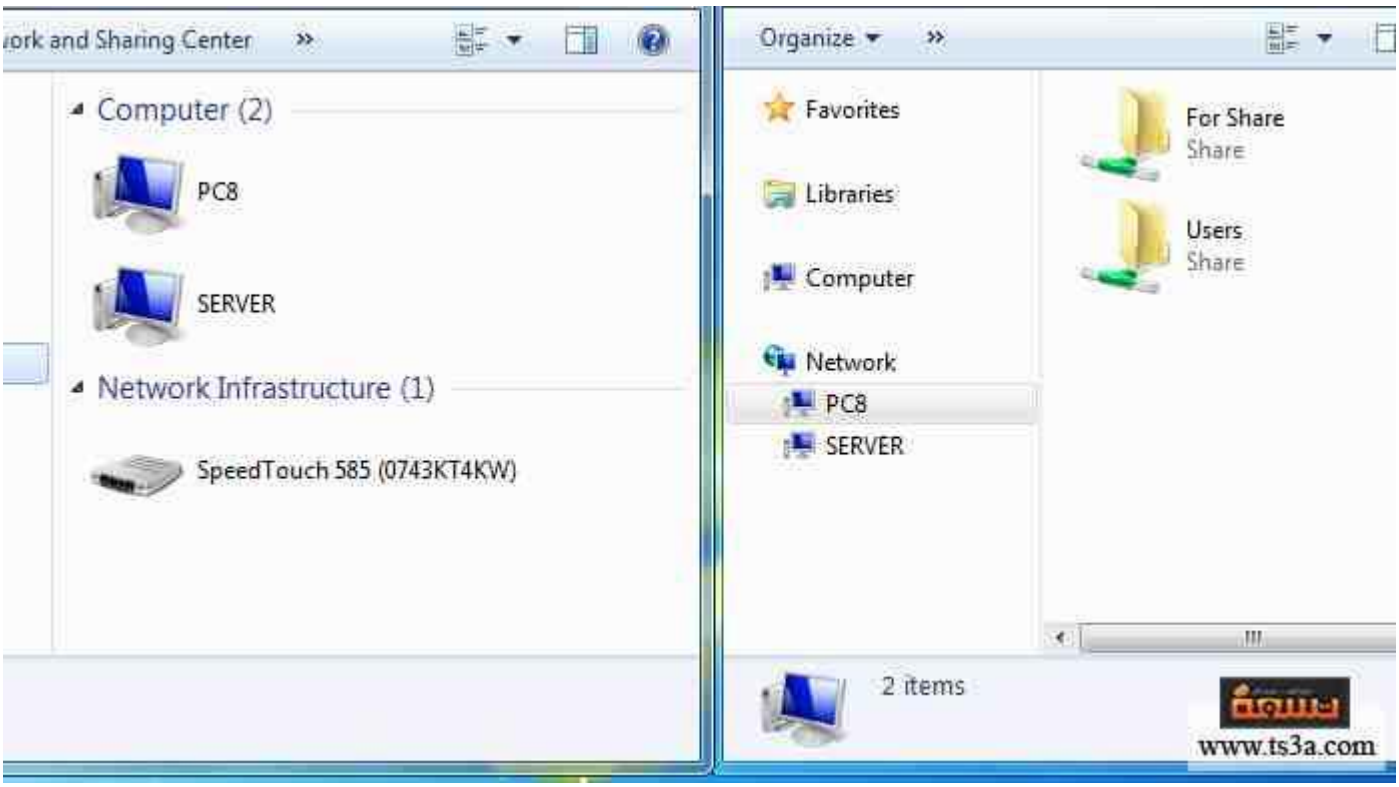
١٥- بعد ذلك سنجد قائمة على يمين خيار Everyone وهي Read بمعنى قراءة الملف فقط و Read/Write ومعناها قراءة الملف والتعديل فيه أيضاً والخيار الأخير Remove أي حذف، اختر المناسب لك ومن الأفضل إذا كنت تريد المحافظة على ملفك من تعديل أي شخص فأختر Read ثم أختر Share كما هو واضح بالصورة هكذا قاربنا على إتمام معرفة كيفية مشاركة الملفات.
ستظهر قائمة تأكيد بأن الملف قد تم مشاركته ما عليك إلا اختيار Done فقط .



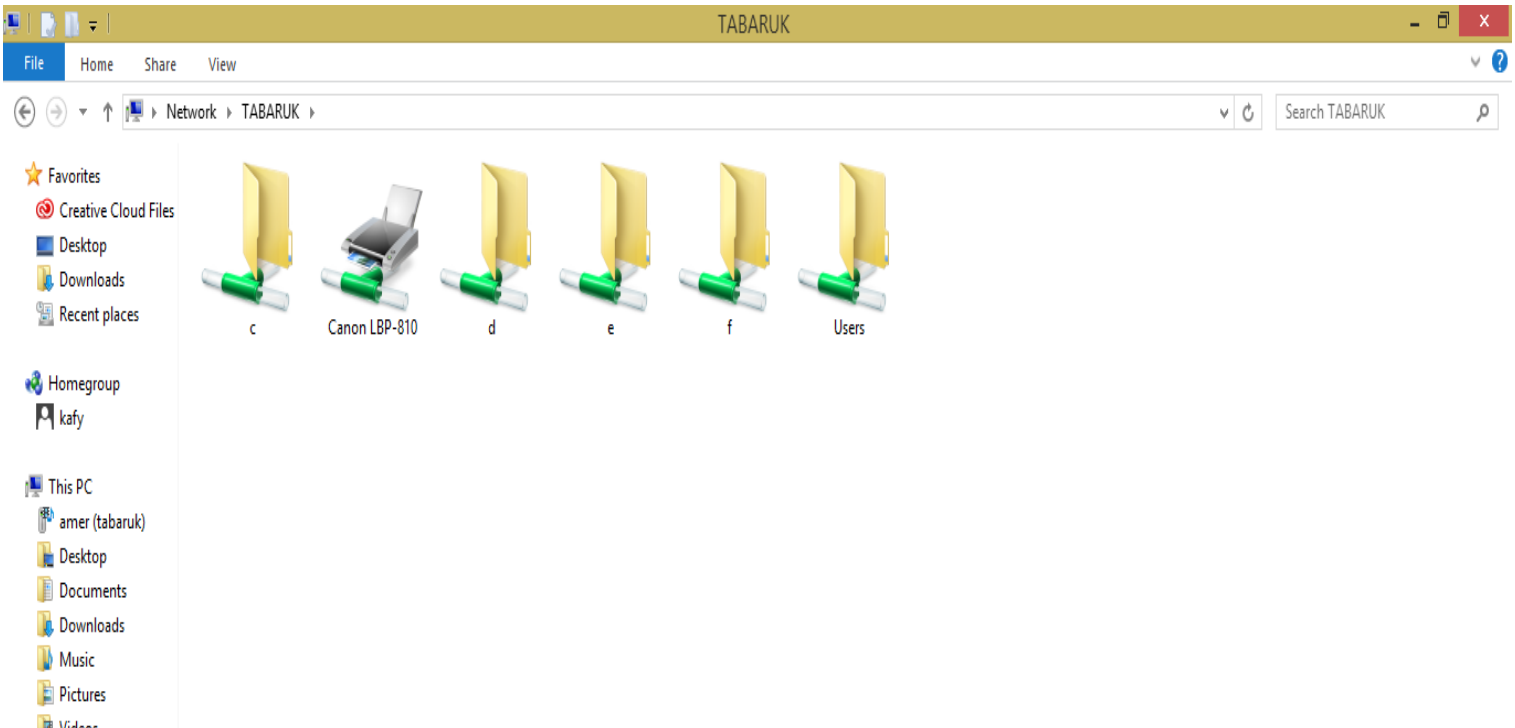
١٦- أخيراً للتأكد من أن الملف تم مشاركته نذهب للملف ثم نضغط على الزر الأيمن للفأرة ثم نختر **Properties** ثم نختر **Advanced Sharing** ستظهر قائمة يجب أن تأكد من وجود علامة على **Share This Folder** كما هو موضح بالصورة.



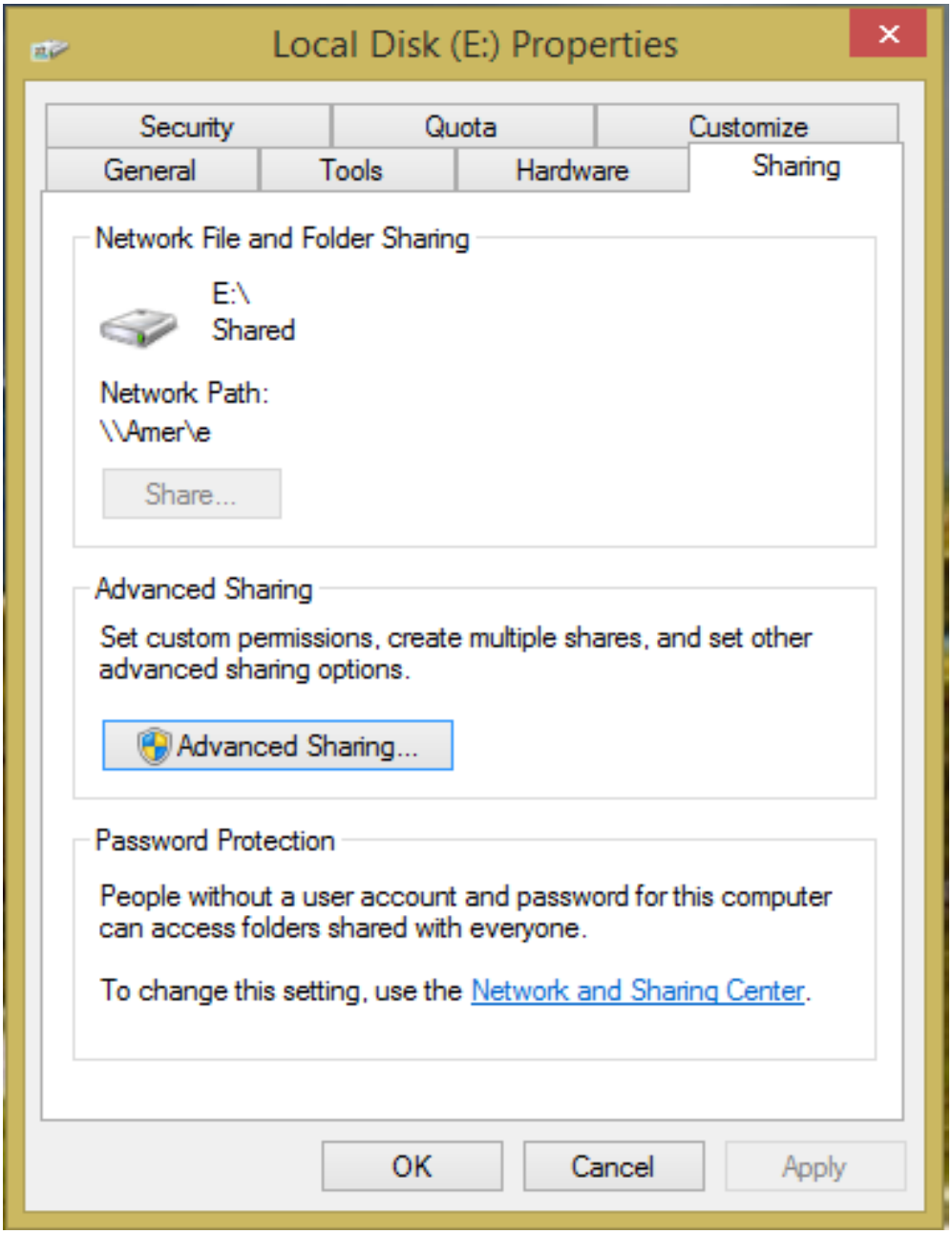
أما إذا أردنا رؤية الملفات المشاركة من أجهزة أخرى بطريقة بسيطة سنذهب إلى **Network** ستظهر لنا الأجهزة المجاورة وما تشارك به، وسنجد أيضاً الملف الذي قمنا بمشاركته مع باقي الأجهزة المجاورة كما هو مقسم في الصورة .



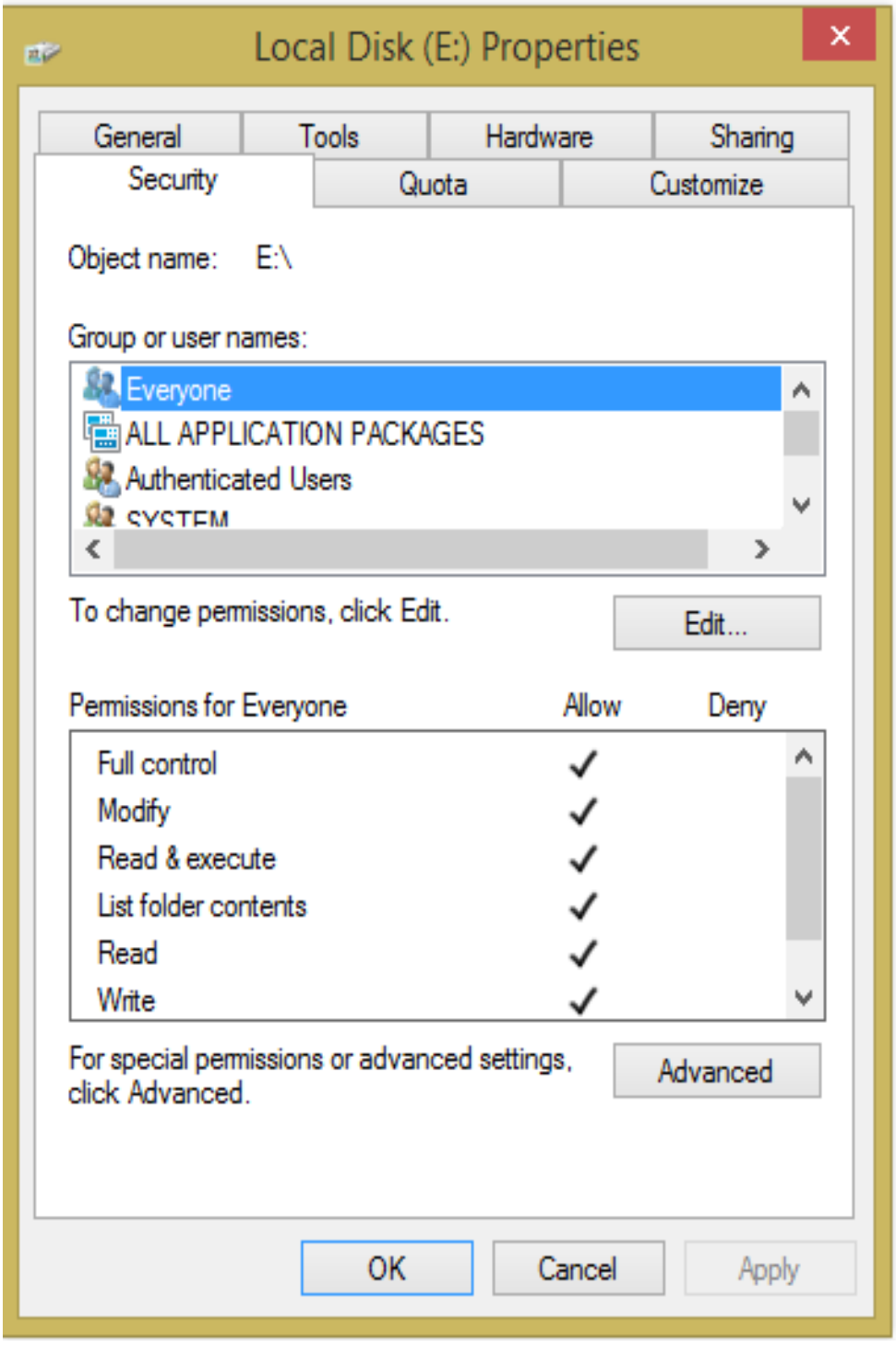
او ربما هذه الصورة التي تعني مشاركة القرص الصلب للخادم بكافة بارتشناته ومشاركة كافة الحاويات والملفات مع الاخذ بنظر الاعتبار الصلاحيات المعرفة مسبقا من قبل مسؤل الشبكة اي قراءة فقط او قراءة وتعديل او..... الخ



هذة النافذة تدل على ان الدرافير E انه مشارك بكافة محتوياته



هذه النافذة لتنظيم الصلاحيات **permission**



امن الشبكات

أساسيات أمن الكمبيوتر Computer Security Basics:

التهديدات(*Threats*) :

أي حدث أو فعل من المحتمل أن ينتج انتهاك للسياسات أو الإجراءات الأمنية. سواء كان مقصود أو غير مقصود ، خبيث أو غير ذلك ونها :.

- **الوصول غير المقصود أو غير المخول لتغيير البيانات .**
- **انقطاع الخدمة .**
- **انقطاع الوصول إلى المصادر.**
- **الدمار في المعدات .**
- **الوصول غير المخول أو تدمير المرافق .**

مثال : إرسال بريد الكتروني يحتوي معلومات حساسة بالخطأ لشخص غير معني يعتبر تهديد ، على الرغم من أنه توجيه خاطئ غير مقصود .

نقاط الضعف (*Vulnerabilities*) :

أي ظرف يترك النظام عرضةً للهجوم ، ويتضمن أشكالاً عديدة :

- الثغرات في البرمجيات ونظم التشغيل
- الاستخدام السيئ لبرمجية أو بروتوكول اتصال
- التصميم الضعيف للشبكة
- الأمن الفيزيائي الضعيف
- كلمة مرور غير آمنة
- إدخال مستخدم دون التحقق من الهوية
- عيوب التصميم في البرمجيات ونظم التشغيل

مثال : إعداد router ليسمح بمرور كلي من الانترنت إلى LAN يعتبر نقطة ضعف .

المخاطر (Risks) :

مؤشر لفرصة التعرض لتدمير أو فقدان ، وفي نظم المعلومات هو مرتبط بفقدان النظام، الطاقة، الشبكة ، والخسائر الفيزيائية . كذلك فهو يؤثر على البشر،الممارسات ، العمليات .

مثال : الموظفون السابقون الساخطين من الممكن أن يشكلوا خطراً كبيراً في حال الوصول إلى البيانات في عملهم السابق ومن الممكن أن يزيلوها !!!

عوامل الأمن *Security Factors* :

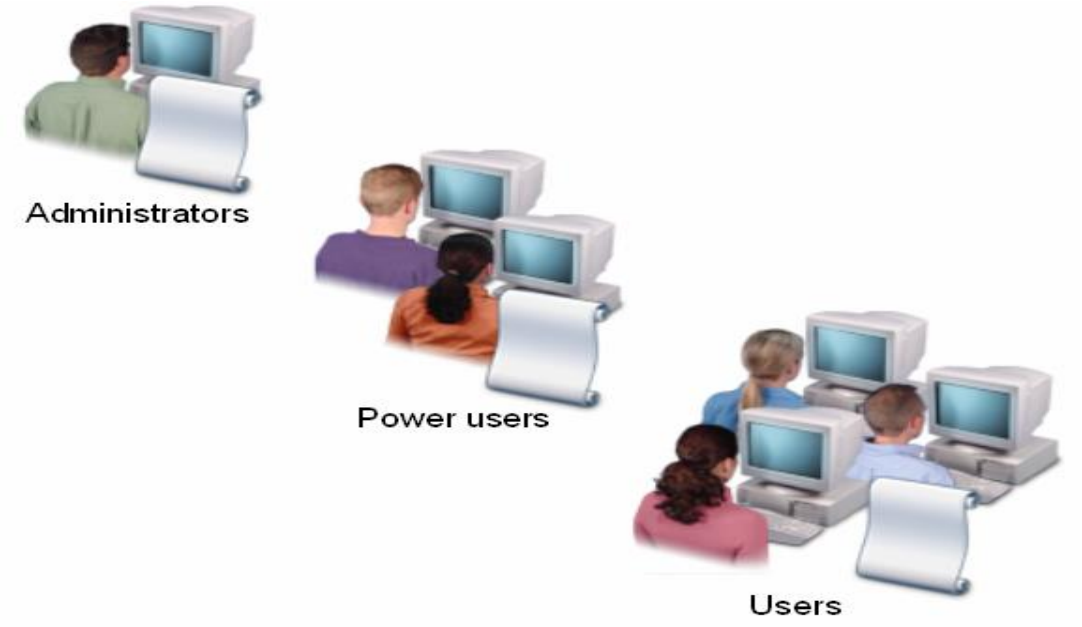
معظم أنظمة الأمن تعتمد على أربعة عوامل رئيسية لتحقيق أهداف الأمن :

- **المصادقة *Authentication* : هو عملية تعريف فريد لفرد معين أو كيان .**
- **الترخيص *Authorization* : عملية تحديد ما هي الحقوق والامتيازات التي يمتلكها كائن معين .**
- **التحكم بالوصول *Access Control* : عملية تحديد وتعيين الأذونات للموارد المتعددة ، والأغراض والبيانات**
- **المراجعة أو المحاسبة *(Auditing or accounting)* : عملية تتبع أو تسجيل فعاليات ونشاطات النظام والوصول إلى الموارد**




مبدأ الامتيازات :

يملي هذا المبدأ على أن المستخدمين والبرامج يجب أن يملكوا الحد الأدنى من الوصول الضروري لهم لإنجاز واجباتهم والمهام المطلوبة منهم . يتضـــمن المرافق ، معدات الحاســـوب ، البرمجيات ، المعلومات . الأذونات التي تمنح للمستخدم عند الحاجة ، ومن ثم إبطالها عند انتهاء إنجازه للمهمة التي تحتاج هذه الأذونات حيث نلاحظ في الصورة ثلاث مستويات (رجال الادارة،مستخدمين ذو صلاحية خاصة ، ومستخدمين ذو صلاحيات محددة).

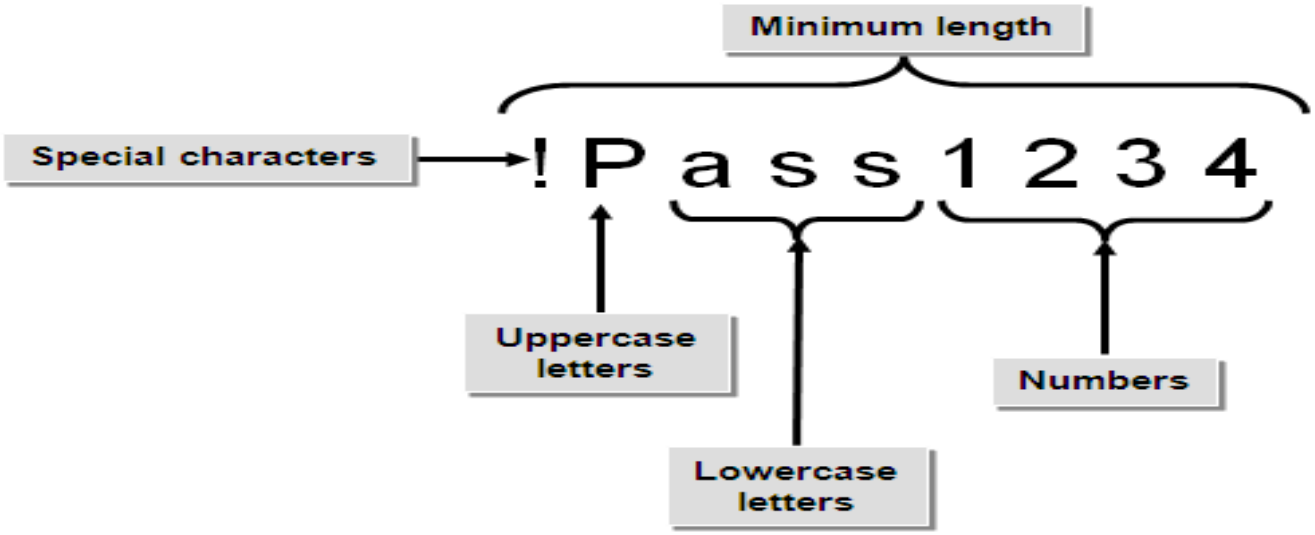


مبدأ كلمة المرور القوية *Strong Passwords*

هي كلمة المرور التي تحقق المتطلبات المعقدة الموضوعة من مسؤول النظام System administrator وموثقة في السياسة كلمة المرور Password policy .كلمة المرور القوية تزيد من أمان النظام وتقلل من احتمالية تخمين كلمة المرور والكشـــف عنها .

متطلبات كلمة المرور القوية :

- **تحديد أقل طول لكلمة المرور .**
- **تتطلب الحروف ، تركيبة من الأحرف اي كبيرة وصغيرة، الأرقام والرموز .**
- **منع استخدام سلاسل الحروف مثل اسم المستخدم وكلمات القاموس او حرف مجاور الى حرف ضمن الكيبورد.**



تشفير البيانات Data Encryption :

ما هو التشفير أو التعمية *Cryptography*

التشفير هو العلم الذي يستخدم الرياضيات للتشفير وفك تشفير البيانات. التشفير يُمكّنُك من تخزين المعلومات الحساسة أو نقلها عبر الشبكات غير الآمنة- مثل الإنترنت- وعليه لا يمكن قراءتها من قبل أي شخص ما عدا الشخص المرسل لـــه. وحيث أن التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات، فإن تحليل وفك التشفير (*Cryptanalysis*) هو علم لكسر و خرق الاتصالات الآمنة.

أهداف التشفير:

١. السرية أو الخصوصية (Confidentiality) :

هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.

٢.تكامل البيانات (Integrity) :

وهي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.

٣.إثبات الهوية (Authentication) :

وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم).

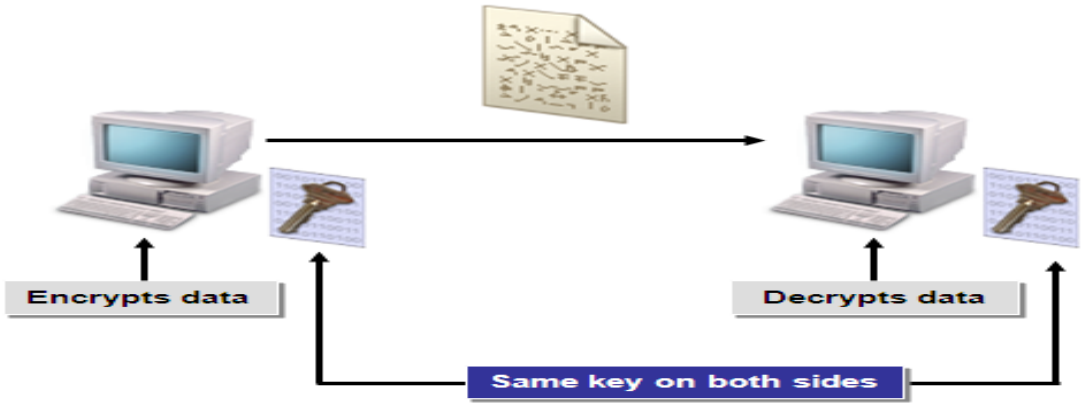
إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات للأشخاص ليتم الحفاظ على أمن معلوماتهم.

أنواع التشفير :

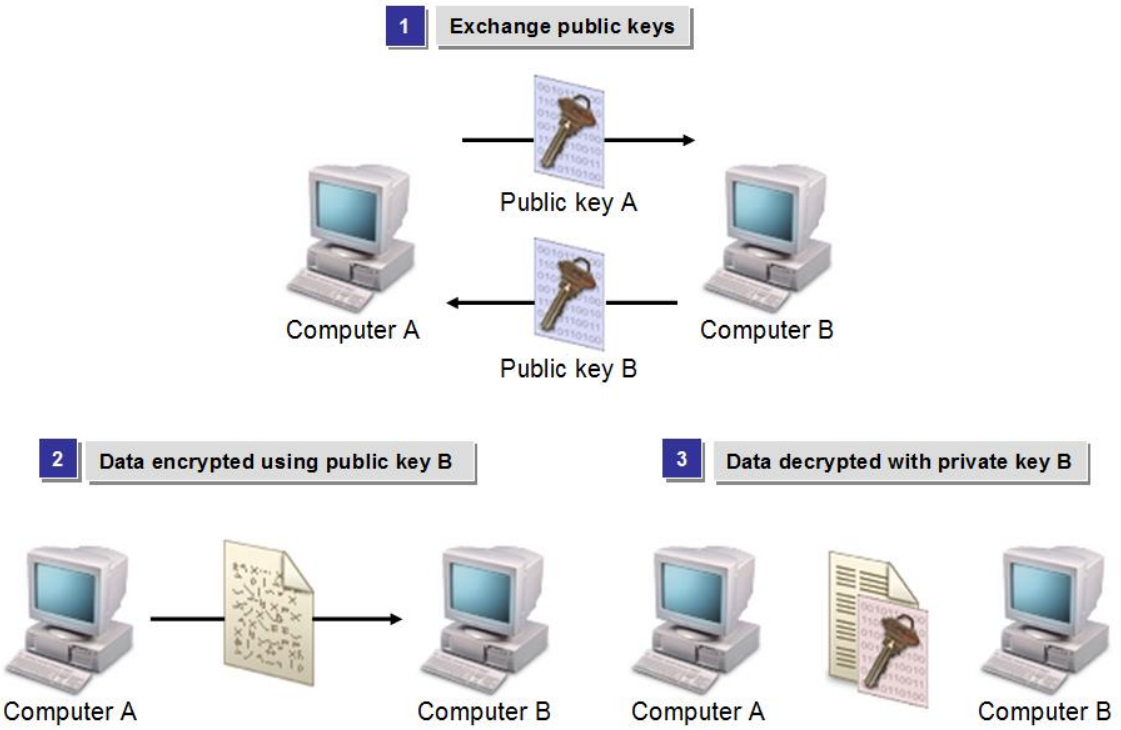
حالياً يوجد نوعان من التشفير وهما كالتالي :

١. التشفير التقليدي. (*Conventional Cryptography*) (المفتاح المشترك / المتماثل)

نفس المفتاح يستخدم للتشفير والتحليل للرسالة. المفتاح الآمن يجب أن يكون موصولا بأمان بين الطرفين المتصلين.



٢. تشفير المفتاح العام. (*Public Key Cryptography*) (زوج المفاتيح/ الغير متماثل) كل طرف يمتلك مفتاحين ، مفتاح عام.أي شخص يستطيع الحصول عليه ، ومفتاح خاص ، معروف بشكل فردي وخصوصي فقط.أي شخص يستخدم المفتاح العام لتشفير البيانات: فقط الحامل للمفتاح الخاص المرتبط يستطيع فك تشفيرها .



الأمن المحلي Local Security :

أحد مكونات الخطة الأمنية الشاملة هو تطبيق الأمن على الشبكة المحلية ، في هذا الموضوع سنتعرف على مكونات الأمن في الشبكة المحلية .

إذا كانت مؤسستك تهتم بأمن المستخدمين ، الأنظمة ، البيانات ،الاجهزة وغيرها. يجب تطبيق عدة مستويات آمان على مكونات الشبكة المختلفة ، يجب تأمينها من الداخل للخارج كذلك الأمر من الخارج إلى الدخل .

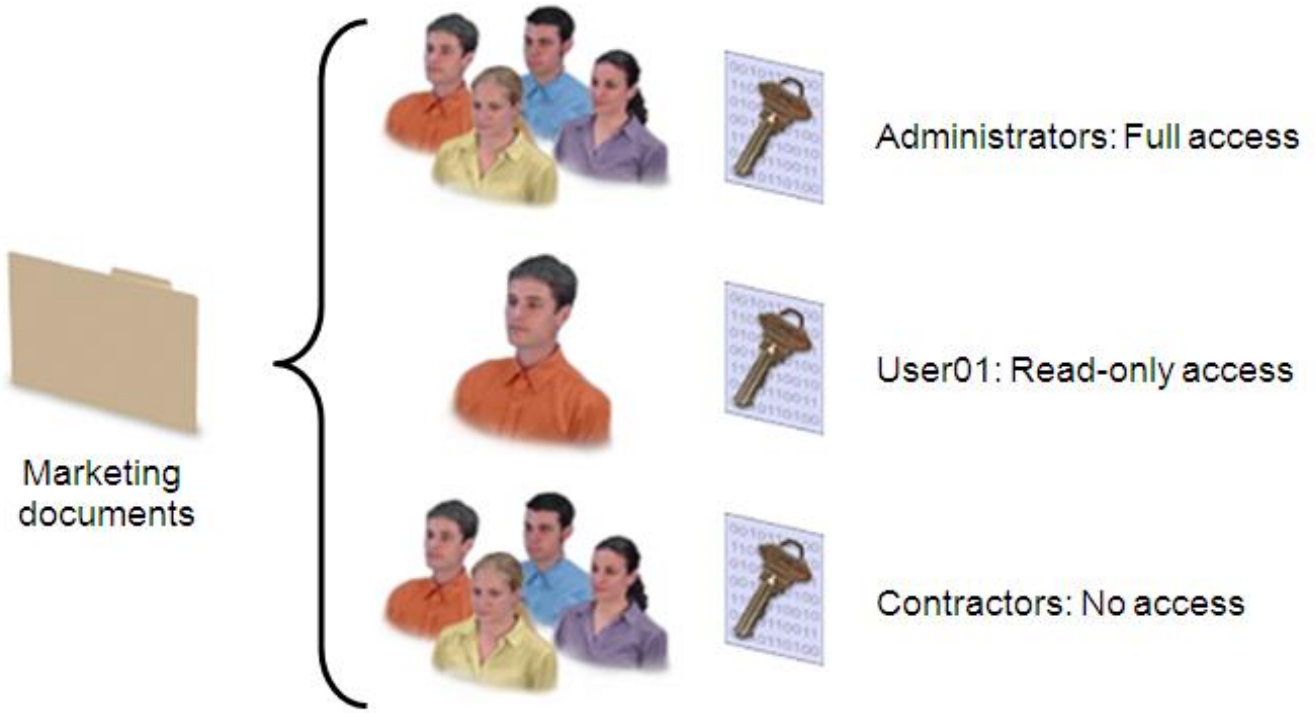
الأمن على مستوى المشاركة و على مستوى المستخدم *Share-Level and User-Level Security* :

في الامن على مستوى المشاركة أي مستخدم يمتلك معلومات المصادقة (عادة كلمة المرور) .اي إذا تعرضت كلمة المرور للخطر ، يجب إعادة إنشاؤها " تغييرها " ومن ثم إعادة توزيعها على المستخدمين الشرعيين .

في الامن على مستوى المستخدم ، جميع إعدادات الأمن ، الحقوق ، الأذونات ترتبط مع حسابات مستخدمين محددة ، عند مصادقة المستخدم فإن النظام يبني وحدة تحتوي ملف تعريف أمان المستخدم ، ثم ، نظام تحكم الوصول يتحقق من محتوى الوحدة ليحدد فيما إذا كان يحق للمستخدم الوصول للمغلومات المعينة أم لا ، والامن على مستوى المستخدم حل محل الامن على مستوى المشاركة في العديد من تطبيقات الشبكة .

الأذونات Permissions:

هي إعدادات الامن التي تحدد مستوى الوصول الذي يملكه حساب المستخدم أو المجموعة . الأذونات من الممكن أن ترتبط بموارد متنوعة ، مثل الملفات ، الطابعات ، مجلدات المشـــاركة ، دليل شـــبكة قواعد البيانات ، الأذونات عادة تستطيع تكوينها للسماح بمستويات مختلفة من الامتيازات أو رفض الامتيازات للمستخدمين الذي لا يحق لهم الوصول .



أذونات ملفات ومجلدات NTFS :

يمكنك ضبط أذونات ملفات ومجلدات NTFS من خلال علامة التبويب أمان من مربع حوار خصائص للملف أو المجلد ، الأذونات القياسية للملفات والمجلدات تتضمن القراءة، الكتابة ، القراءة والتنفيذ ، التعديل ، والتحكم الكامل . الجدول التالي يصف الأذونات بشكل أكثر تفصيل .

أذن المجلد	يمكنك من
Read (R)	**عرض بيانات المجلد ، خصائص ،المالك ، الأذونات**
Write (W)	**الكتابة على المجلد ، الإضافة ، قراءة وتغيير خصائصه**
List Folder Content (L)	**عرض بيانات المجلد ومن الملفات في المجلد ، عرض الخصـائص ، المالك ، الأذونات ، تنفيذ الملفات داخل المجلد أو البرامج المرتبطة فيها ، يورث سرد محتويات المجلد للمجلدات وليس للملفات ، ويظهر فقط عند عرض أذونات المجلد**
Read & Execute (RX)	**مماثل سرد محتويات المجلد إلا أنه يورث للملفات والمجلدات**
Modify (M)	**القراءة ، الكتابة ، التعديل ، التنفيذ للملفات في المجلدات ، تغيير الخصـائص للمجلدات أو الملفات بداخله**

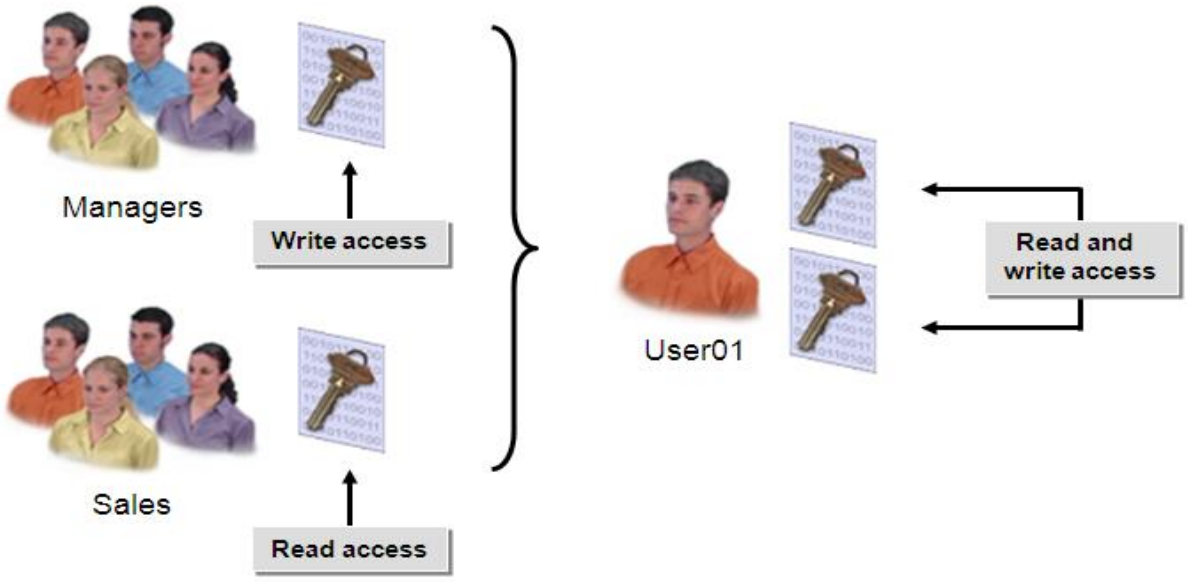
Full Control (FC)	القراءة ، الكتابة ، التعديل ، تنفيذ الملفات في المجلدات ، تغيير الخصـــائص والأذونات ، أخذ ملكية المجلد أو الملفات التي بداخله

أذونات خاصة Special Permissions :

كذلك يدعم الويندوز أذونات خاصة ، التي تقسم الأذونات القياسية إلى وحدات منفصلة وتسمح بالتحكم الدقيق لمن يسمح له لتنفيذ إجراءات معينة على الملفات والمجلدات ، أنت تستطيع تخصيص ملكية الأذونات بناءاً على احتياجات معينة لمنظمتك ، هناك بشكل افتراضي ١٤ إذن خاص يمكنك مزجها ومطابقتها .

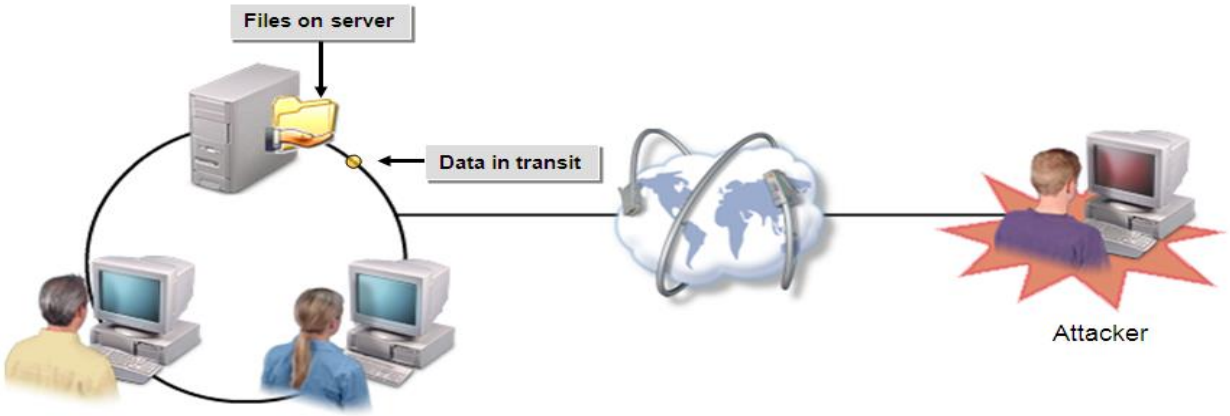
أذونات فعالة Effective Permissions :

الأذونات تراكمية ، هذا يعني أنه عند عضوية المستخدم بأكثر من مجموعة وكل واحدة منها لديها أذونات للموارد ، فإن أذونات المستخدم الفعالة الكلية هي تجميع من جميع الأذونات المنفصلة المعينة .



سرقة البيانات Data Theft :

هجوم يتم من خلاله دخول غير مرخص للحصول على معلومات الشبكة المحمية . المهاجم من الممكن أن يستخدم اعتمادية مسروقة للدخول على الخادم وقراءة البيانات المخزنة على الملفات . أو ، سرقة البيانات أثناء انتقالها خلال وسائط الشبكة باستخدام "packet sniffer – based – or software- hardware" وهو جهاز أو برنامج لمراقبة شبكة الاتصالات والتقاط البيانات .

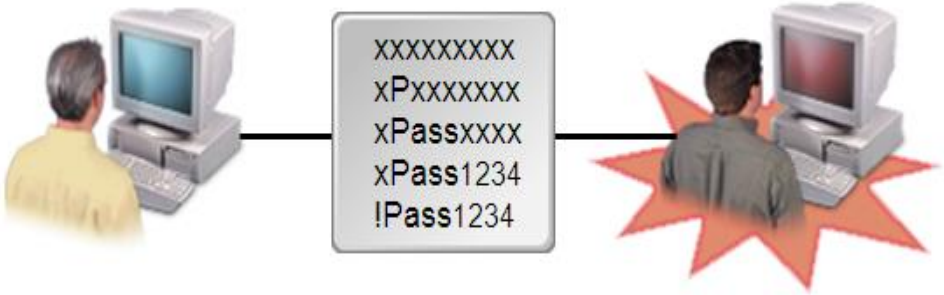


اللصوص والمهاجمين Hackers and Attackers :

المتسللين والمهاجمين هما مصطلحان مترابطان للأفراد الذين يمتلكون المهارات اللازمة للوصول إلى نظام الكمبيوتر من خلال وسائل غير مصرح بها أو غير موافق عليها . إن الهاكر هو مصطلح لذلك المستخدم البارع في برمجة الحاسوب وإدارة نظامه . التسلل إلى النظام هو إشارة إلى مهارة فنية ارتبطت مع تطفل الأنظمة المؤذي وغير الأخلاقي . اما المهاجم فهو مصطلح يعبر دائما عن تسلل للنظام مؤذٍ .

هجمات كلمات المرور Password Attacks :

أي نوع من الهجمات التي يحاول فيها المهاجم الحصول واستخدام كلمات المرور بشكل غير مشروع . المهاجم من الممكن أن يسرق أو يخمن كلمة المرور ، أو يكسر ملف كلمات المرور المشفرة . هجمات كلمات المرور تظهر في سجل التدقيق بمحاولاته الناجحة والفاشلة .



طرق حماية البيانات :

بعد الموازنة بين التهديدات الأمنية المحتملة مع كلفة تطبيق وإدامة عمل الشبكة بشكل آمن ، يمكن للمسؤول تخفيف أثر فقدان البيانات وضمان مستوى ملائم لوظائف الشبكة .

ولحماية البيانات على الشبكة ، بإمكانك إتباع التوجيهات التالية :

- أحرص دائما على تزيل وتنصيب احدث (operating system) ، والتحديثات لكل من أجهزة السيرفر والعميل .
- درب المستخدمين للتعرف وردع أي هجوم .
- أنشر برامج كشف الدخلاء والحماية من الفيروسات لمراقبة نشاطات البرامج غير المرخصة ،مثل وجود فيروس ، برامج كسر كلمة السر password-cracking ، أو أحصنة طروادة .
- الحد من الوصول المادي للشبكة غير المرخص.
- استخدام كلمة مرور للمستخدم قوية ومعقدة ، وتغييرها بشكل منتظم .
- تطبيق مصادقة قوية وتشفير على البيانات المخزنة على خوادم الشبكة .
- تشفير البيانات أثناء التراسل لمنع قراءتها من الدخلاء .
- أحفظ البيانات الحساسة بشكل خاص ، ولا تضع أية بيانات أنت غير مستعد لفقدانها في حال فقدان الجهاز أو سرقته على الأجهزة اللاسلكية .
- حدث البرمجيات على الأجهزة اللاسلكية والراوتر لتزويدك بوظائف إضافية لسد الثغرات الأمنية
- اختبار وظائف النظام للتأكد من أن الخدمات والموارد في متناول المستخدمين الشرعيين فقط .
- وثق التغييرات .

سياسات كلمة المرور Password Policies :

و تمثل جانباً مهماً جداً من جوانب سياسة الأمن . قد تمثل أضعف حاجز عند الاتصال بالشركة . من الضروري جداً أن يعي جميع مستخدمي الشبكة أهمية الاحتفاظ بسرية كلمات المرور الخاصة بهم . حيث بعض المستخدمين يكتب كلمة المرور الخاصة به على الطاولة أو يضعها تحت لوحة المفاتيح أو يلصقها في أي مكان على شاشة الحاسب، لماذا؟ ، لأنه لا توجد سياسات تحْكم استخدام كلمات المرور بحيث يكون كل مستخدم حذر تجاهها و مدرك لها. ومن الواضح معرفة ما سيحدث فيما لو استطاع شخص ما غير مصرح له بالدخول للشبكة ، بهذا نكون قمنا بتسهيل عمل المخترق Hacker بإعطائه كلمة المرور. إذا كان لا بد من تسجيل كلمة المرور، تأكد أن السياسات تشمل طريقة للتعامل مع مثل هذه الحالة ، كأن تغلف بمظروف محكم الإغلاق و تحفظ في مكان آمن . ولا بد أن يتم تغطية مسئوليات المدراء و مسئوليات المستخدمين فيما يخص كلمة المرور عند وضع السياسات.

أما كلمة المرور نفسها فيجب أن لا تكون واحداً مما يلي :

- كلمة من القاموس
- رقم هاتف
- اسم شخص أو اسم شيء
- كلمة مرور بنفس الأحرف (مثل aaaaaa)
- اسم مكان او اسم علم
- نمط سهل من الأحرف على لوحة المفاتيح مثل zxcv) أو Qwer) اي حرف بجانب حرف

شرح كيفية التحكم بالمستخدمين من حيث الصلاحيات المعطاة لهم من خلال السيرفر..

مقدمة حول الصلاحيات

تكمن الصلاحيات على تهيئة القرص الصلب بنظام الملفات NTFS ، الذي يمكنك بإعطاء الحماية والصلاحيات لكل من حسابات المستخدمين User Account أو المجموعات Groups أو على الكمبيوترات Computers على مصادر الشبكة .

مبدأ عمل الصلاحيات :.

يخزن نظام NTFS قائمة تحكم للوصول [access control list (ACL)] إلى كل مجلد وملف مخزن في القرص الصلب الذي هيئ بنظام ملفات NTFS ، الـ ACL تحتوي على قائمة بجميع حسابات المستخدمين و المجموعات و الكمبيوترات التي تمنحك الوصول إلى المجلدات أو الملفات ونوعية هذا الوصول ايضاً. فعند طلب مستخدم للوصول إلى مجلد أو ملف معين ، فان الـ ACL يجب أن تحتوي على متدخلات حسابات المستخدمين و المجموعات أو الكمبيوترات .. وتسمى هذه المدخلات بـ access control entry (ACE) ، المدخلات يجب أن تحدد نوعية الوصول للمستخدم الذي طلب فتح مجلد أو ملف وهل له الصلاحية بفتحه أو منعه ، يعني إذا لم ننشأ ACE داخل ACL فان الويندوز سوف يمنع المستخدم من الوصول إلى المصدر سواء كان مجلد أو ملف

ضبط اذونات الملفات و المجلدات :.

لضبط اذونات الملفات و المجلدات ، نفذ الخطوات التالية :

١- بزر الفارة الأيمن على المجلد أو الملف الذي تريد تطبيق الاذونات عليه واختر Properties .

٢- من مربع حوار الخصائص اختر التبويب Security .

٣- المستخدمين أو المجموعات الذين يملكون وصولاً إلى الملف أو المجلد من قبل سيكونون مذكورين في اللائحة Name ، يمكنك تغيير اذونات أولئك المستخدمين و المجموعات بتنفيذ ما يلي :

- اختر المستخدم أو المجموعة الذي تريد تغيير صلاحياته.
- استعمل اللائحة Permissions لمنع أو منح اذونات الوصول .

ضبط اذونات الطابعة :.

الطابعات الشبكية هي احد المواد المشتركة ،وبالتالي يمكنك ضبط اذونات الوصول لها .

١- استعمل خصائص الطابعة التي تريد أن تضبط تكوينها لضبط اذونات الوصول .

٢- افتح مربع الحوار ثم اختار علامة التبويب Security.

٣- اختر المستخدم الذي تريد تطبيق الاذونات عليه ، وإذا لم يكن موجود في اللائحة اضغط على Add وأضف كائن

٤- ثم OK .

فهم اذونات الوصول إلى الطابعة :.

الاذونات الأساسية التي يمكن منحها أو منعها للطابعات هي Print (طباعة) و Manage Documents (إدارة المستندات) و Manage Printers (إدارة الطابعات) ،

سوف نبين الإعدادات الافتراضية لمربع الحوار Print Permissions التي تستعمل لأي طابعة شبكية جديدة تنشئها :.

يمكنك Administrator و Printer Operators و Server Operators تحكماً كاملاً على الطابعات بشكل افتراضي، هذا يتيح لك إدارة الطابعة و أعمال طباعتها.

منشئ (Creator) أو مالك (Owner) المستند يملك إدارة مستنده، هذا يتيح للشخص الذي طبع بإدارة مستنداته كتغييرها أو حذفها .

يستطيع Everyone الطباعة على الطابعة، هذا يمكن كل المستخدمين على الشبكة من الوصول إلى الطابعة.

الخاتمة

غدت الشبكات جزءا أساسيا في حياتنا الشخصية والمهنية فبإمكانك اليوم أن ترسل رسالة مكونة من عدة صفحات وصور وأصوات ورسومات متحركة إلى مجموعة أشخاص في أي مكان دفعة واحدة وفي دقائق معدودة، وأصبح من الممكن أن تتصل من حاسوب منزلك أو مقر عملك ببنوك المعلومات والشركات والمكتبات العالمية للحصول على المعلومات التي تهمك. كما أصبح متاحاً الآن عقد مؤتمرات دولية وندوات تفاعلية لأطراف متباعدة عبر شبكة الانترنت، وهناك أيضاً التعليم عن بعد والطب عن بعد والتجارة الإلكترونية والحكومة الإلكترونية. كل ذلك لم يكن ممكناً بدون الاندماج بين تكنولوجيا الاتصالات وتكنولوجيا الحاسبات وإيجاد ما يسمى بشبكة الحاسوب.

و نخلص إلى القول أن التجارة الإلكترونية عاجلاً أم أجلاً ستقتحم دارنا ولكن علينا أن نعد لها العدة من أجل أن نكسب منها. ويجب ألا يغيب عن ذهننا إننا قوم دلهم كتابهم وحثهم على ممارسة التجارة لأنها عمل مبارك إذا اتبعنا وسائل الكسب الحلال. لذلك علينا إعداد العدة اللازمة كحكومات وهيئات ومؤسسات وأفراد والابتعاد عن شعار البضاعة التي تباع لا ترد ولا تبدل. فاليوم الأسواق العالمية تتقارب والحدود تتلاشى وتحرير التجارة قادم وحرية رأس المال محققة. لان الثقافة العالمية الجديدة قادمة إلينا وكل ما علينا إلا أن نتفاعل معها ونؤثر فيها ونكسب منها وألا نتركها تعبث فينا وتسيرنا وترمينا قتلى في عقر دارنا. وكل هذا يحدث في التحكم عن بعد والاتصال بالشبكات العالمية وهذا ايضا ينطبق على الشبكة المحلية من خلال زيادة المعرفة البسيطة للتاهل الى المعرفة العالمية ولا ننسى انها سيف ذو حدين بالاستخدام فأن حسن الاستخدام ربحنا وان اسئنا الاستخدام ذبحتنا، وهنا انا دائما اذكر المثل الخاص بالسكين ان حسن استخدامها طابات كل اعمالك واعمال غيرك وان اسات استخدامها ذبحتك وذبحت غيرك ورمتك في السجن ان لم يكن الموت عافاكم اللهً .

ليوم اصبح النظام العالمي الجديد يتحول تدريجياً ليصبح عالماً إلكترونياً ويتطلب من الحكومات والمؤسسات الدولية الاهتمام في استكمال البنية التحتية لتكنولوجية الاتصالات في جميع أنحاء البلد الواحد ومن ثم العالم اجمع. ومن ثم الاهتمام في بناء الشبكات المحلية وتطويرها وربطها في الشبكات العالمية .

وهنا اقول ان الشبكة المحلية هي المفتاح الرئيسي master key والمدخل الرئيسي للشبكات العالمية ومن كان ذو معرفة بالشبكات المحلية سيكون مؤهل وفعال في استخدام الشبكات الاخرى لان هناك عوامل مشتركة كثيرة في الاستخدام والاجهزة والانظمة والامن وغيرها..... وفق الله الجميع للاستفادة من العلم وخير الناس من نفع الناس

المؤلف

٢٠١٨-١١-٢٩