



الجمهورية العربية السورية كلية تكنولوجيا المعلومات والاتصالات قسم المعلومات
الجمهورية العربية السورية جامعة طرطوس
كلية هندسة تكنولوجيا المعلومات والاتصالات
قسم المعلومات



المشروع:

(تصميم وادارة شبكة داخلية لكلية هندسة تكنولوجيا المعلومات والاتصالات)

إعداد الطالب:

يزن عيسى حسن
محمد اسعد الخازم

بإشراف:
الدكتورة: لبنى علي

الفهرس:

الفصل	محتويات الفصل
1	الغاية من المشروع
2	مقدمة عن الشبكات
3	أنواع الشبكات
4	خطوات بناء الشبكة

المشاكل أثناء العمل	5
المراجع	6

1. الغاية من المشروع:

- بناء وإدارة شبكة داخلية بين المستخدمين (العميد - رؤساء الأقسام - المكاتب الإدارية - الدكاترة - الطلاب) بهدف مشاركة الموارد (أجهزة - معلومات - تطبيقات)

2- مقدمة :

شبكة الحاسوب أو الكمبيوتر network هي نظام لربط جهازي حاسوب أو أكثر من أجل تبادل المعلومات والبيانات بينها . من الممكن أن تكون أجهزة الحاسوب قريبه جداً من بعضها وذلك مثل أن تكون في غرفة واحدة ويتم وصل الأجهزة بعدها وسائل منها أجهزة الاتصال السلكية أو اللاسلكية . ومن الممكن أن تكون شبكة الحاسوب مكونة من مجموعة أجهزة في أماكن بعيدة مثل الشبكات بين المدن أو الدول وحتى القارات ويتم وصل مثل هذه الشبكات في كثير من الأوقات بالإنترنت أو بأجهزة الستالايت . يعبر علم دراسة شبكات الحاسوب من أحد فروع علم الاتصالات .

الشبكة في أبسط أشكالها تتكون من جهازين متصلين ببعضهما بواسطة سلك ، ويقومان بتبادل المعلومات والموارد المتاحة للشبكة مثل الآلة الطابعة أو البرامج التطبيقية أي كان نوعها وكذلك تسمح بالتواصل المباشر بين المستخدمين تخيل الكم الهائل الذي ستحتاجه من الأقراص المرنة في حالة عدم وجود شبكة وكيف ستبادر المعلومات كذلك في حالة وجود طابعة واحدة في موقع يحتوى على أكثر من نهاية كيف سيتم استخدام تلك الطابعة .

السمات الخاصة بالشبكة لعمل شبكة حاسب يجب توافر المتطلبات التالية :

- 1- وسيط ناقل " عبارة عن أسلاك أو وسائل لاسلكية

2- موائم لتوسيع تلك الوسائط إلى الشبكة الان لنتعرف على دور الخادم والزبون الحواسيب التي تقدم البيانات أو الموارد في الشبكات الحالية يطلق عليها اسم Servers أو مزودات أو خوادم.

3. هناك أنواع للشبكات الحاسوبية:

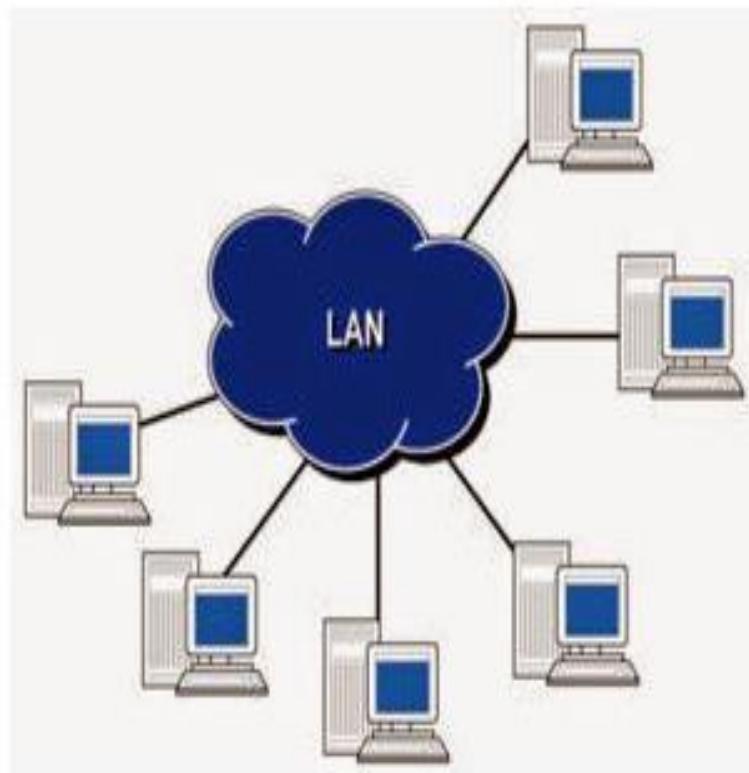
أنواع شبكات الحاسوب

3.1. حسب المساحة الجغرافية التي تغطيها :

يمكن تصنيف شبكات الحاسوب بحسب حجمها و المساحة الجغرافية التي تتغطيها غطيها ، ومن أشهر هذه التصنيفات ما يلي:

3.1.1. الشبكة المحلية (Local Area Network) :

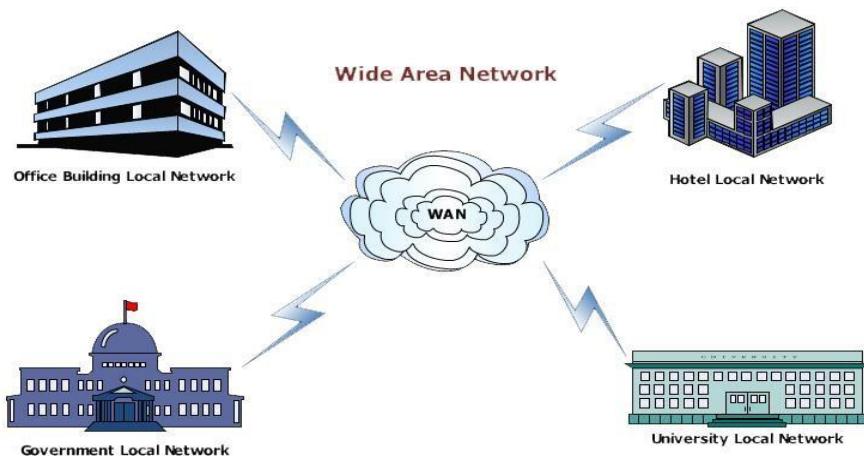
و هي عبارة عن شبكة تربط بين عدد من الأجهزة، ويكون ذلك ضمن منطقة جغرافية ذات مساحة ضيقة كبيوت أو مكاتب في مبني، أو عدد من المباني المتاخرة، أو في المدارس، وعادة ما تكون هذه الشبكات خاضعة لأفراد أو منظمات معينة.



الشكل 1_1 _3

3_1_2 الشبكة المتباعدة (Wide Area Network) :

هي الشبكات التي تربط بين الأجهزة الحاسوبية الموزعة على مساحات جغرافية واسعة ، بحيث تتضمن عدداً من الشبكات المحلية المرتبطة بعضها البعض عن طريق جهاز موجه (Router) ، وتعد شبكة الإنترن特 - والتي تغطي مساحة سطح الأرض بالكامل - مثلاً على هذا النوع من الشبكات. لا يخضع هذا النوع من الشبكات لجهاة أو منظمة معينة ، وإنما تتعدد الجهات المالكة والمنظمة لها .



الشكل
2_1_3

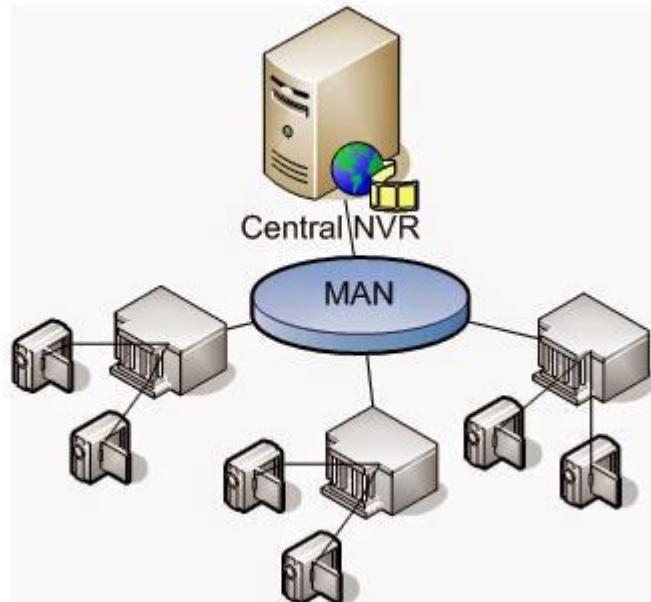
3_1_3. الشبكة اللاسلكية (Wireless LAN) :

هي عبارة عن شبكات محلية موصولة ببعضها البعض عبر تقنيات الاتصال اللاسلكي كتقنية الواي-فاي (Wi-Fi)



الشكل 3_1_3

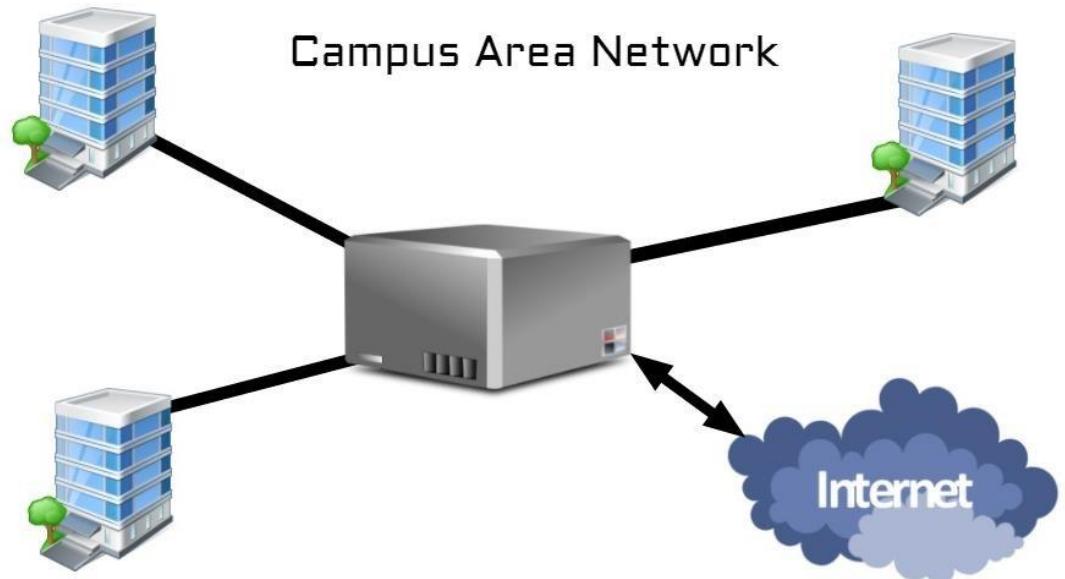
4_1_3 شبكة المنطقة الإقليمية (Metropolitan Area Network) هي الشبكات التي تغطي مساحات واسعة أوسع من تلك التي تغطيها الشبكات المحلية ، ولكنها أصغر من التي تغطيها الشبكات المتباعدة ، فهذا النوع من الشبكات يعد مناسباً للتغطية مدينة أو إقليم معين . عادة ما يخضع هذا النوع من الشبكات للحكومات والشركات الضخمة .



الشكل 3_1_4

كما توجد أنواع أخرى من الشبكات التي يمكن تصنيفها حسب المساحة الجغرافية التي تغطيها ،

4_1_3 ومن هذه الشبكات تلك الموجودة في الحرم الجامعي (Campus Area Network) حيث تضم عدداً من الشبكات المحلية الموصولة ببعضها البعض؛ إلا أنها أصغر حجماً من الشبكات الإقليمية ، ومنها أيضاً الشبكات المتخصصة بربط الخوادم بأجهزة تخزين البيانات ، وتسمى بشبكات التخزين (Storage Area Network)



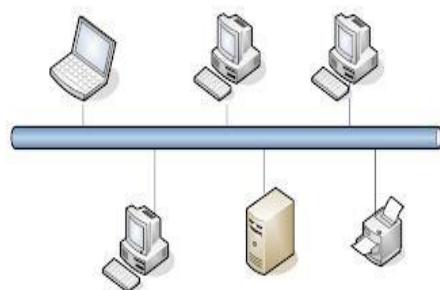
الشكل 5_1_3

3_2. حسب شكل الشبكة

3_2_1. الخطية الشبكة الخطية (Bus Topology) :

هي الشبكة التي تتتألف من كابل واحد يربط بين الأجهزة المتصلة بها ، بحيث يتم نقل البيانات من خلاله عبر الأجهزة حتى تصل إلى الجهاز المنشود ، ويعد هذا النوع من الشبكات سهل الإنشاء والتركيب؛ إذ إنها لا تحتاج إلى عدد كبير من الوصلات مقارنة بأنواع الأخرى من الشبكات. من مشاكل هذه الشبكات هو أنها أنها تعد مناسبة فقط لعدد قليل من الأجهزة، فلو زاد عدد الأجهزة المتصلة لقل أداء الشبكة ، كما أنه في حال حدوث مشكلة معينة في الكابل الرئيسي، فإن ذلك سيتسبب في اختلال الشبكة بالكامل .

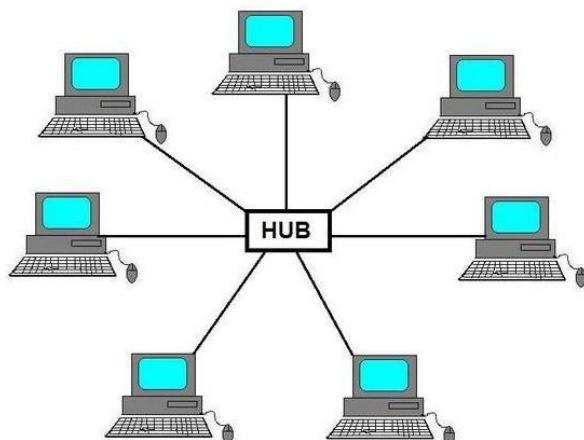
BUS Topology



الشكل 1_2_3

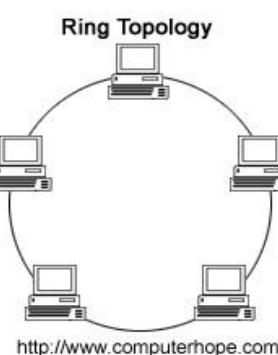
3_2_2. الشبكة النجمية (Star Topology) :

هي الشبكة التي تتصل فيها الأجهزة ببعضها البعض عبر جهاز موزع (Hub)، بحيث يعبر النقطة المركزية فيها، وهي من أكثر الشبكات شيوعاً وانتشاراً في المنازل، فهي سهلة الإصلاح والصيانة، كما أنها تحتوي على عدد من الميزات والخصائص العملية، كعدم تأثر أجهزة الشبكة ببعضها البعض في حال حدوث مشكلة في إحداها. تتميز هذه الشبكات بأداء عالٍ نظراً للعدد القليل من الأجهزة المتصلة، كما أن أداؤها يعتمد على أداء الجهاز الموزع، وفي حال حدوث مشكلة فيه، فإن ذلك سيؤثر على الشبكة بشكل كامل.



الشكل
2_2_3

3_2_3 الشبكة الحلقة (Ring Topology): يكون كل جهاز موصلاً بجهازين آخرين في الشبكة، وفي نهاية المطاف، يوصل الجهاز الأخير بالجهاز الأول، مشكلين بذلك دائرة أو حلقة. عند إرسال جهاز معين في الشبكة رسالة لجهاز آخر فيها، تنتقل الرسالة عبر الحلقة باتجاه واحد، إما مع عقارب الساعة أو عكسها حتى تصل للجهاز الهدف. من مساوى هذا النوع من الشبكات هو أنها تختل بالكامل في حال حدوث خلل في جهاز معين أو وصلة فيها، كما كما تعد عملية صيانتها أصعب بالمقارنة مع الشبكات الخطيّة.

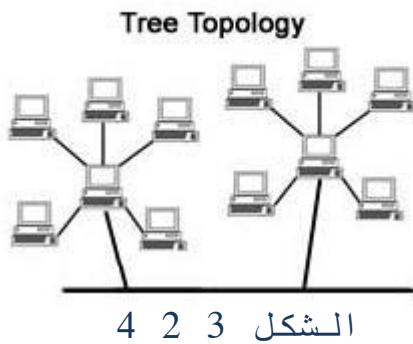


الشكل
3_2_3

3_2_4 الشبكة الشجرية (Tree Topology) :

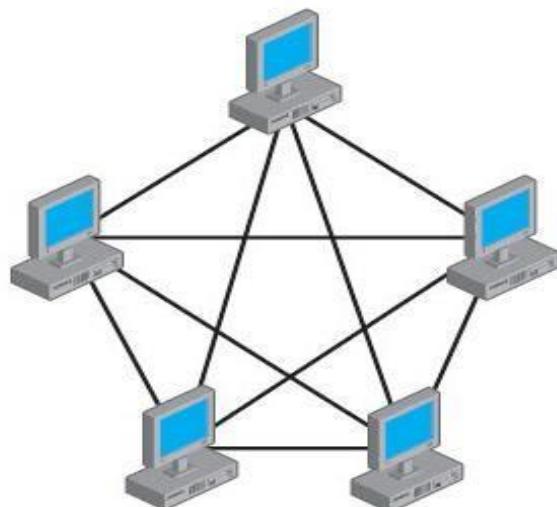
تدمج ما بين الشبكة النجمية والشبكة الخطية؛ حيث يتم تقسيم الأجهزة إلى مجموعات، ويتم وصل كل مجموعة منها بجهاز موزع (Hub) (معينين)، وفي نهاية المطاف توصل الأجهزة الموزعة مع بعضها البعض بواسطة كابل واحد. ما يميز هذا النوع من الشبكات هو إمكانية توسيعتها بسهولة عند

لزوم ذلك، كما أنها سهلة الإدارة والصيانة؛ مما يجعلها مناسبة للاستخدام في الشركات.



3_2_3 الشبكة الشبكية (Mesh Topology) :

تعتمد على مبدأ المسارات (Routes)؛ حيث يتم توصيل جميع أجهزة الشبكة ببعضها البعض لبعض مشكلين بذلك شبكة شبكية كاملة، أو توصيل بعض الأجهزة فقط بجميع الأجهزة الأخرى، أما المتبقية منها فيتم وصلها بعدد محدود محدد من الأجهزة دون غيرها، وفي هذه الحالة الحالة تسمى شبكة شبكية جزئية. عند إرسال جهاز في الشبكة رسالة لجهاز آخر فيها، فإن للرسالة أن تتخذ أي من المسارات المؤدية للجهاز الهدف. تتخذ شبكة الإنترنت بالإضافة إلى شبكات واسعة أخرى هذا الشكل من الشبكات، وتعد الشبكات الشبكية سهلة الصيانة؛ إلا أنها أنها معقدة التركيب والإعداد مقارنة بشبكات النجمة، والحلقة، والشبكات الخطية.



الشكل 5_2_3

3_3 شبكة المعلومات

شبكة المعلومات أو الشبكة هي نظام يتكون من عدد من الحواسيب التي تتصل فيما بينها مما يؤدي إلى منحها القدرة على تناقل المعلومات والبيانات فيما بينها بشكل تام، حيث تتصل مع بعضها البعض إما من خلال خطوط معينة، أو من خلال جهاز حاسوب مركزي، تتضمن الشبكات أيضًا على عناصر أخرى هامة منها البرمجيات، والأجهزة المرسلة والمستقبلة للبيانات. في الحقيقة

تطورت وسائل الاتصالات بعد أن كان هناك تطور كبير جداً في التقنيات المختلفة كل على حدى، فالحاسوب وحده أخذ فترة طويلة من الزمن إلى أن وصل إلى ما وصل إليه اليوم، كما أن تطور الشبكات ترافق مع ازدياد حاجة الإنسان في شتى الميادين والحقول إلى التواصل مع الآخرين، مما حقق فائدة كبيرة لمختلف أصناف الناس من كافة الأماكن، ومن هنا فإنه يمكننا استعراض بعض أهم الفوائد التي استطاع الإنسان أن يجنيها بسبب اعتماده الكبير على شبكات المعلومات المختلفة.

3_3_1. فوائد شبكة المعلومات

1. توفير المال الذي كان ينفق على العديد من الأمور الأساسية وعلى رأسها عملية نقل المعلومات، حيث صار المال الموفّر الموفّر ينفق في مجالات وأمور أكثر أهمية للإنسان، وعلى مستوى المنشآت الاقتصادية فقد صار بإمكان زيادة هامش الربح، أو إنفاق الأموال على تحسين جودة المنتجات والخدمات المقدمة مما يعمل على تحسين نوعية الأعمال المقدمة من قبلها، فالشبكة بإمكانها أن تقوم بما لا يمكن لأي حاسوب مفرد أن يقوم به.

2. مكنت من إتباع أسلوب الإدارة المركزي بشكل أكبر وأفضل من قبل، ذلك أن كافة مستخدمي الشبكات في بيئة الأعمال المتعددة يستعملون البيانات والمعلومات نفسها التي توفرها الشبكة لهم، وليس هذا فقط، بل صار بإمكان استعمال المعلومات نفسها من قبل العديد من الأشخاص من أماكن متعددة جغرافياً، وفي الوقت نفسه.

3. ساعدت العاملين في المؤسسة على تناقل البيانات والمعلومات فيما بينهم بأقل وقت وجهد ممكّنين، حيث أتاح هذا الأمر قدرة كبيرة جداً على أداء المهام المطلوبة من الموظفين بشكل أسرع وأكثر إتقاناً، فالجهد لم يعد يضيع على أعمال بسيطة متفرقة تستنزف الوقت كما كان يحصل سابقاً، بل صار هناك نوع من التركيز وتكتيف الجهود على الأعمال الأكثر أهمية التي تعتبر من صلب عمل المؤسسة، والتي تصب نتائجها الإيجابية في المصلحة العامة لها.

4. صار بإمكان التوسيع في مختلف مناطق العالم بكل سهولة ويسر ودون عناء يذكر، مع وجود إدارة عامة من المقر الرئيسي للمؤسسة، هذا الأمر ساعد وبشكل ملحوظ على زيادة وتحسين نوعية الأعمال، مع زيادة الإنتاجية جداً، كغير واضح.

3_4. تتفرع الشبكات المحلية (LAN) إلى نوعين رئيسيين:

الإنترانت (الشبكة الداخلية intranet) و الإكسترا نت. Extranet

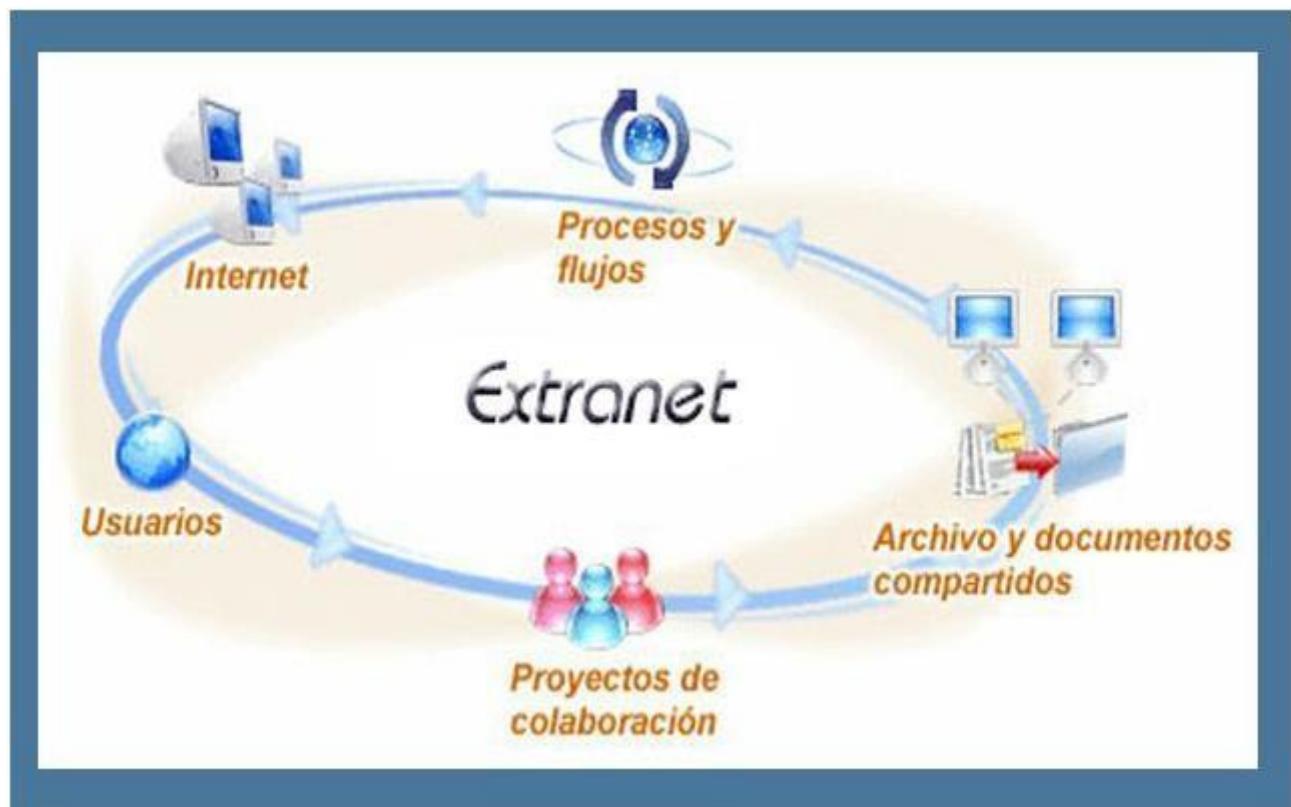
:extranet 1_4_3

تشبه الانترانت لكن الدخول يتم عن بوابة الويب ويمكن الدخول من أي مكان إذا كان المستخدم كلمة السر و اسم المستخدم . الغرض منها السماح بالتعاون

والمشاركة في المصادر ليس فقط داخل المنظمة ولكن للمستخدمين خارج الشركة وممكن أن يكونوا غير موظفين فيها مثل المزودين والزبائن لاستخدام مصادر الشركة والأكسترا نت تساهم بشكل فعال بسلسة التزويد.

شبكة خصوصية شبيهة بالإنترنت إلا أن الشركات والمؤسسات تسمح غالباً عبر معرف وكلمة سر (للشركاء التجاريين أو الموردون أو العملاء ب الوصول إليها لتبادل البيانات والمعلومات).

ظهرت شبكة الأكسترا نت نتيجة لانتقادات التي وجهت إلى نظام الانترانيت وفي مقدمتها الاستقلالية وبعد عن الأطراف الخارجية ، حيث يرى البعض أن نجاح مشروع ما لن يأتي إلا بعلاقة متواصلة واتصال دائم مع موزعيه وعملائه والذي يؤدي في النهاية إلى علاقة متشابهة.



الشكل 3_4_1

3_4_2. الشبكة الداخلية (الإنترانet)

تعرف بأنها الشبكة التي تربط في اتصالها بين مجموعة من الحواسيب الكائنة ضمن نطاق محدود المساحة كما هو الحال في الجامعات، والمدارس، والشركات، وتشبه في اتصالها شبكة الإنترنط، لكنها تختلف عنها بمحدودية البيانات والمعلومات المسموح تناقلها بين أطراف الشبكة؛ حيث إن المنظمات بغض النظر عن نوعها أو هدفها تعمل على حجب المواقع التي لا تخدم مصلحتها ، وتفتح المجال لمرور البيانات والمعلومات التي تخدم مصلحتها ، وتهتم عمل الطرفين من موظفي أو مستخدمي الشبكة المخول لهم بذلك



الشكل 2_4_3

1_2_4_3 ميزات الشبكات الداخلية

سهولة التواصل بين المستخدمين المخول لهم بالدخول إلى الشبكة .

سهولة المعاملات؛ حيث لا تشرط عليك الذهاب شخصياً لإتمام عمل ما إلى الجهة المختصة بهذا العمل، كالحاجة إلى إتمام معاملة ما ، فلا يتلزم ذلك الموظف القائم على إتمام هذه المعاملة الذهاب إلى الجهة المختصة، كل ما عليه مراسلة الجهة المعنية عبر الشبكة وإتمام عمله.

1. المصداقية : حيث إن محدودية مستخدمي الشبكة تقلل من حجم الشائعات سريعة الانتشار . سهولة نقل الملفات بين أجزاء المنظمة الواحدة .
2. سهولة الاستخدام المتعدد للبرنامج أو التطبيق الواحد .

2_2_4_3 تقسيم هذه الشبكة إلى نوعين :

1-شبكات الند للند

2-شبكات المجال

3_2_2_4_1 شبكات الند للند (Peer To Peer Network)

يستخدم هذا المصطلح للتعبير عن الشبكات التي يشارك فيها كل كمبيوتر موارده مع مجموعة أخرى من الأجهزة على الشبكة ، وكل جهاز على هذه الشبكة هو جهاز مسؤول بمفرده ، أي يقوم كل مستخدم بالتحكم بشكل كامل بالموارد الخاصة به ، وأنظمة التشغيل على الأجهزة أيضاً يمكن أن تختلف من جهاز للأخر .

محدوديات شبكات الند للند

لو كان لدى في شبكات الند للند عشر مستخدمين بحاجة للوصول إلى ملف عبر الشبكة ، يجب أن أنشأ في جهاز المورد المشارك عشر مستخدمين ، واستخدم هذه الحسابات من قبل المستخدمين على حدا للوصول إلى هذا المورد . ونقوم بإنشاء المستخدمين حتى نتمكن من تحديد صلاحيات مختلفة ، لأنه لا يمكن لمستخدم واحد أن أحد له صلاحيات مختلفة . وكذلك إذا أردنا أن نطبق سياسة معينة في الشبكة ، يجب أن نفعل هذه السياسة على جميع أجهزة الشبكة حتى . لذلك هذا النوع من الشبكات لا يناسب العمل

Peer-to-Peer / Ad-Hoc



الشكل 1_2_2_4_3

3_4_2_2_2 شبكات المجال :

وتسمى أيضاً شبكات المخدم Server / Client Networks يطلق هذا المصطلح على الشبكات التي تعتمد على المخدم ، وهذا ينفرد أحد الأجهزة (هو المخدم) هو بتقديم خدمه مميزه لا يقوم بها أحد غيره ،

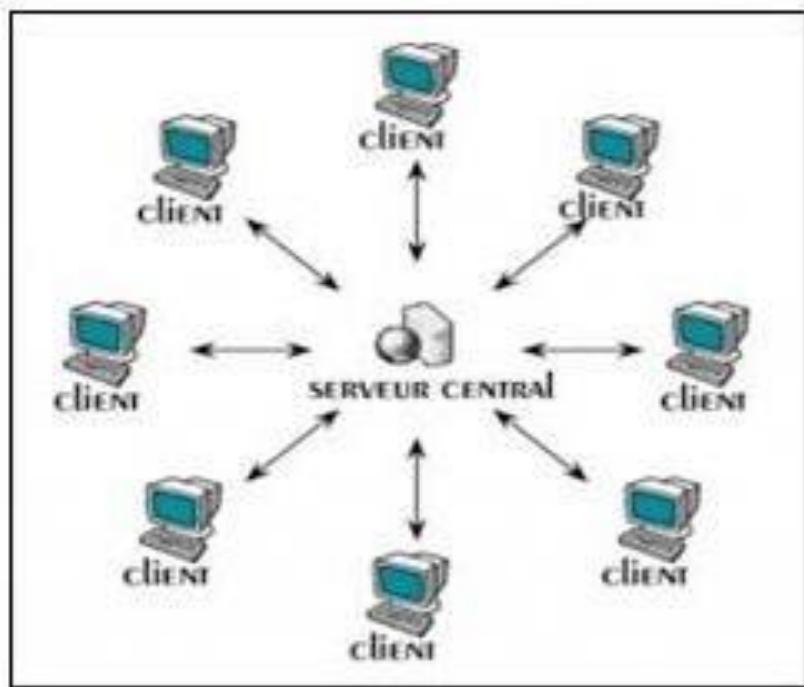
ويطلق على باقي الأجهزة التي تستفيد من هذه الخدمات اسم العميل أو الزبون . تعد شبكات المخدم زبون أكثر تنظيماً من شبكات الند للند لوجود خادم مركزي يقوم بعملية التنظيم المركزية للشبكة Centralized Administration ويتحقق مستوى أمن للمعلومات أعلى من شبكات الند للند

توجد عدة أسماء لهذه الشبكة ، منها العميل/الخادم ، الزبون/المزود وكلها أسماء تحمل نفس المعنى ، فبداية سوف نوضح مفهوم المسميات لهذه الشبكة .

العميل - الزبون : Client - والمقصود بهذه المسميات هو جهاز كمبيوتر أو الشخص الذي يستخدم الكمبيوتر المتصل بالشبكة والذي يستفيد من الخدمات المقدمة من خلال الشبكة ، فمثلاً عند تصفحك لموقع لقراءة مقال ، تكون أنت العميل المستفيد من الخدمة التي يقدمها خادم الويب Web Server - الخادم بالموقع .

الخادم - المزود : Server - وتعريفه هو أنه جهاز حاسوب ذو إمكانيات قوية أي أنه يحتوي على معالج ببيانات CPU قوي ، وذاكرة عشوائية RAM كبيرة ومساحات للتخزين Hard Disk كبيرة ، هنا يقصد بها أكثر من أي جهاز كمبيوتر شخصي PC/Laptop ، وذلك حتى يتمكن الخادم من تقديم خدماته لأكثر

من عميل في آن واحد، ويحتوي الخادم على نظام تشغيل خاص مثل Windows Server أو إصدار Linux ، ويستخدم الخادم في تقديم العديد من الخدمات، على سبيل المثال خادم لاستضافة المواقع الإلكترونية ، خادم بريد إلكتروني، خادم لقواعد البيانات، خادم ملفات، خادم طباعة ، الخ.



الشكل

2_2_2_4_3

ما هي مزايا شبكة العميل/الخادم ؟

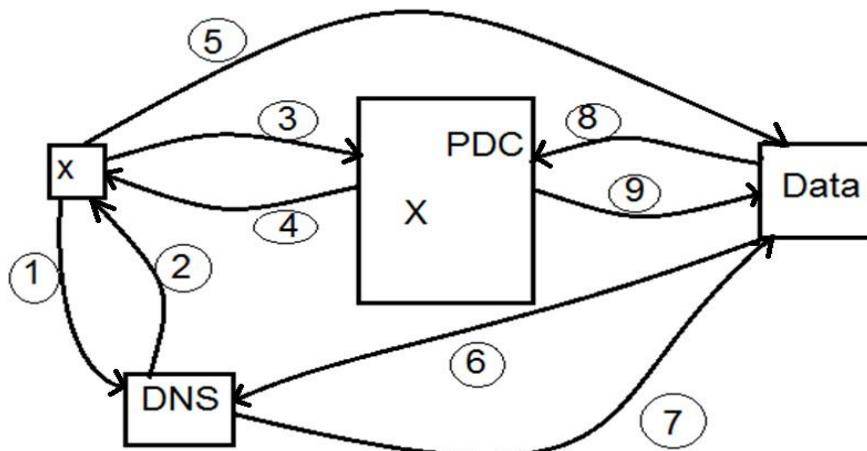
- . أمان الشبكة يعتبر من أهم مميزات نظام العميل/الخادم حيث لا يمكن لأي شخص تداول أي معلومات من خلال الشبكة إلا إذا كان مصرحاً له باستخدام هذه المعلومات
- . المركزية في إدارة الشبكة أيضاً تعتبر من أهم مميزات هذا النظام، حيث أن دخول أي فرد للشبكة يكون من خلال الخادم، وتداول أي ملفات يكون من خلال الخادم أيضاً
- . يسهل عمل النسخ الاحتياطي لملفات الشبكة، حيث أن كل المحتويات موجودة في مكان واحد
- . قدرة هذا النظام على التوسيع في الشبكة بسهولة، بالإضافة عملاً جدد أو إضافة خادم آخر للشبكة ما هي عيوب شبكات العميل/الخادم ؟
- . ارتفاع تكلفة هذا النظام، حيث يتطلب تشغيله وجود جهاز خادم واحد على الأقل، ودائماً ما تكون تكلفة هذا الجهاز مرتفعة، وأيضاً إذا

استخدمنا للخادم أنظمة تشغيل غير مفتوحة المصدر ، تكون تكلفتها أيضاً باهظة الثمن

• يتطلب العمل بهذا النظام وجود شخص ذو مهارات فنية عالية ، وذلك حتى يتمكن من إدارة الشبكة ، ومواجهة أي مشكلات قد تحدث بالشبكة . في حالة تعطل جهاز الخادم ، فإن الشبكة بأكملها تتعرض ، ولتفادي ذلك العيب يمكن إضافة خادم احتياطي في الشبكة ولكن يزيد ذلك الخادم الاحتياطي من تكلفة الشبكة

آلية الحصول على الخدمة في شبكات المخدم زبون:

يكون Active Directory (AD) مسؤولاً عن تسجيل حسابات المستخدمين وتحديد إمكانية الوصول إلى الموارد على الشبكة وذلك من خلال خدمة تسمى TGS (Ticket Granting Service) ، وبدورها هذه الخدمة مسؤولة عن إعطاء المفاتيح لـ كل مستخدم والتي تسمى TGT (Ticket Granting Ticket) . وتلعب خدمة DNS دوراً أساسياً في تحديد من هو المكون المسؤول عن كل مورد من موارد الشبكة . وللوضوح ذلك نأخذ مثالاً لآلية وصول مستخدم ما إلى البيانات على شبكة المجال



آلية الحصول على الخدمة في شبكات المخدم زبون

يسأل المستخدم الـ DNS من مسؤول عن إعطاء خدمة Ticket .
8- يجب الـ DNS المستخدم بأن PDC (Primary Domain Controller) هو المسؤول عن إصدار Ticket .

3- يخاطب المستخدم جهاز PDC ويطلب منه Ticket للدخول إلى المورد (البيانات) .

4- يعطي PDC الكرت للمستخدم . (TGT)

5- يطلب المستخدم البيانات بناءً على Data TGT .

6- تخاطب DNS لتسأله من هو المسؤول عن إعطاء Ticket .

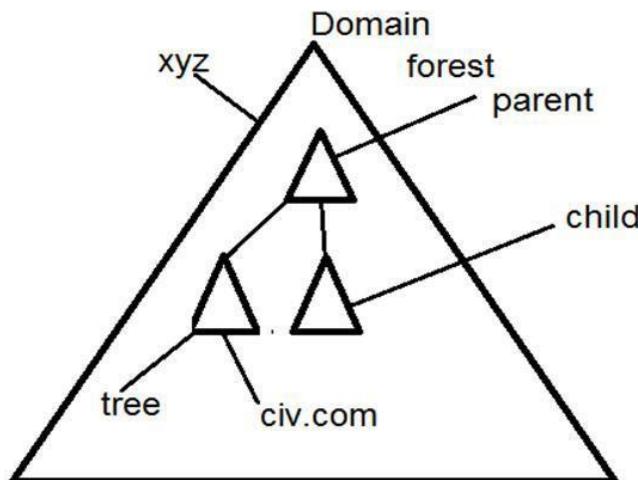
7- يجب DNS بأن جهاز PDC هو المسؤول عن إعطاء Ticket .

2- يخاطب السيرفر PDC ويأسأله هل هذا Ticket صادرة عنك أم أنه عملية . Hacking .

9- وعند ها يجب السيرفر بأنها صحيحة فيحصل المستخدم على البيانات المطلوبة .

مكونات (هرمية) شبكات المجال :

يكون لشبكة المجال هرمية تسمى الغابة (Forest) (و ضمن هذه الغابة يوجد أولاد) (وكذلك أشجار .) (فعنده إنشاء شبكة المجال لأول مرة يسمى هذا المجال باسم معين ويكون هو المجال الأب (Parent) (وبين نفس الوقت هو عبارة عن الغابة .) فمثلاً إذا اخترت اسم المجال الأب xyz.com فهذا يعني أن اسم الغابة كذلك xyz لأن أول مجال أقوم بإنشائه تسمى الغابة باسمه .



هرمية شبكات المجال

بعد إنشاء المجال الأب (parent) (يمكن إنشاء أولاد لهذا المجال Child) : (وهو عبارة عن مجال أيضاً ولهم مستخدميه المختلفين عن مستخدمي المجال الأب ولكن هذا المجال يرث اسم المجال الأب، فمثلاً إذا كان اسم المجال الأب xyz.com ، كمثال على ذلك شركة رئيسية ممكناً أن يكون اسم المجال الابن abc.xyz.com ، كمثال على ذلك شركة Trust وأيضاً لها فرع في مكان آخر ، ولكن ليس الهدف من هذه العملية هو فقط وراثة الاسم بل وراثة الثقة Trust أيضًا ما بين الأب والابن ، أي استطيع من abc أن أصل إلى الموارد من xyz من دون استخدام اسم مستخدم وكلمة مرور . ويوجد كذلك الأشجار Tree وهو عبارة عن مجال ضمن الغابة ، يأخذ اسم مثلاً civ.com معنى ذلك أنه لا يرث الاسم كما في child ولكن الذي يقوم بوراثته هو الثقة ، كمثال على ذلك لدى شركة مثل XYZ وتريد افتتاح شركة ثانية ولا تريد لأحد أن يعلم أنها تابعة ل XYZ ولكن بنفس الوقت تكون تابعة للشركة الأم .

حتى نقوم بإنشاء شبكة المخدم زبون والتي يطلق عليها أ اسم شبكة المجال (Domain) يجب توفر ما يلي :

- 1- جهاز حاسب يملك مواصفات عالية من ناحية سرعة المعالجة وسعة التخزين والذواكر .
- 2- يطلق على هذا الجهاز الذي يملك المواصفات السابقة اسم مخدم عندما يتم تحميله بنظام تشغيل ويندوز سيرفر

حصراً) 2000 أو 2003 أو 2008 أو أي إصدارات أخرى). عند توفر الشرطين السابقين فإننا نحصل على ما يسمى بالمخدم . يقدم هذا المخدم خدمات عديدة لمستخدمين الشبكة مثل خدمات تخزين الملفات، ، DNS، FTP، DHCP، Email، ووجود خدمة أساسية إدارية يقوم بها هي خدمة Network Management وفي هذه الحالة يسمى جهاز المخدم بمحكم المجال .

نظام التشغيل سيرفر ويندوز 2008 :
هو من أحدث أنظمة التشغيل الخاصة بالمخدمات من مايكروسوفت، وقد تم إصداره في العام 2008بني ويندوز سيرفر من نفس الشيفرة المصدرية الخاصة بـ ويندوز فيستا ، لذا فإنه يشاركه في الكثير من بنيته الأساسية وطريقة عمله . ويتميز بدعم أفضل للشبكات مثل الشبكات اللاسلكية ودعم لبروتوكول الإنترنت الإصدار السادس ، ولذلك IPv6 خاصة بالسرعة والأمان وتشخيص أفضل للمشكلات والمرافق .
تحسينات لديه



4. خطوات بناء الشبكة

- ✓ توثيق يتم فيه فحص البنية التحتية للشبكة(نقاط خدمة - كابلات -سويتشات - راوتر)
- ✓ -تجهيز السيرفر بنظام تشغيل ويندوز سيرفر 2008 وتنصيب خدمة ال active directory لجعله محكم
- ✓ -تقديم تصور عن مكاتب الكلية (دكاترة ومهندسين وطلاب عن طريق تنسيقهم ضمن organization ووحدات تنظيمية unit ,groups ,users)
- ✓ -بناء نظام مشاركة بين مستخدمين ضمن الوحدات التنظيمية

✓ - السياسات التي تم تطبيقها على الوحدات التنظيمية والمستخدمين

4_1. التوثيق:

يرتبط توثيق الطبقة الأولى بالأمور التالية :

- تحديد موقع كل من MDF و IDF في الشبكة
- نماذج وكمية الكابلات التي تصل MDF و IDF
- توضع النقط الجدارية في الغرف وتوزع الكابلات
- أرقام ومحددات الكابلات

يبدو في الجدول التالي توضع كل من IDF و MDF في الشبكة :

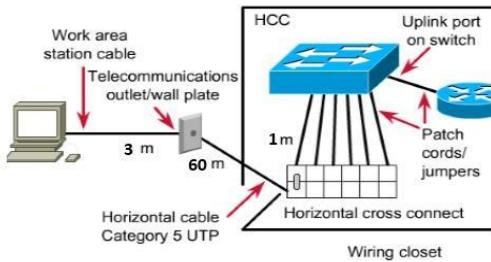
الاسم	الموقع	المكونات
MDF	FLOOR1	switch4 , router,enterpriseserver, workgroup server
IDF1	FLOOR0	Switch1,switch2,switch3
IDF2	FLOOR2	Switch5, switch6
IDF3	FLOOR3	Switch7

وتتوزع التوصيات على الشكل التالي :

- ✓ من محطة العمل باتجاه النقطة الجدارية أقصى طول للكبل هو 2 متر .
- ✓ من النقطة الجاربة باتجاه لوحة التوصيل Patch panel طول الكابل حوالي 60 متر .
- ✓ من لوحة التوصيل HCC باتجاه المبدل حوالي المتر الواحد لأن لوحة التوصيل في شبكة الكلية متوضعة قريبة جداً من المبدل .

ويوضح الشكل المجاور هذه الأطوال :

ونظراً لكون بناء الكلية مكون من عدة طوابق ويوجد مبدل أو أكثر في كل طابق فإن أطول الكابلات التي ستصل هذه المبدلات مع MDF سيكون كبيراً .

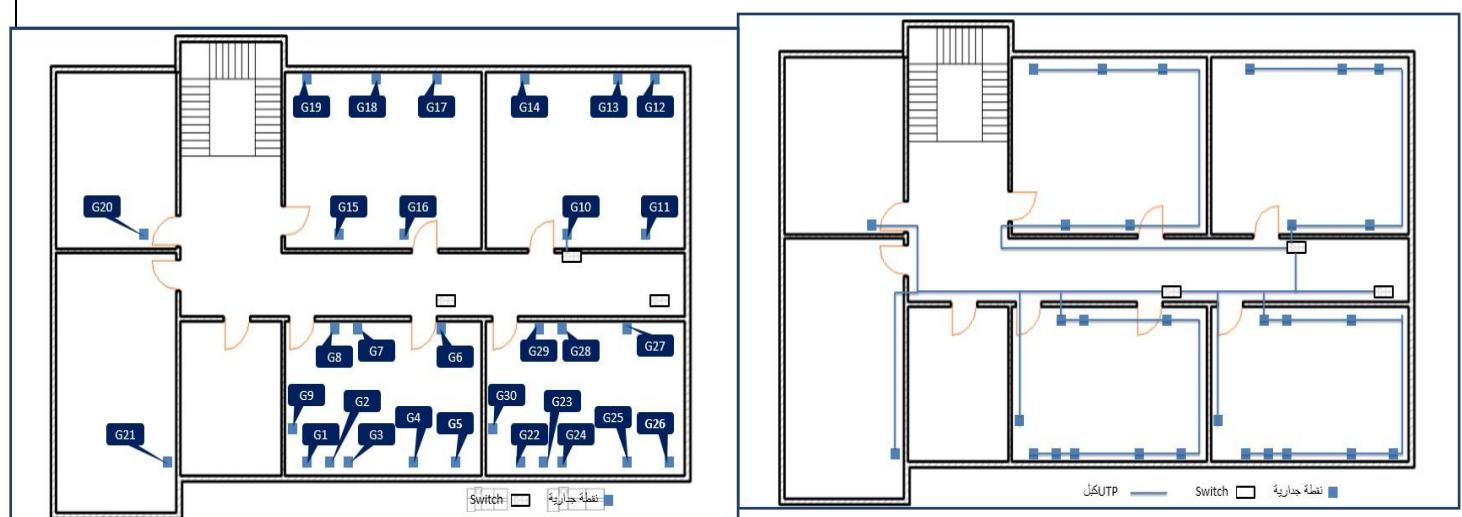


تسمى هذه الوصلات VCC (وهي التي تصل مع MDF)

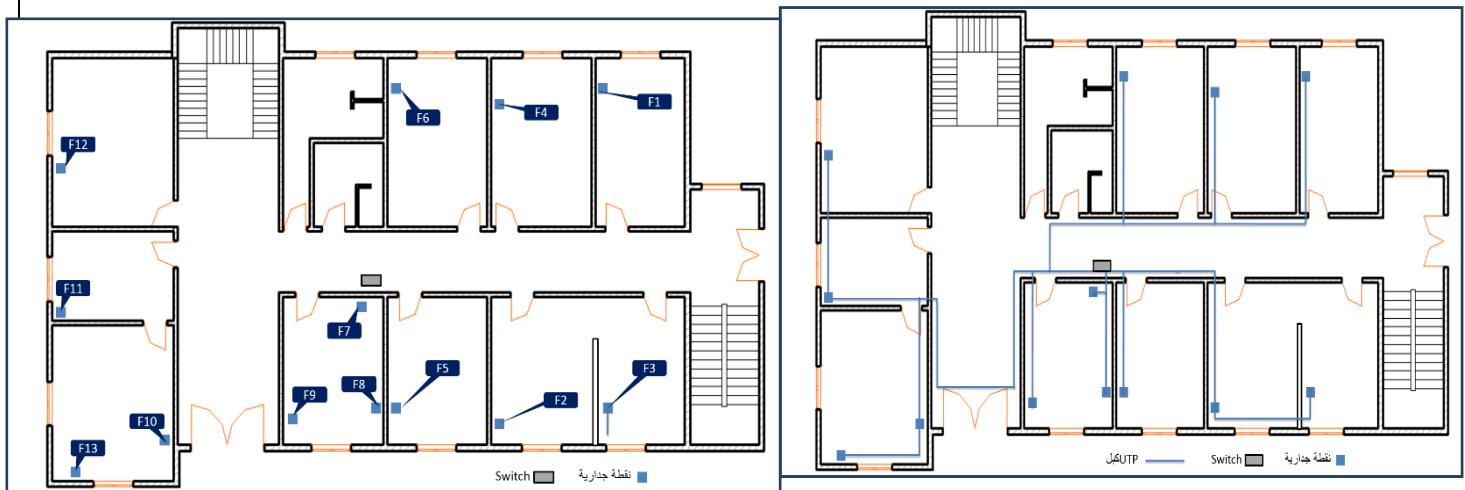
ليف بصري ولكنها غير مستخدم في شبكة الكلية ، وجميع الكابلات هي من النوع UTP (100BaseT) وهذا يعتبر من الأخطاء المرتكبة في تصميم شبكة الكلية حيث يجب أن تكون سرعة الكابلات من نوع VCC أكبر من سرعة HCC (على سبيل المثال VCC يجب أن تكون 1000BaseT و HCC تكون 100BaseT) .

أما بالنسبة للتوزع الكابلات والنقاط الجدارية فهي موضحة بالخططات التالية:

الطابق 0

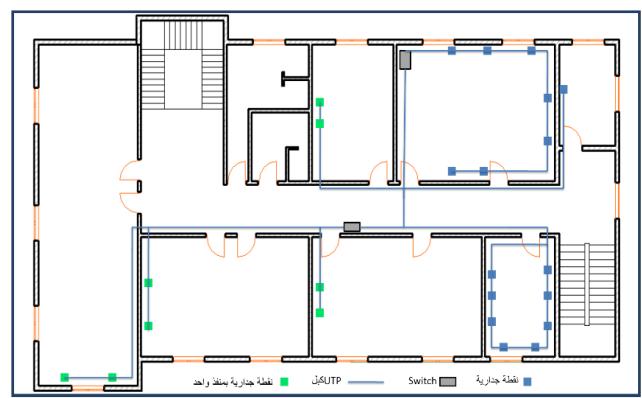
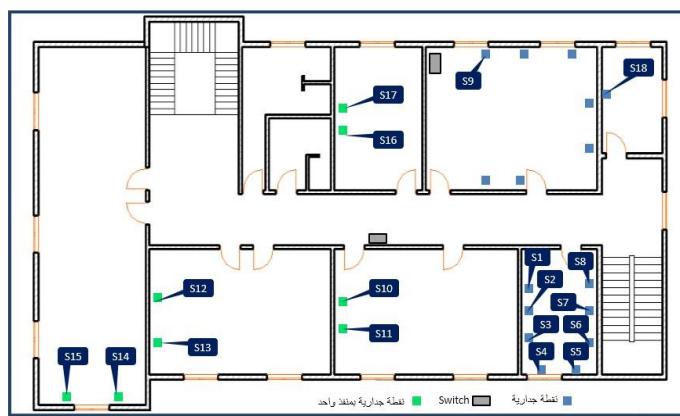


الطابق 1



الثاني

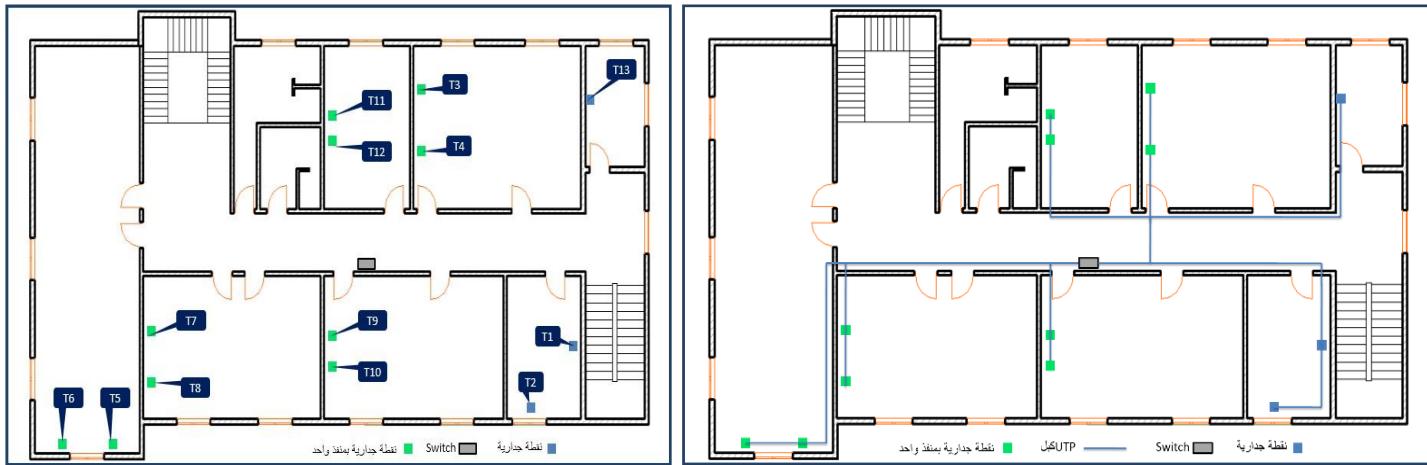
الطبق



connection	Cable id	room	Cross connection paired /port	Type of cable	status
IDF1 TO R1	G1,1	1 مخبر	HCC1 /PORT6	UTP 100 MPRS	Used
IDF1 TO R1	G1,2	1 مخبر	HCC1 /PORT9	UTP 100 MPRS	NOT USED
IDF1 TO R1	G2,1	1 مخبر	HCC1 /PORT14	UTP 100 MPRS	USED
IDF1 TO R1	G2,2	1 مخبر	HCC1 /PORT11	UTP 100 MPRS	USED
IDF1 TO R1	G4,2	1 مخبر	HCC1 /PORT19	UTP 100 MPRS	USED
IDF1 TO R1	G5,1	1 مخبر	HCC1 /PORT17	UTP 100 MPRS	USED
IDF1 TO R1	G5,2	1 مخبر	HCC1 /PORT4	UTP 100 MPRS	USED
IDF1 TO R1	G6,1	1 مخبر	HCC1 /PORT5	UTP 100 MPRS	USED
IDF1 TO R1	G6,2	1 مخبر	HCC1 /PORT2	UTP 100 MPRS	USED
IDF1 TO R1	G7,1	1 مخبر	HCC1 /PORT15	UTP 100 MPRS	USED
IDF1 TO R1	G7,2	1 مخبر	HCC1 /PORT12	UTP100 MPRS	USED
IDF1 TO R1	G8,1	1 مخبر	HCC1 /PORT13	UTP100 MPRS	USED
IDF1 TO R1	G8,2	1 مخبر	HCC1 /PORT7	UTP100 MPRS	USED
IDF1 TO R1	G9,1	1 مخبر	HCC1 /PORT3	UTP 100MPRS	USED
IDF1 TO R1	G4,1	1 مخبر	HCC1 /PORT18	UTP100MPRS	USED
IDF1 TO R1	G3,2	1 مخبر	HCC1 /PORT8	UTP 10MPRS	USED

IDF1 TO R1	G3,1	1 مخبر	HCC1 / PORT16	UTP	100 MPRS	USED
------------	------	--------	---------------	-----	----------	------

الطباق 3



الطبق الارضي

ماخذ مغطى	G9 , 2	1 مخبر			
IDF1 TO R4	G10 , 1 (BLUE)	4 مخبر	HCC2 / PORT8	UTP 100 MPRS	USED
IDF1 TO R4	G10 , 2 (RED)	4 مخبر	HCC2 / PORT5	UTP 100 MPRS	USED
IDF1 TO R4	G11 , 1	4 مخبر	HCC2 / PORT10	UTP 100 MPRS	USED
IDF1 TO R4	G11 , 2	4 مخبر	HCC2 / PORT1	UTP 100 MPRS	USED
IDF1 TO R4	G12 , 1	4 مخبر	HCC2 / PORT3	UTP 100 MPRS	USED
IDF1 TO R4	G12 , 2	4 مخبر	HCC2 / PORT4	UTP 100 MPRS	USED
IDF1 TO R4	G13 , 1	4 مخبر	HCC2 / PORT6	UTP 100 MPRS	USED
IDF1 TO R4	G13 , 2	4 مخبر	HCC2 / PORT9	UTP 100 MPRS	USED
IDF1 TO R4	G14 , 1	4 مخبر	HCC2 / PORT7	UTP 100 MPRS	USED
IDF1 TO R4	G14 , 2	4 مخبر	HCC2 / PORT2	UTP 100 MPRS	USED
IDF1 TO R3	G15 , 1	3 مخبر	HCC / PORT13	UTP 100 MPRS	USED
IDF1 TO R3	G15 , 2	3 مخبر	HCC / PORT18	UTP 100 MPRS	USED
IDF1 TO R3	G16 , 1	3 مخبر	HCC / PORT19	UTP 100 MPRS	USED
IDF1 TO R3	G16 , 2	3 مخبر	HCC / PORT12	UTP 100 MPRS	USED
IDF1 TO R3	G17 , 1	3 مخبر	HCC / PORT14	UTP 100 MPRS	USED
IDF1 TO R3	G17 , 2	3 مخبر	HCC / PORT17	UTP 100 MPRS	USED
IDF1 TO R3	G18 , 1	3 مخبر	HCC / PORT11	UTP 100 MPRS	USED
IDF1 TO R3	G18 , 2	3 مخبر	HCC / PORT15	UTP 100 MPRS	USED
IDF1 TO R3	G19 , 1	3 مخبر	HCC / PORT22	UTP 100 MPRS	USED
IDF1 TO R3	G19 , 2	3 مخبر	HCC / PORT16	UTP 100 MPRS	USED
غير موصولة	G21 , 1	2 فيزياً	HCC / PORT	UTP 100 MPRS	

غير موصولة	G21 , 2	مخبر فيزياء 2	HCC / PORT	UTP 100 MPRS	
IDF1 TO R2	G22 , 1	2 مخبر	HCC3 / PORT	UTP 100 MPRS	غير موصولة
IDF1 TO R2	G22 , 2	2 مخبر	HCC3 / PORT	UTP 100 MPRS	غير موصولة
IDF1 TO R2	G23 , 1	2 مخبر	HCC3 / PORT8	UTP 100 MPRS	USED
IDF1 TO R2	G23 , 2	2 مخبر	HCC3 / PORT19	UTP 100 MPRS	USED
IDF1 TO R2	G24 , 1	2 مخبر	HCC3 / PORT18	UTP 100 MPRS	USED
IDF1 TO R2	G24 , 2	2 مخبر	HCC3 / PORT	UTP 100 MPRS	غير موصولة
IDF1 TO R2	G25 , 1	2 مخبر	HCC3 / PORT11	UTP 100 MPRS	USED
IDF1 TO R2	G25 , 2	2 مخبر	HCC3 / PORT10	UTP 100 MPRS	USED
IDF1 TO R2	G26 , 1	2 مخبر	HCC3 / PORT22	UTP 100 MPRS	USED
IDF1 TO R2	G26 , 2	2 مخبر	HCC3 / PORT21	UTP 100 MPRS	USED
IDF1 TO R2	G27 , 1	2 مخبر	HCC3 / PORT20	UTP 100 MPRS	USED
IDF1 TO R2	G27 , 2	2 مخبر	HCC3 / PORT14	UTP 100 MPRS	USED
IDF1 TO R2	G28 , 1	2 مخبر	HCC3 / PORT	UTP 100 MPRS	غير موصولة
IDF1 TO R2	G28 , 2	2 مخبر	HCC3 / PORT	UTP 100 MPRS	غير موصولة
IDF1 TO R2	G29 , 1	2 مخبر	HCC3 / PORT13	UTP 100 MPRS	USED
IDF1 TO R2	G29 , 2	2 مخبر	HCC3 / PORT12	UTP 100 MPRS	USED
IDF1 TO R2	G30 , 1	2 مخبر	HCC3 / PORT7	UTP 100 MPRS	USED
IDF1 TO R2	G30 , 2	2 مخبر	HCC3 / PORT9	UTP 100 MPRS	USED

الطاقة

الأول

connection	Cable id	Room	Cross connection paired /port	Type of cable	status
IDF1 TO R1	F1,1	شؤون الطلاب	HCC1 /PORT2	UTP 100 MPRS	USED
IDF1 TO R1	F1,2	شؤون الطلاب	HCC1 /PORT5	UTP 100 MPRS	USED
IDF1 TO R2	F2,1	امتحانات	HCC1 /PORT8	UTP 100 MPRS	USED
IDF1 TO R2	F3,1	امتحانات	HCC1 /PORT7	UTP 100 MPRS	USED
IDF1 TO R3	F4,1	قسم الاتصالات	HCC1 /PORT4	UTP 100 MPRS	USED
IDF1 TO R3	F4,2	قسم الاتصالات	HCC1 /PORT10	UTP 100 MPRS	USED
IDF1 TO R4	F5,1	رئيس الدائرة	HCC1 /PORT	UTP 100 MPRS	فارغة
IDF1 TO R4	F5,2	رئيس الدائرة	HCC1 /PORT22	UTP 100 MPRS	USED
IDF1 TO R5	F6,1	الديوان	HCC1 /PORT9	UTP 100 MPRS	USED
IDF1 TO R5	F6,2	الديوان	HCC1 /PORT6	UTP 100 MPRS	USED
IDF1 TO R6	F7,1	رؤساء الأقسام	HCC1 /PORT3	UTP 100 MPRS	USED
IDF1 TO R6	F7,2	رؤساء الأقسام	HCC1 /PORT	UTP 100 MPRS	معطلة
IDF1 TO R6	F8,1	رؤساء الأقسام	HCC1 /PORT1	UTP 100 MPRS	USED
IDF1 TO R6	F8,2	رؤساء الأقسام	HCC1 /PORT	UTP 100 MPRS	فارغة
IDF1 TO R6	F9,1	رؤساء الأقسام	HCC1 /PORT	UTP 100 MPRS	فارغة
IDF1 TO R6	F9,2	رؤساء الأقسام	HCC1 /PORT19	UTP 100 MPRS	USED
IDF1 TO R7	F10,1	نائب العميد	HCC1 /PORT17	UTP 100 MPRS	USED
IDF1 TO R7	F10,2	نائب العميد	HCC1 /PORT	UTP 100 MPRS	معطلة
IDF1 TO R7	F13,1	نائب العميد	HCC1 /PORT21	UTP 100 MPRS	USED

IDF1 TO R7	F13,2	نائب العميد	HCC1 / PORT	UTP 100 MPRS	معطلة
IDF1 TO R8	F11,1	سكرتير	HCC1 / PORT18	UTP 100 MPRS	USED
IDF1 TO R8	F11,2	سكرتير	HCC1 / PORT	UTP 100 MPRS	معطلة
IDF1 TO R9	F12,1	العميد	HCC1 / PORT20	UTP 100 MPRS	USED
IDF1 TO R9	F12,2	العميد	HCC1 / PORT16	UTP 100 MPRS	USED

رئيس الدائرة منفذ 22 على لوحة التجميع طابق أول
 شؤون الطلاب F12 (الأزرق) بورت 2 على لوحة التجميع طابق أول
 النائب الإداري (الأزرق) بورت 17 على لوحة التجميع طابق أول
 مبدل الطابق الثاني (بالكوريدور) يتصل مع المنفذ 14 للوحة التجميع لمبدل
 الطابق الأول.

مبدل الطابق الثالث (بالكوريدور) يتصل مع المنفذ 11 للوحة التجميع لمبدل
 الطابق الأول. عبر البورت 7

مبدل طابق المخابر ذو المنفذ 24 (الأول من جهة المخبر 1) يتصل مع المنفذ
 13 للوحة التجميع لمبدل الطابق الأول.

البورت 15 على المبدل متصل بالمبدل الثاني (مقابل مبدل مخبر رامي في
 الغرفة البلورية) في طابق المخابر
 البوتر 19 لمبدل طابق المخابر الأول (خارج الغرفة الزجاجية) فيه مشكلة
 الطابق الثاني

connection	Cable id	room	Cross connection paired /port	Type of cable	status
IDF3 TO ENGLAB	S1,1	مخبر المهندسين	HCC1 / PORT	UTP 100 MPRS	غير موثقة
IDF3 TO ENGLAB	S1,2	مخبر المهندسين	HCC1 / PORT12	UTP 100 MPRS	USED
IDF3 TO ENGLAB	S2,1	مخبر المهندسين	HCC1 / PORT	UTP 100 MPRS	غير موثقة

IDF3 TO ENGLAB	S2 , 2	مخبر المهندسين	HCC1 / PORT	UTP 100 MPRS	غير موثقة
IDF3 TO ENGLAB	S3 , 1	مخبر المهندسين	HCC1 / PORT5	UTP 100 MPRS	USED
IDF3 TO ENGLAB	S3 , 2	مخبر المهندسين	HCC1 / PORT	UTP 100 MPRS	غير موثقة
IDF3 TO ENGLAB	S4 , 1	مخبر المهندسين	HCC1 / PORT2	UTP 100 MPRS	USED
IDF3 TO ENGLAB	S4 , 2	مخبر المهندسين	HCC1 / PORT6	UTP 100 MPRS	USED
IDF3 TO ENGLAB	S5 , 1	مخبر المهندسين	HCC1 / PORT	UTP 100 MPRS	لاتعمل
IDF3 TO ENGLAB	S5 , 2	مخبر المهندسين	HCC1 / PORT	UTP 100 MPRS	لا تعمل
IDF3 TO ENGLAB	S6 , 1	مخبر المهندسين	HCC1 / PORT15	UTP 100 MPRS	USED
IDF3 TO ENGLAB	S6 , 2	مخبر المهندسين	HCC1 / PORT7	UTP 100 MPRS	USED
IDF3 TO ENGLAB	S7 , 1	مخبر المهندسين	HCC1 / PORT4	UTP 100 MPRS	USED
IDF3 TO ENGLAB	S7 , 2	مخبر المهندسين	HCC1 / PORT	UTP 100 MPRS	لاتعمل
IDF3 TO ENGLAB	S8 , 1	مخبر المهندسين	HCC1 / PORT19	UTP 100 MPRS	USED
IDF3 TO ENGLAB	S8 , 2	مخبر المهندسين	HCC1 / PORT	UTP 100 MPRS	غير موثقة
IDF3 TO R 203	S10	القاعة 203	HCC1 / PORT9	UTP 100 MPRS	Used

IDF3 TO R 203	S11	القاعة 203	HCC1 / PORT	UTP 100 MPRS	لا تعمل
IDF3 TO R202	S12	القاعة 202	HCC1 / PORT 14	UTP 100 MPRS	Used
IDF3 TO R202	S13	القاعة 202	HCC1 / PORT18	UTP 100 MPRS	Used
IDF3 TO R201	S14	القاعة 201	HCC1 / PORT24	UTP 100 MPRS	Used
IDF3 TO R201	S15	القاعة 201	HCC1 / PORT	UTP 100 MPRS	مأخذ معطل
IDF3 TO R204	S16	القاعة 204	HCC1 / PORT	UTP 100 MPRS	غير موجودة
IDF3 TO R204	S17	القاعة 204	HCC1 / PORT	UTP 100 MPRS	غير موجودة
IDF3 TO ELECTRLAB	S18	مخبر الكترونيات	HCC2 / PORT2	UTP 100 MPRS	USED
IDF3 TO ELECTRLAB	S19	مخبر الكترونيات	HCC2 / PORT3	UTP 100 MPRS	USED
IDF3 TO ELECTRLAB	S20	مخبر الكترونيات	HCC2 / PORT4	UTP 100 MPRS	USED
IDF3 TO ELECTRLAB	S21	مخبر الكترونيات	HCC2 / PORT5	UTP 100 MPRS	USED
IDF3 TO ELECTRLAB	S22	مخبر الكترونيات	HCC2 / PORT6	UTP 100 MPRS	USED
IDF3 TO ELECTRLAB	S23	مخبر الكترونيات	HCC2 / PORT7	UTP 100 MPRS	USED
IDF3 TO MANAGROO	S24	الهيئة الادارية		UTP 100 MPRS	

connection	Cable id	Room	Cross connection paired /port	Type of cable	Status
IDF4 TO R304	T1	القاعة 304	HCC1/PORT	UTP 100 MPRS	تم إزالتها
IDF4 TO R304	T2	القاعة 304	HCC1/PORT	UTP 100 MPRS	تم إزالتها
IDF4 TO R305	T3	القاعة 305	HCC1/PORT4	UTP 100 MPRS	USED
IDF4 TO R305	T4	القاعة 305	HCC1/PORT1	UTP 100 MPRS	USED
IDF4 TO R301	T5	القاعة 301	HCC1/PORT22	UTP 100 MPRS	USED
IDF4 TO R301	T6	القاعة 301	HCC1/PORT	UTP 100 MPRS	لا تعمل
IDF4 TO R302	T7	القاعة 302	HCC1/PORT23	UTP 100 MPRS	USED
IDF4 TO R302	T8	القاعة 302	HCC1/PORT21	UTP 100 MPRS	USED
IDF4 TO R303	T9	القاعة 303	HCC1/PORT	UTP 100 MPRS	لا تعمل
IDF4 TO R 303	T10	القاعة 303	HCC1/PORT20	UTP 100 MPRS	USED
IDF4 TO ACCOUNTING	T11	المحاسبة	HCC1/PORT5	UTP 100 MPRS	USED
IDF4 TO LIBRARY	T12 , 1	المكتبة	HCC1/PORT3	UTP 100 MPRS	USED
IDF4 TO LIBRARY	T12 , 2	المكتبة	HCC1/PORT	UTP 100 MPRS	لا يمكن الوصول لها

IDF4 LIBRARY	TO T13,1	المكتبة	HCC1/PORT	UTP 100 MPRS	لا يمكن الوصول لها
IDF4 LIBRARY	TO T13,2	المكتبة	HCC1/PORT	UTP 100 MPRS	لا يمكن الوصول لها

المشاكل والحلول المقترنة

❖ يوجد SWITCH معطل في الطابق الأرضي متصل به 18 نقطة اتصال ولحل هذه المشكلة : لدينا حلين

الحل المؤقت: يوجد لدينا بورتات على السويتش الثالث شاغرة يمكننا توصيل عدد معين من النقاط به وبالتالي نجعل المخبر مخدم بنصف عدد النقاط وهذا أفضل من بقائه دون اتصال

الحل الفعلي: يجب تركيب سويتش جديد

❖ تم العثور على أكبال غير موصولة إلى لوحة التجميع في طابق المخابر وتم توثيقها بأنها لا تعمل ولذلك يجب مراجعة التوصيلات وإعادة وصلها بسبب وجود نقاط غير موصولة إلى أي بورت

Cable id	room	Cross connection paired /port
G22,1	مخبر 2	HCC3/PORT
G22,2	مخبر 2	HCC3/PORT
G24,2	مخبر 2	HCC3/PORT
G28,1	مخبر 2	HCC3/PORT
G28,2	مخبر 2	HCC3/PORT

❖ يوجد العديد من النقاط معطلة (مكسورة) وبعضها فارغ كما هو مذكور في التوثيق السابق يجب إصلاحها

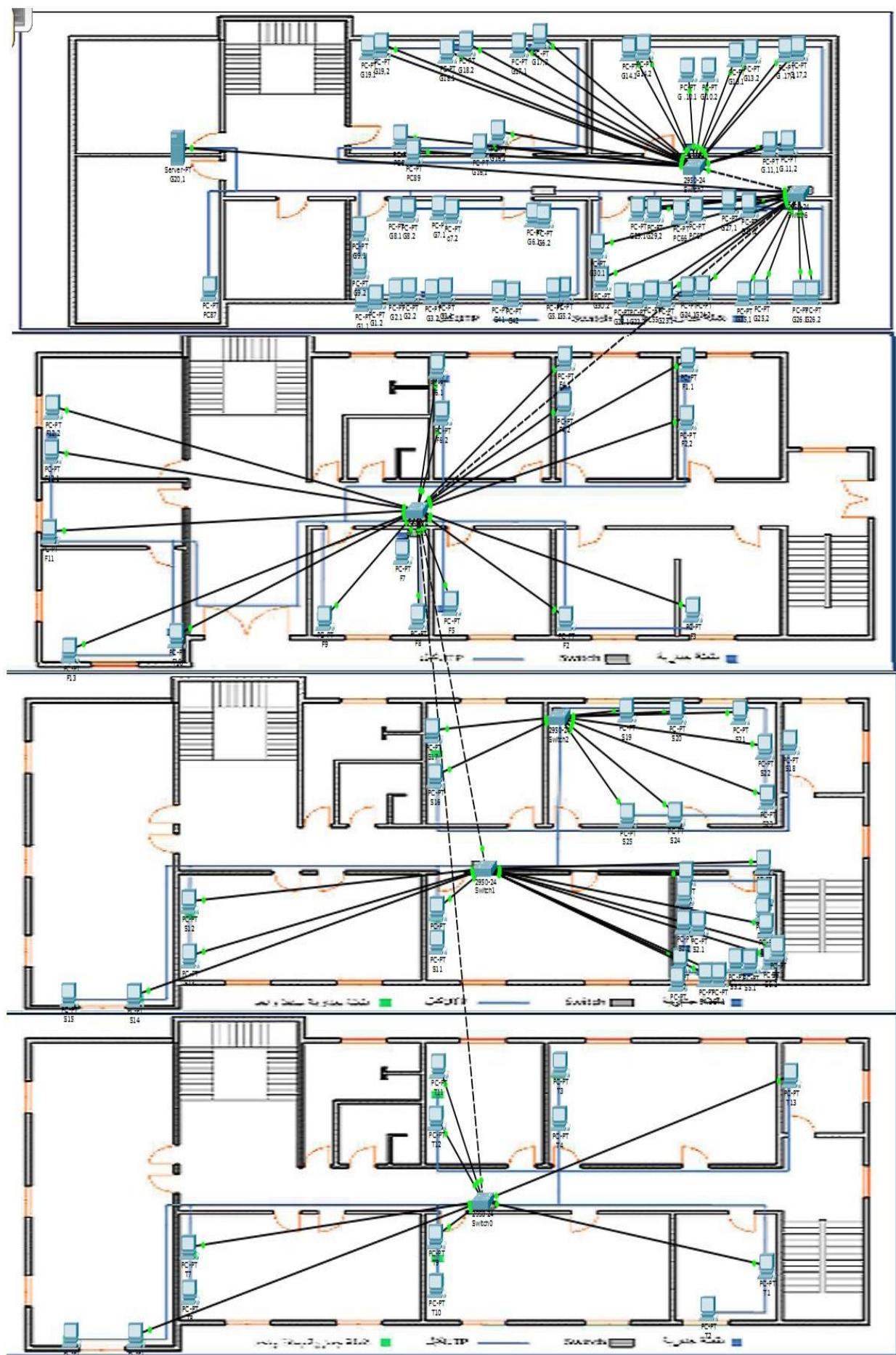
Cross connection paired /port	room	Cable id
HCC1/PORT	رئيس الدائرة	F5,1
HCC1/PORT	رؤساء الأقسام	F7,2

HCC1 / PORT	رؤساء الأقسام	F8 , 2
HCC1 / PORT	رؤساء الأقسام	F9 , 1
HCC1 / PORT	القاعة 201	S15

❖ يوجد بعض النقاط في الطابق الثاني والثالث رغم أنها متصلة إلى لوحة التجميع ولكنها لا تعمل قد تكون المشكلة في الكبلات أو في منافذ لوحة التجميع ويجب فحصها

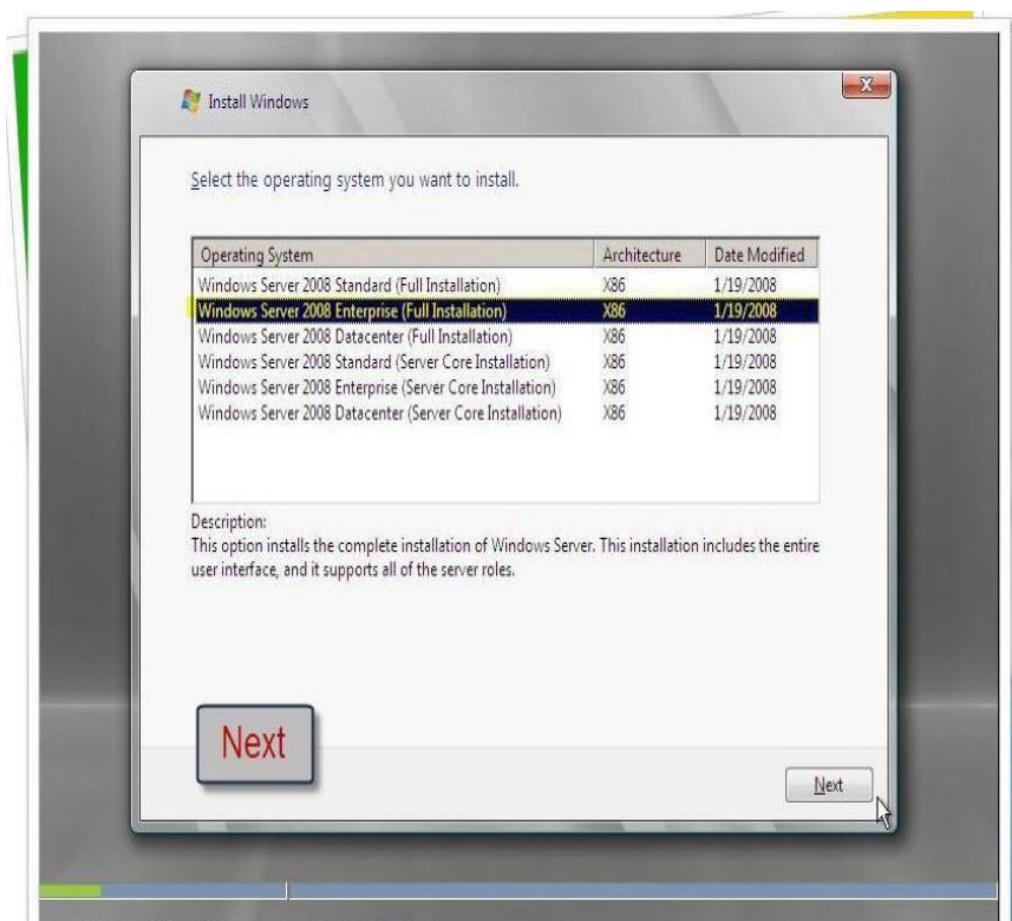
Cable id	room	Cross connection paired /port
S11	القاعة 203	HCC1 / PORT
T6	القاعة 301	HCC1 / PORT
T9	القاعة 303	HCC1 / PORT

وتم توثيق الجداول السابقة على شكل مخطط بواسطة برنامج tracer packet وتم إرفاق الملف مع ملفات المشروع



4_2 . خطوات تثبيت نظام التشغيل الـ 2008 :

يجب إتباع الخطوات بحسب الصور التالية



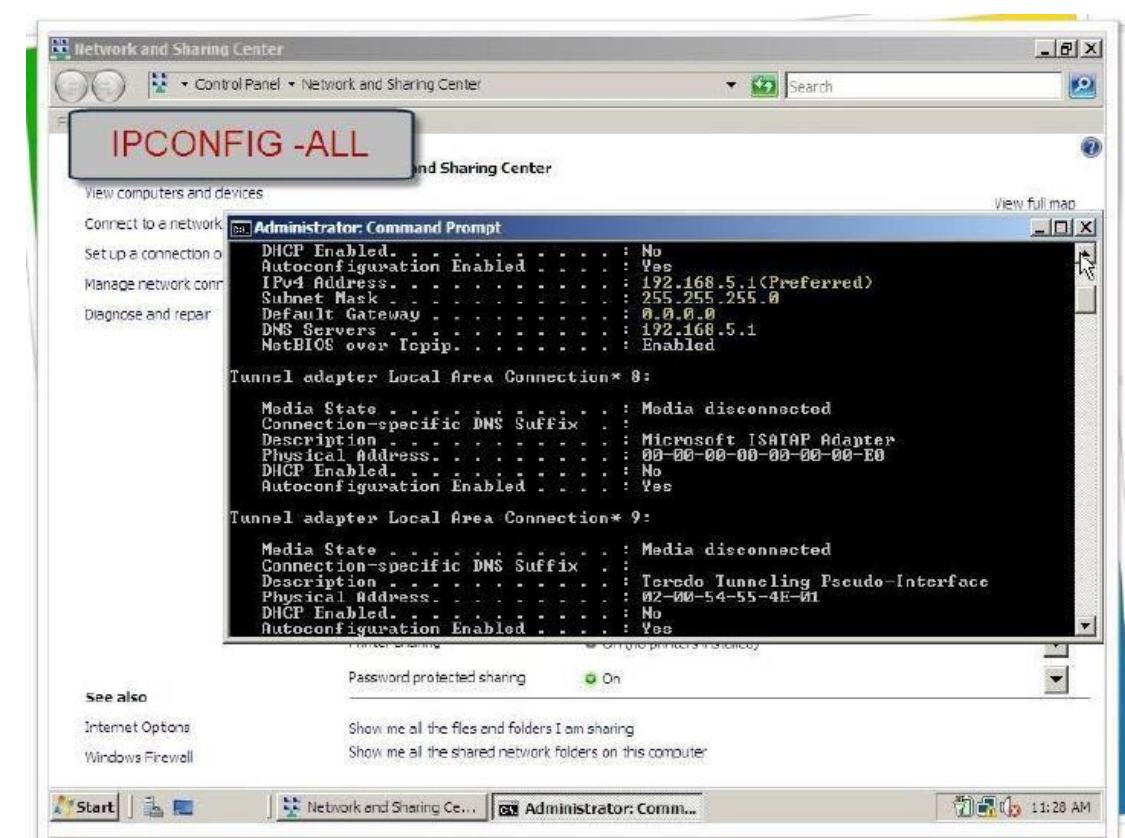
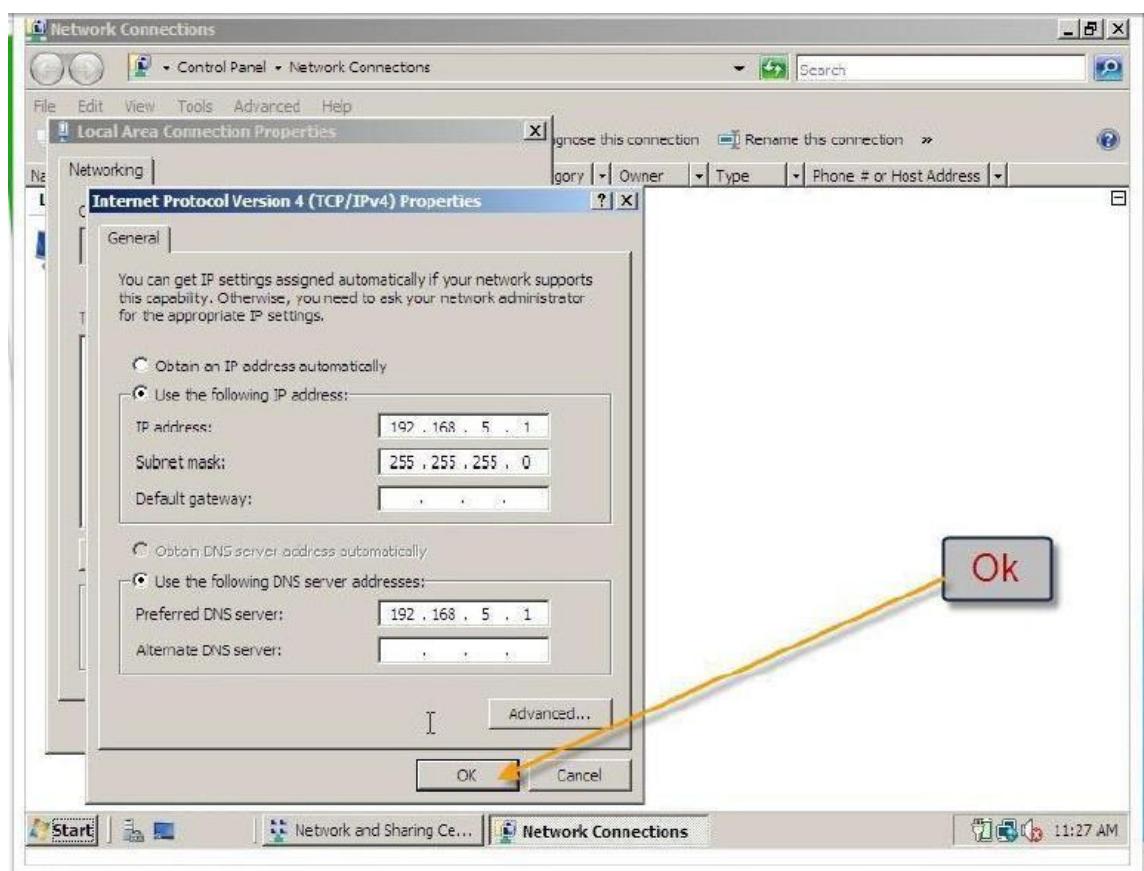


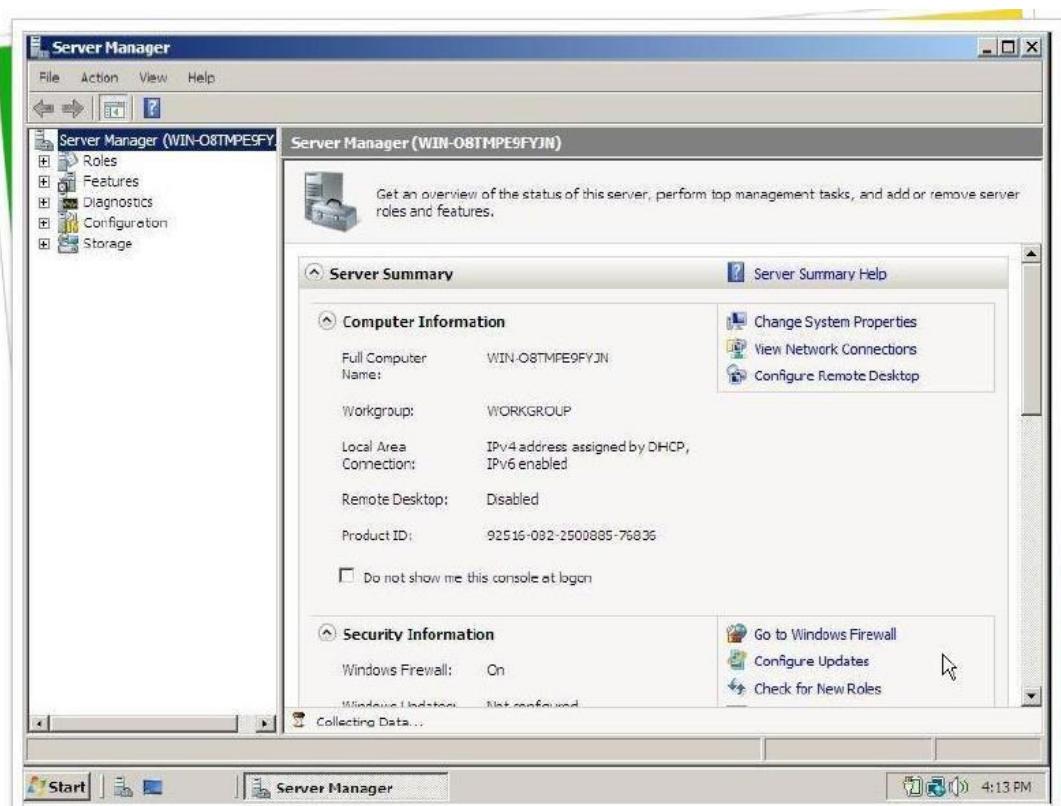


يجب وضع كلمة مرور معقدة أي مللفة من رموز وأحرف وأرقام ويجب ألا تقل عن 2 محارف.



يتم تحديد عنوان IP للسيرفر بشكل ستاتيكي، وكذلك تحديد عنوان dns وهو نفس عنوان ip أي أننا نقوم بجعل السيرفر هو مخدم dns بالإضافة إلى كونه متحكم للمجال





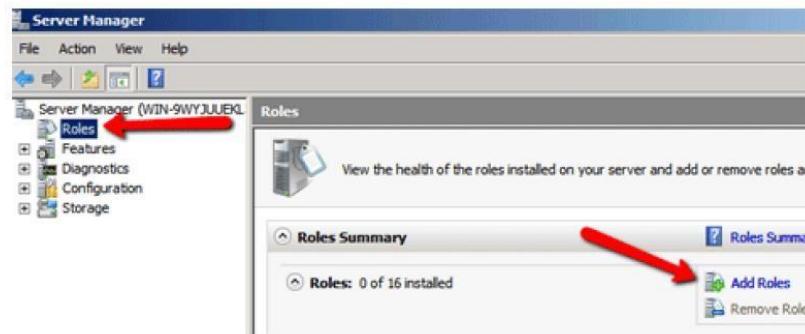
من خلال Role يتم تحديد الوظيفة التي سيقوم بها السيرفر من خلال إضافة مهمة جديدة له ، ويمكن جعل المخدم يقوم بمهمة واحدة فقط أو أكثر من مهمة ، وتخالف Feature عن Role بأن إضافة Feature تعني أن المهمة التي سيقوم بها السيرفر موجودة في Windows Server 2003 وغيرها موجودة في 2008 ، بينما إضافة Role أن المهمة تكون غير موجودة في كلا الإصدارين .

إعداد متحكم المجال :

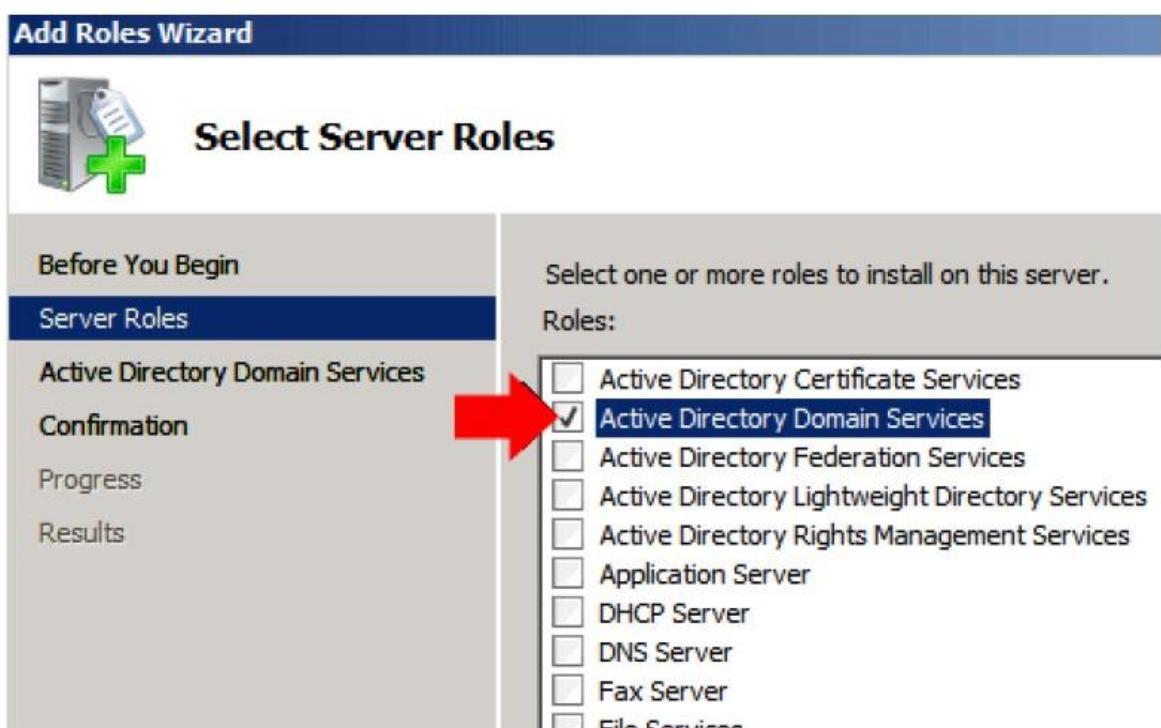
جهاز المخدم عندما يكون غير منضم إلى أي مجال يسمى standalone server ، أما عندما نسند إلى مهمة

الإدارة فيصبح متحكم للمجال dc ، وفي حال أسندا إليه أي وظيفة أخرى (غير متحكم المجال) وأضفناه إلى مجال ما فيسمى هذا المخدم member . server

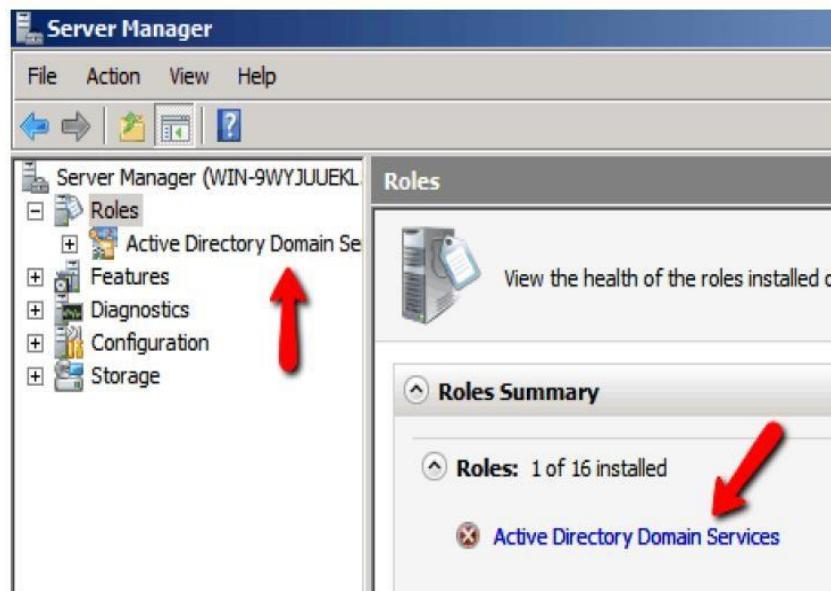
حتى يقوم المخدم بوظيفة إدارة الشبكة يجب إضافة خدمة active directory إلى هذا المخدم . وتحمّل هذا الخدمة موقع مركزي لإدارة وآمن الشبكة نفتح : server manager



: active directory

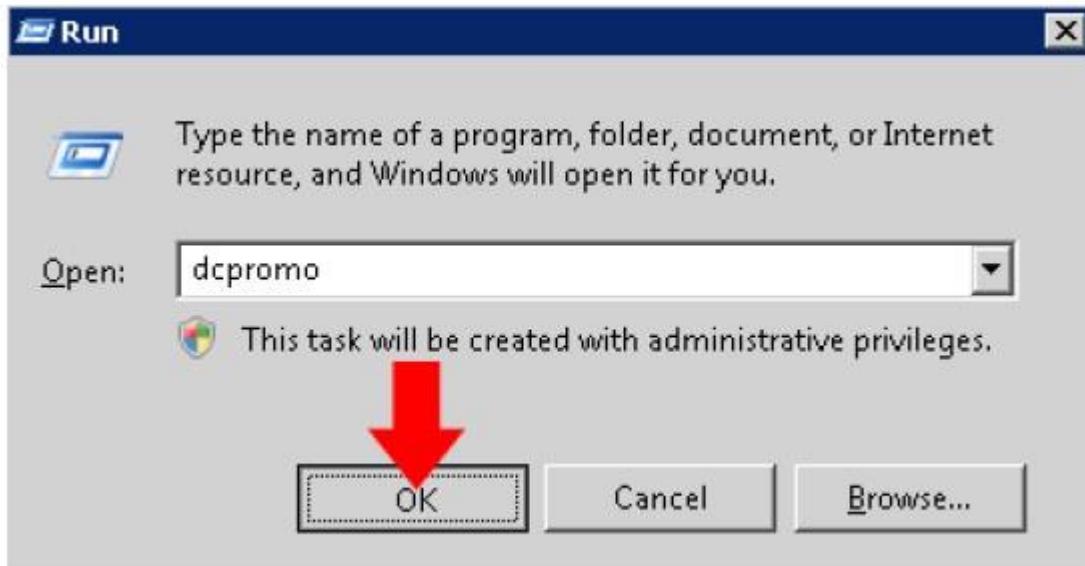


فيتم إضافة هذه الخدمة إلى قائمة الخدمات التي يقدمها المخدم . ولكن تحتاج هذه الخدمة إلى عملية إعداد تتضمن إنشاء شبكة المجال وتحديد مواصفاتها .



: active directory طريقة إعداد خدمة

من تبويب run من قائمة أبدأ نكتب (domain controller promote) : معنى ذلك أننا سنقوم الان بترقية الـ windows سيرفر 2008 من كونه سيرفر عادي إلى أن يصبح متحكم بالمجال .



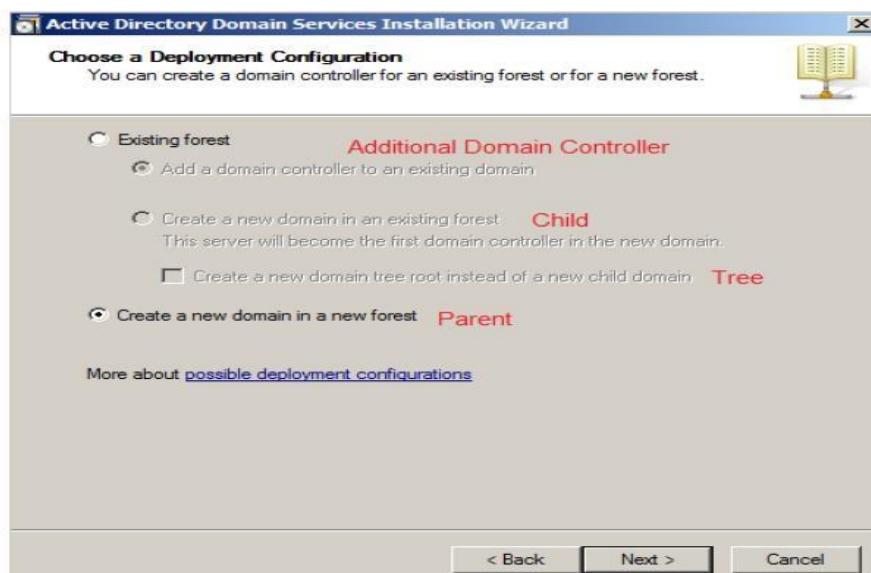
نختار advanced لكي نحصل على خيارات اعداد اكثـر ، ثم التالـي فـتـظـهـرـ نـافـذـةـ تعـرـيفـيـةـ نـخـتـارـ التـالـيـ

الخطوة التالية هي تحديد نوع متحكم المجال ، هل هو child أو tree أو additional أو new forest

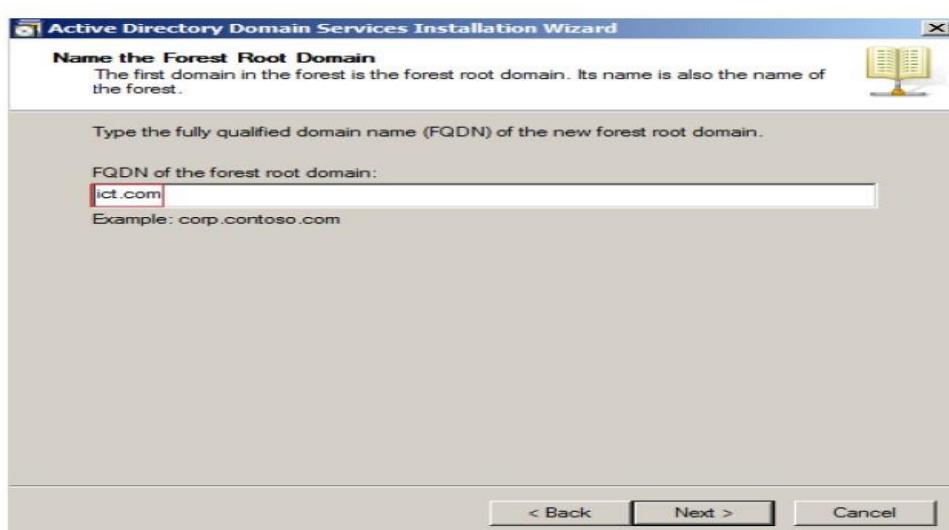
الخيار الأول: الشق الأول مهم وهو يمثل تفعيل controller additional domain : وفكرته أنه في حال حصول انهيار أو تعطل لمتحكم المجال الأساسي سوف تتقطع كامل الشبكة لأنه هو قاعدة البيانات لكافة الحسابات، لذلك يقوم بعمل نسخة إضافية (additional) بمثابة مرآة للنسخة الأساسية (primary) عند إضافة مستخدم مثلاً للمتحكم الأساسي يضاف تلقائياً في المتحكم الإضافي (وفى حال حصول عطل تقوم باستدامها . ويتم تفعيله من خلال اختيار الخيار الأول existing forest .

وبالنسبة للشق الثاني من الخيار الأول هو تحديد فيما إذا كان هذا المتحكم هو tree أو child لمجال ما موجود .

والخيار الثاني : هو الذي سنقوم بتفعيله والذي يحدد إنشاء مجال جديد parent (في غابة جديدة ويكون نوع متحكم المجال هنا primary)



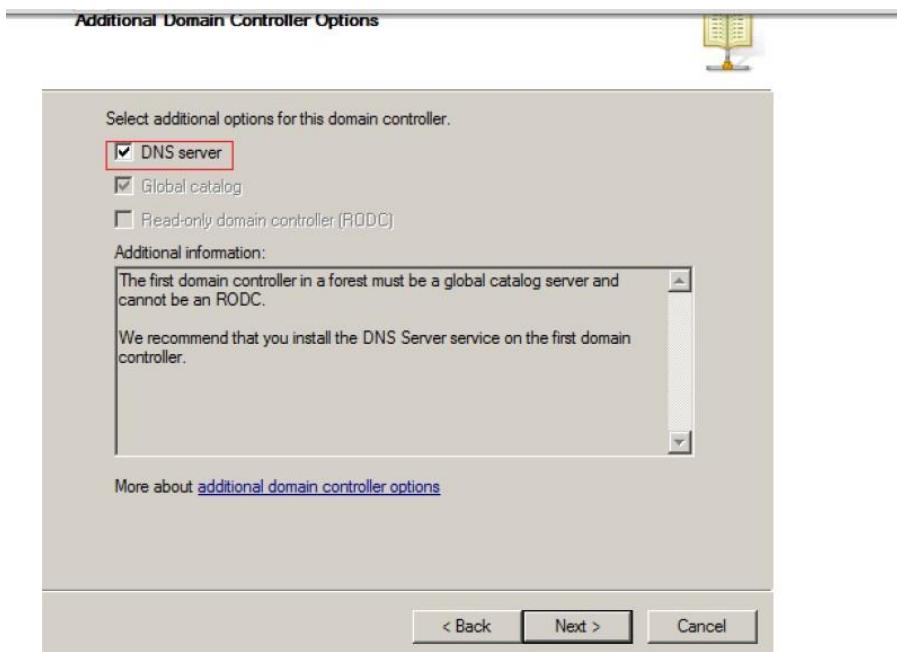
الخطوة التالية هي تحديد الاسم الكامل للمجال :) NAME



الخطوة التالية هي تحديد اسم المجال (NETBIOS NAME) ول يكن مثلا ICT.

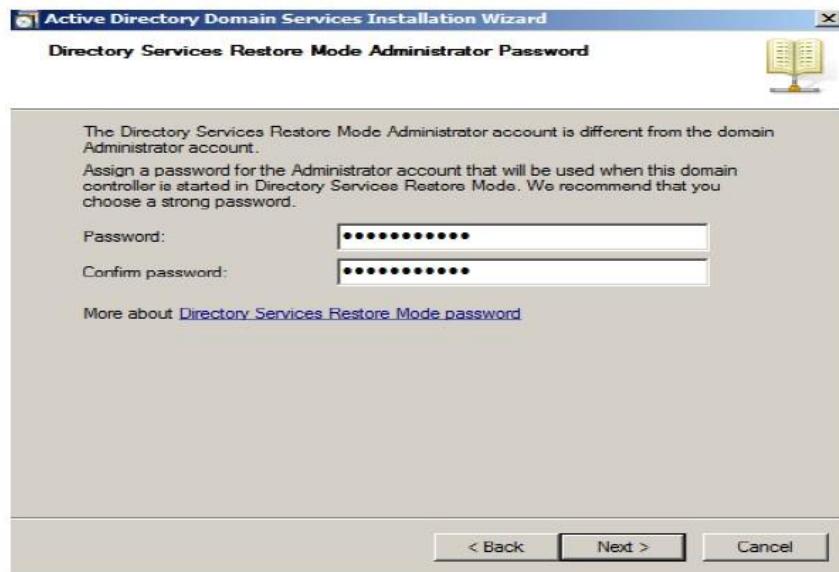
وبعد ذلك نحدد أي نوع (اصدارات) من سيرفرات CHILD TREE يدعم هذا المجال ، وهذا الخيار يحدد بحسب أنواع المخدمات المستخدمة في الشبكة ونختار مثلا أنه يدعم فقط خدمات Windows server

الخطوة التالية هي تنزيل خدمة dns :



بعد ذلك يتم تحديد المكان الافتراضي لتنزيل خدمة ntds وهي تحمل بشكل افتراضي على القرص C . ويجب أن تتوفر مساحة حرة 250MB على هذا القرص.

بعد ذلك نصل إلى Active Directory restore mode : أي إذا تعطل directory restore أو أريد أن أخذ منه نسخة احتياطية من الذي يحق له أن يعمل عملية الاستعادة هذه (هنا يجب وضع كلمة مرور معقدة .)



نضغط التالي فيعطي ملخص عن الإعدادات السابقة ومن ثم نختار finish ونقم بعد ذلك بإعادة تشغيل المخدم .

3_4 تقديم تصور عن مكاتب الكلية (دكاترة ومهندسين وطلاب عن طريق تنسيقهم ضمن وحدات تنظيمية ومجموعات ومستخدمين) organization unit : ,groups ,users

قمنا ببناء وحدة تنظيمية وقمنا بتنسيقها باسم HTMA تشمل وحدات التنظيمية التالية

-**الأقسام** :تشمل الوحدات التنظيمية الفرعية التالية : معلومات - اتصالات-نظم حاسوبية

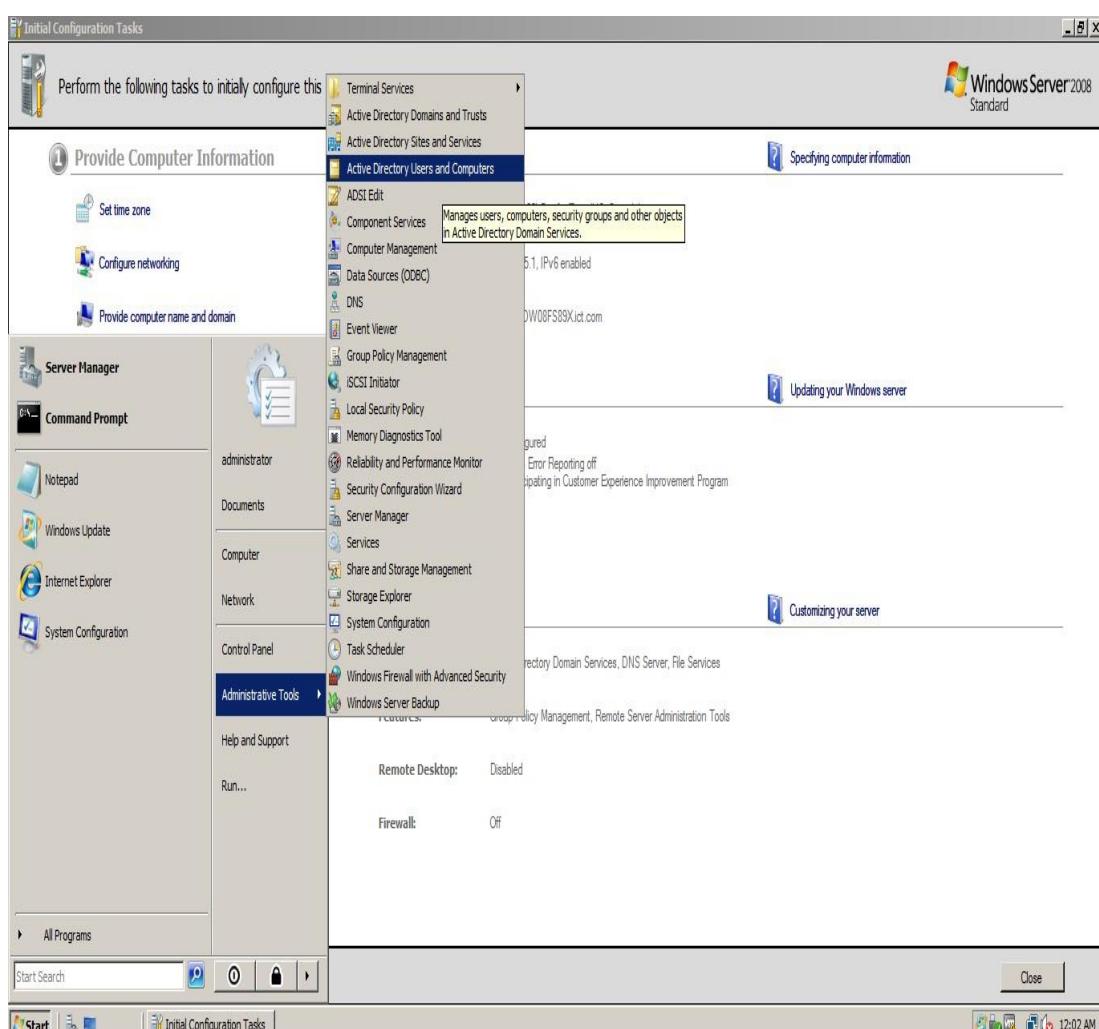
-**العميد ونوابه**:تشمل الوحدات التنظيمية الفرعية التالية: لعميد -نائب العميد

-**المكاتب الإدارية**:تشمل الوحدات التنظيمية الفرعية التالية: امتحاناتديوان- رئيس الدائرة - سكرتيرة العميد -شؤون الطلاب

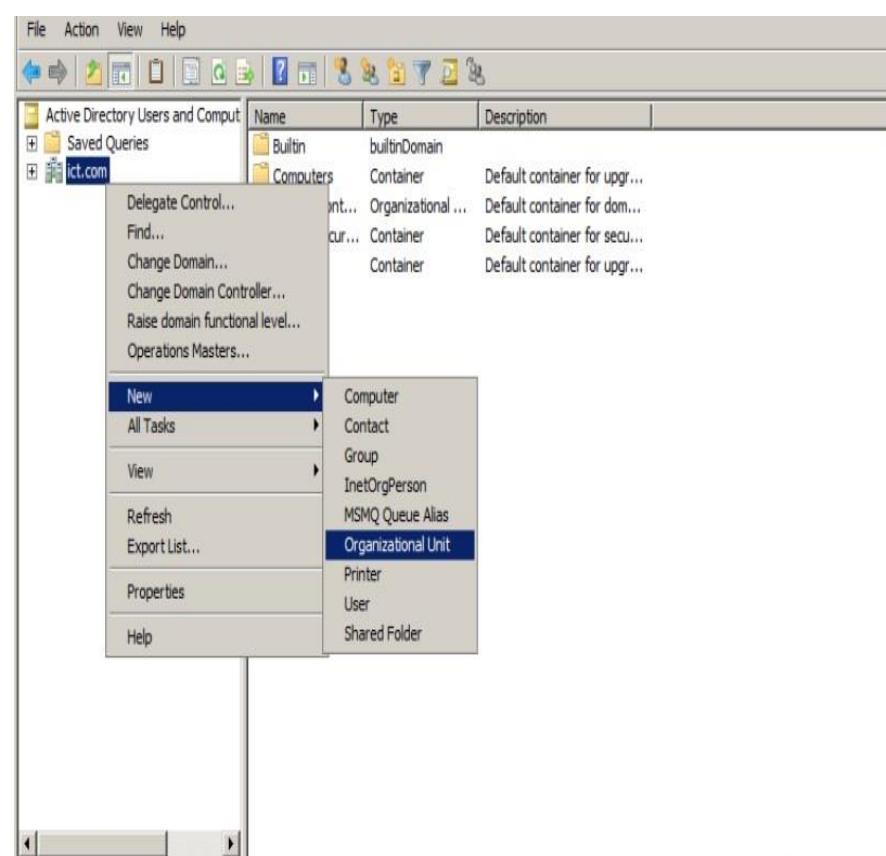
-**الطلاب**:تشمل الوحدات التنظيمية الفرعية التالية: سنة أولى-سنة ثانيةسنة ثالثة-طلاب الاتصالات - طلب المعلومات - الهيئة الإدارية

4_3_1. آلية إنشاء الوحدات التنظيمية :

يتم الوصول إلى active directory من قائمة أدوات أبدأ ومن ثم أدوات إدارية active directory users and computer



← new 2. ثم بالضغط على المجلد بالزر اليميني organization unit →



ثم بتطبيق الخطوات السابقة قمنا بالوصول إلى التصور التالي

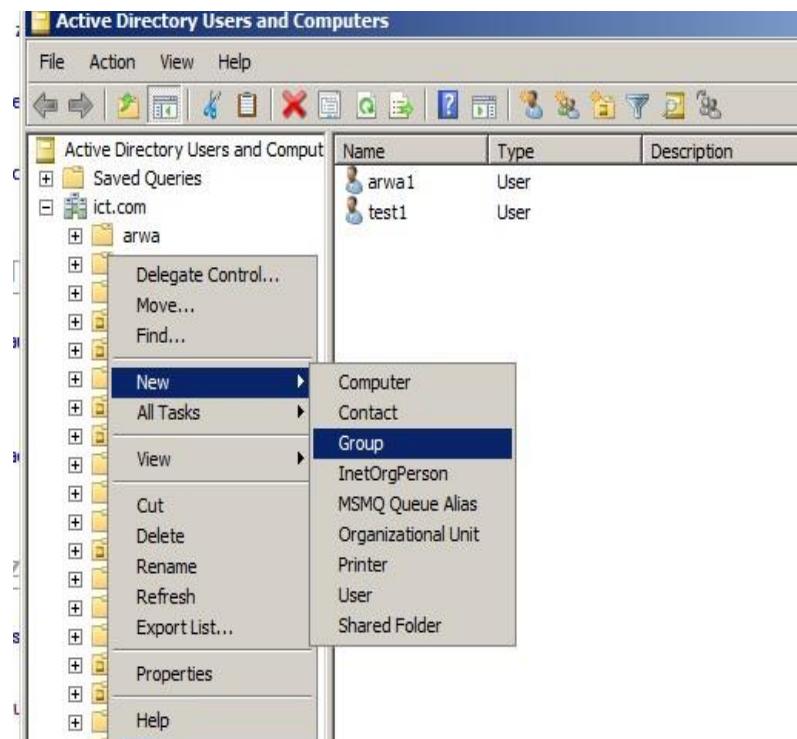


التصور

النهائي للكلية

3_4 .إنشاء الـ group :

بالضغط على زر اليميني على الوحدة التنظيمية المراد إنشاء مجموعة المستخدمين بداخلها ← new ← . Group

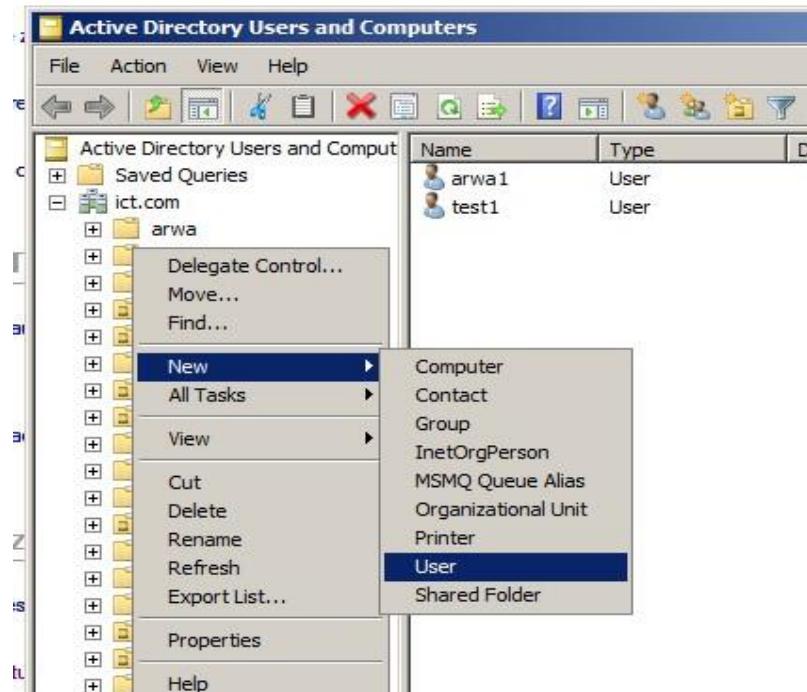


:group :الغاية من إنشاء ال

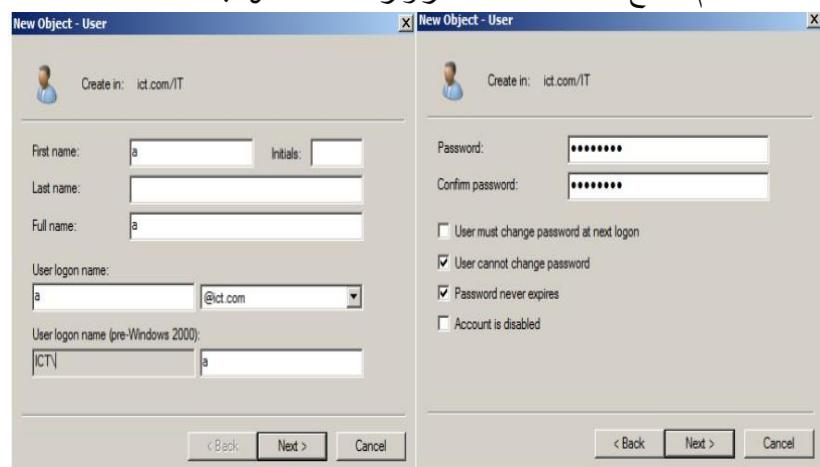
عند تطبيق سياسة أو مشاركة على ال group فأنها تطبق على جميع المستخدمين ضمن المجموعة وعند إضافة أي مستخدم جديد إلى ال group يطبق عليه السياسات المطبقة على ال group تلقائيا

3_3.إنشاء المستخدمين :

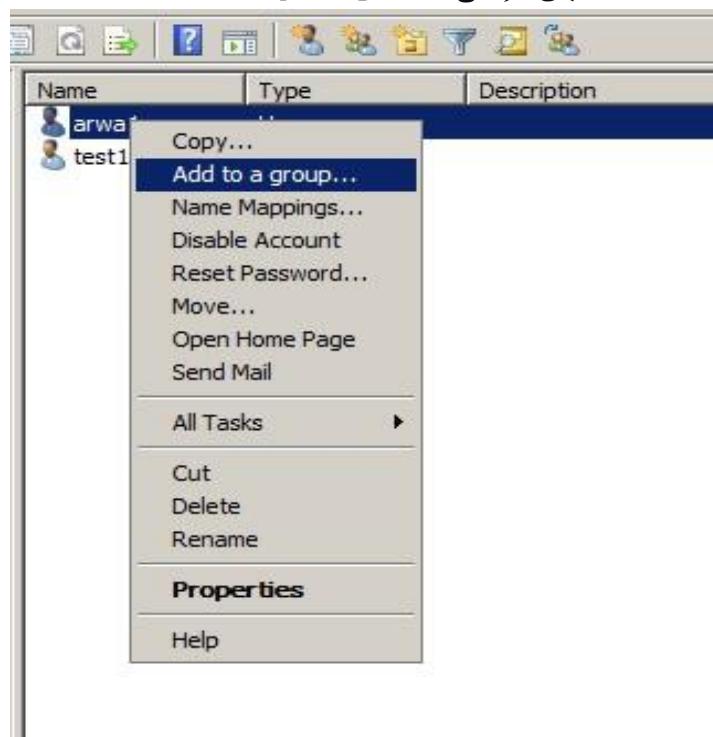
بالضغط على الوحدة التنظيمية التي نريد إنشاء المستخدمين بداخلها ←
user ← new



ثم نحدد اسم كل مستخدم مع كلمة المرور الخاصة به



ثم نقوم بإضافة المستخدمين إلى الـ :group



بتطبيق الخطوات السابقة قمنا بإنشاء عدد من المستخدمين وتم توثيقهم في الجداول التالية مع كلمات مرور أولية :

كلمة المرور	اسم المستخدم
Faict123!@#	D.fadigisnah
Mdict123!@#	D.mirnadrgam
Mmict123!@#	D.mohammednaser
Maict123!@#	D.mohammedanber
sbict123!@#	D.mohammedsadeq
Naict123!@#	D.najimohammed

Lict123!@#	D.loubnahali
Aict123!@#	D.ahmedibrahem
Noict123!@#	Nourjeibali
Geict123!@#	Genwaria

ouict123!@#	Aula ibrahem
Miict123!@#	Mai ali
Hhict123!@#	Hasanalhassab
Alict123!@#	Alaamahfouz
Mnict123!@#	Mirnajbara
Mrict123!@#	Marahmfleh
Mdict123!@#	Mohammed omran
Llict123!@#	Lailaismaael
Yyict123!@#	D.Yaroubdayoub
Jsict123!@#	D.jafarsleman
Mbict123!@#	D.maheribraem
Aasict123!@#	Ali abo saeed
Mhict123!@#	Mary albahlit
Neict123!@#	Nerminobeid
Rict123!@#	Reemalean
Hsict123!@#	Halasleman
Raict123!@#	Raedjabour
Piict123!@#	Reemissa
Amict123!@#	Ammarhasan
Shict123!@#	Shroukmostafah
Zoict123!@#	Zeinabomran
Hhict123!@#	D.hasanalboustani
Ssict123!@#	D.souzysaleh
Ddict123!@#	D.mohammedmolhem
Neict123!@#	Noumayounes
Nnict123!@#	Ranahasan
Kict123!@#	D.ranimknaj
Boict123!@#	Boulosalghoury
Salict123!@#	D.salahnouralden
Ghict123!@#	D.ghassanmohammed
Nict123!@#	Nabelhasan
Sy1ict123!@#	St1y1
Sy2ict123!@#	Std2y1
Sy3ict123!@#	Std3y1
Sy4ict123!@#	Std4y1
Sy5ict123!@#	Std5y1
S1y2ict123!@#	Std1y2

S2y2ict123!@#	Std2y2
S3y2ict123!@#	Std3y2
S4y2ict123!@#	Std4y2
S5y2ict123!@#	Std5y2
S1y3ict123!@#	Std1y3
S2y3ict123!@#	Std2y3
S3y3ict123!@#	Std3y3
S4y3ict123!@#	Std4y3
S5y3ict123!@#	Std5y3
S1y4ict123!@#	Std1y4
S2y4ict123!@#	Std2y4
S3y4ict123!@#	Std3y4
S4y4ict123!@#	Std4y4
S5y4ict123!@#	Std5y4
S1y5ict123!@#	Std1y5
S2y5ict123!@#	Std2y5
S3y5ict123!@#	Std3y5
S4y5ict123!@#	Std4y5
S5y5ict123!@#	Std5y5
Mohict123!@#	Mohammed ferzat
Ouiict123!@#	Oulaali
Yoict123!@#	Yousefabdo
Maict123!@#	Maissaleh

Atict123!@#	Aatidal hussen
Bobict123!@#	Bothina hasan
Booict123!@#	Bouthina kalifah
Faict123!@#	Faten rostom
Hat123!@#	Hatem ali
Mumict123!@#	Mohammed souliman
Aatict123!@#	Attidal masry
Ahict123!@#	Ahlam alomr
Liict123!@#	Lial hamdan
Mnict123!@#	Manal mouhammed
Momict123!@#	Mouhammed alshimaly
Ramict123!@#	Rama saleh
Sriict123!@#	Sirag ganem
Soict123!@#	Souzan shadod
Yaict123!@#	Yara assad
Leict123!@#	Lenda drbo

Meict123!@#	Maisaa hasan
Mayict123!@#	Maya ahmmmed
Raiict123!@#	Ramia saeed
Rzict123!@#	Roz ibrahim
Sheict123!@#	Shereen knag
Sosict123!@#	Souzan ahmmmed
Laict123!@#	Lames gahgah

Active Directory Users and Computers

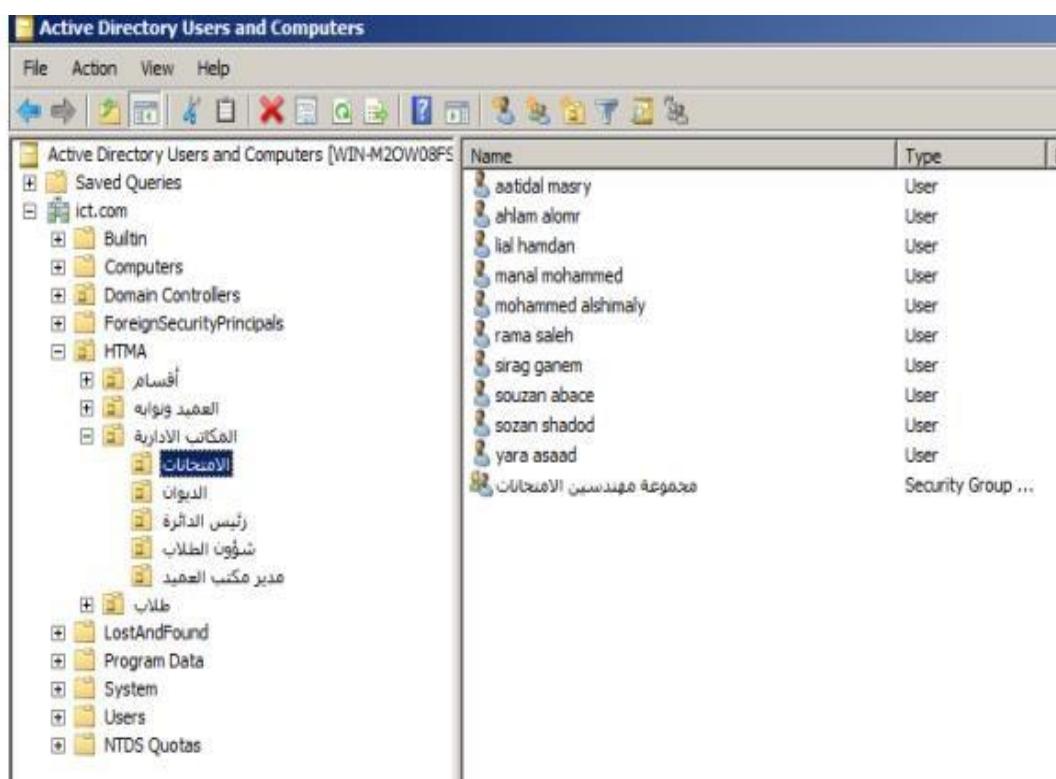
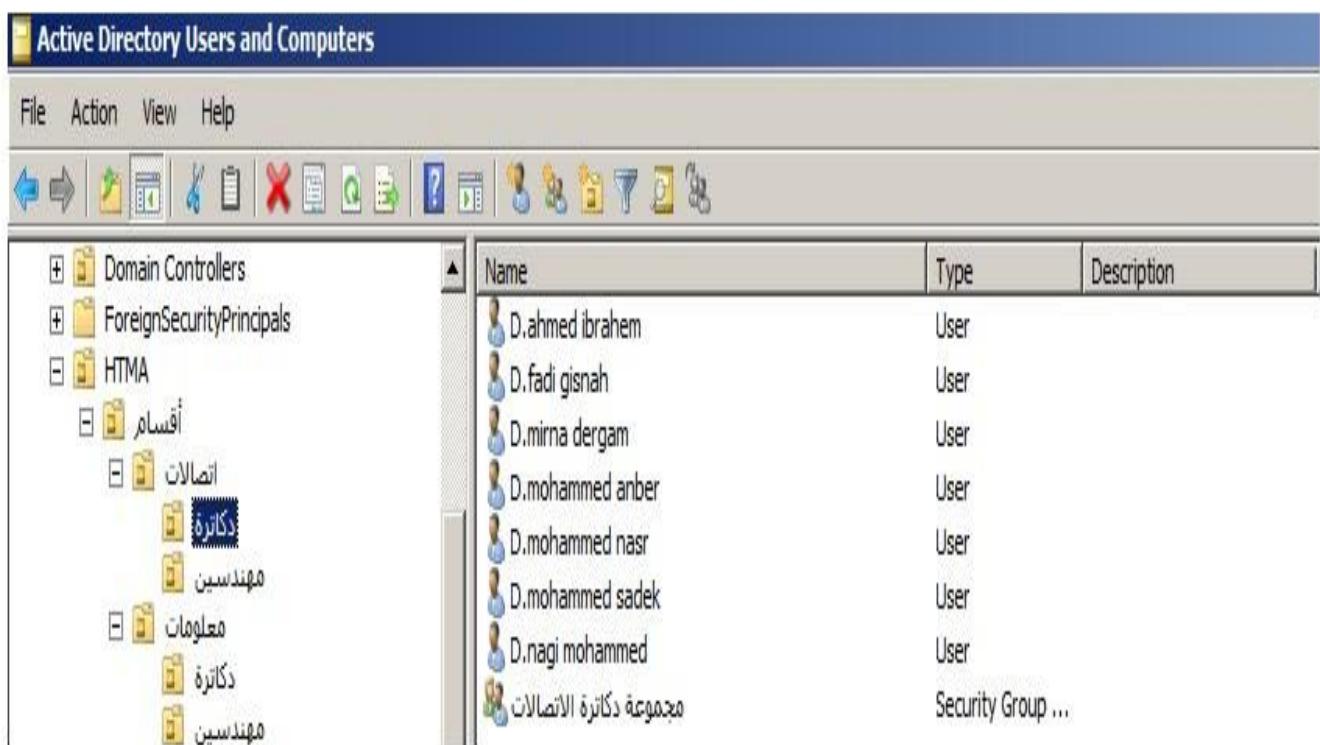
File Action View Help

Active Directory Users and Computers [WIN-M2OW08FS]

- Saved Queries
- ict.com
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - HTMA
 - أقسام
 - العميد ونوابه
 - المكاتب الادارية
 - الامتحانات
 - الديوان

Name	Type	Descript
aatidal masry	User	
ahlam alomr	User	
lial hamdan	User	
manal mohammed	User	
mohammed alshimaly	User	
rama saleh	User	
sirag ganem	User	
souzan abace	User	
sozan shadod	User	
yara asaad	User	
مجموعة مهندسين الامتحانات	Security Group ...	

شكل a_3_3_4

شكل b_3_3_4
شكل c_3_3_4

4. بناء نظام المشاركة :

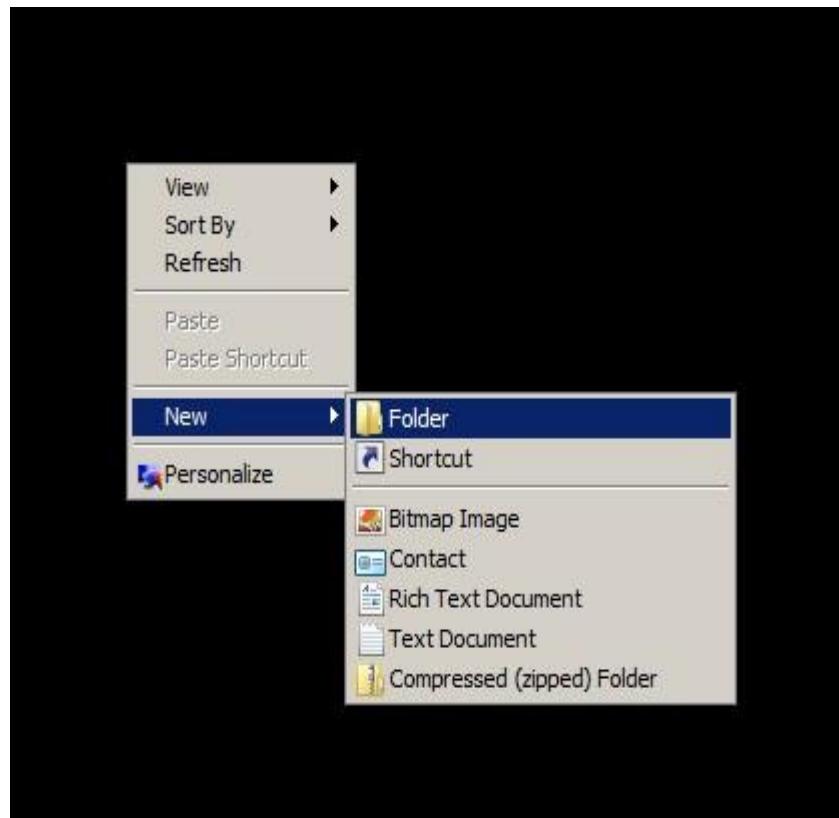
تكللت جهود الإنسان بالنجاح في تطوير حياته التي سعى إلى تطويرها منذ فجر التاريخ، والتي بدأها منذ بدء الخليقة ، ضمن قدراته المادية والعقلية ، حتى وصلنا إلى ما نحن عليه الآن من تطور تكنولوجي وغيره في حياتنا ، حتى أصبحنا في رفاهية لم يرها القدماء أبداً . مع مرور العصور ، بدأ الإنسان بالتفكير بابتكار طرق ووسائل تساعده على التواصل مع الآخرين ، فبدأت من (الحمام الراجل) ، ومن ثم ظهرت فكرة البريد العادي ، لكن عيوب هذه الوسائل أكثر من إيجابياتها ؛ حيث تستغرق وقتاً طويلاً وجهداً كبيراً في إيصال الرسالة أو المعلومة المطلوب إيصالها في وقت محدد للشخص

المرسل إليه ، حتى التواصل مع أفراد المنطقة الواحدة التي تفصلهم مسافات كان صعباً بعض الشيء ، لكن ليس مع حلول عصر السرعة والتكنولوجيا ؛ حيث ظهرت الاتصالات في بداية الأمر ، ومن ثم ظهرت الحواسيب ، ففكر الإنسان كثيراً ، باستفادة من جهاز الحاسوب مع الاتصالات معاً ، لجعلها وسيلة اتصال ، وعمل جاهداً حتى نجح في ذلك ، وأطلق الإنسان الشبكات ، ليتسع نطاقها وتشمل العالم كله

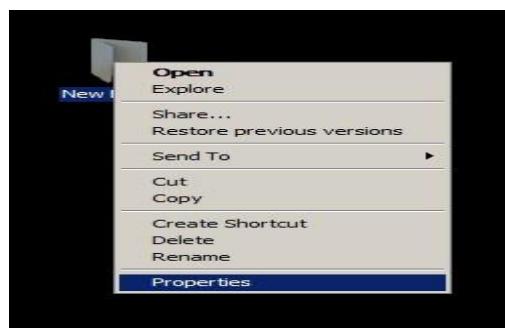
وللقيام بمشاركة الموارد بسهولة ضمن الكلية فنحن بحاجة إلى شبكة داخلية كما أوردنا سابقاً طريقة تصميمها فماذا تعني المشاركة :

آلية مشاركة الموارد : هي السماح للمستخدمين بالوصول إلى الموارد على الشبكة ، هذه الموارد ممكن أن تكون بيانات أو تجهيزات ، عن طريق الاتصال بالجهاز التي تكون هذه الموارد مشاركة عليه .

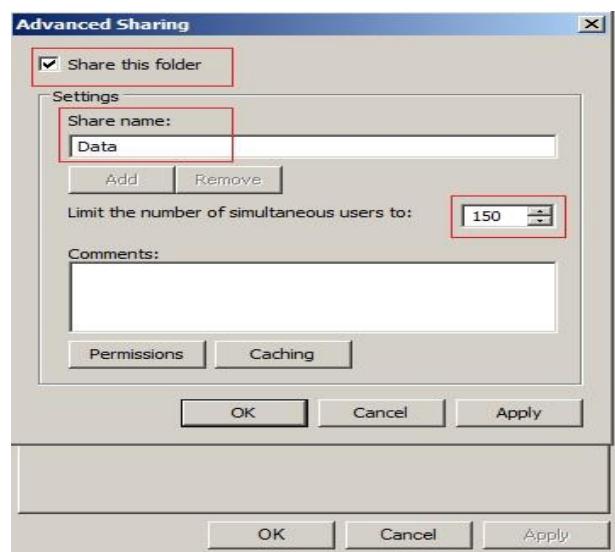
1. ننشأ مجلد على سطح المكتب لجهاز DC



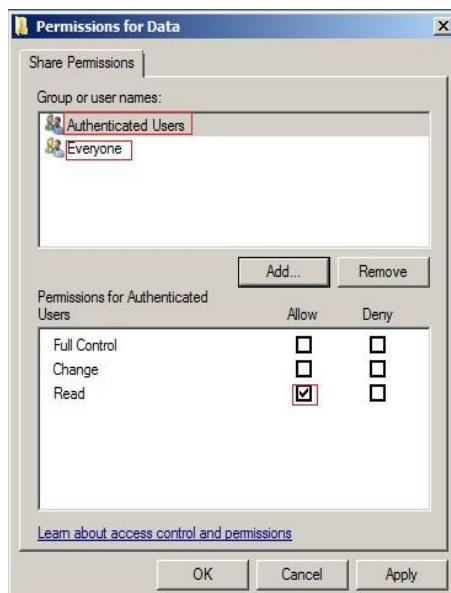
1. نحدد اسم للمجلد وذلك بحسب الملفات المسؤول عن مشاركتها
2. ونفتح تبويب المشاركة



2. من خيارات متقدمة نفعل خيار مشاركة المجلد، ونحدد عدد المستخدمين الذي يمكنهم الوصول معاً إلى هذا المجلد



3. نفتح الصلاحيات : permission فنجد الصلاحيات الافتراضية للجميع هي Everyone ، معنى ذلك أن أي مستخدم يستطيع فقط يقرأ محتوى المجلد ، نضيف إلى القائمة Authenticated User .



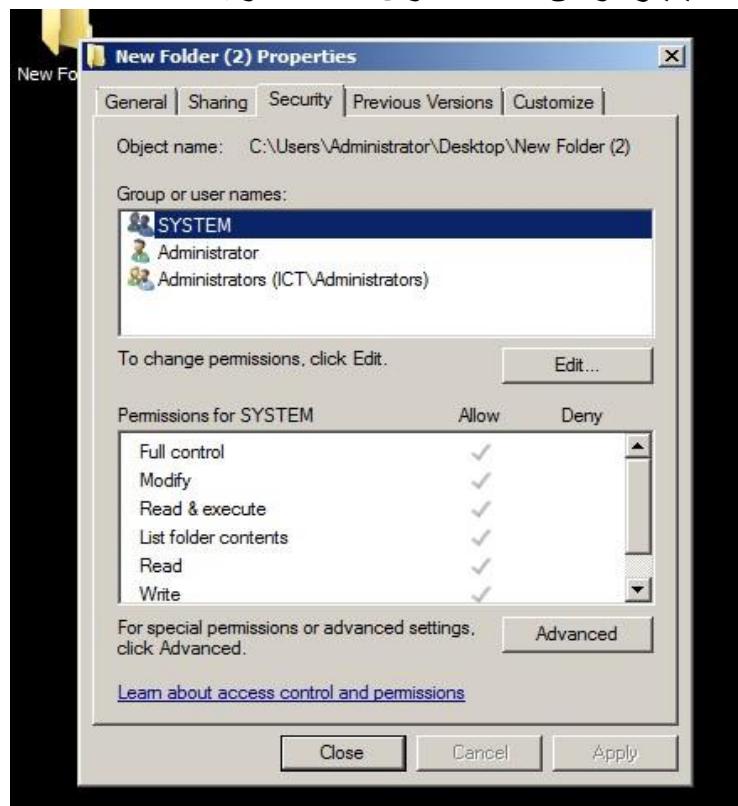
ماذا تختلف Everyone عن Authenticated User ؟ Everyone أي مستخدم (منضم للمجال أو غير منضم) يمكنه الوصول إلى المجال (حتى لو كان في مجموعة WORKGROUP بمفرد أنه يعرف عنوان IP للجهاز الموجود عليه المجال المشارك ، بينما Authenticated User حسرا المستخدمين الموجودين في المجال أي الذين لديهم حساب في Active Directory لذلك وبشكل افتراضي يتم حذف Everyone من قائمة الصلاحيات ونضيف Authenticated User في حال أردنا أن نجعل المجلد متاح لجميع المستخدمين المسجلين في المجال . وكذلك نضيف Administrator ونعطيه

ولكن عندما نريد إضافة مستخدمين بشكل مخصص نقوم User ونعطيهم من ثم نضيف المستخدمين المحددين ونعطيهم Administrator وبصلاحيات تحكم كاملة (مع الإبقاء على الصلاحيات المطلوبة) Full Control Authenticated بحذف

1. ونقوم أيضاً بتفعيل المشاركة على مستوى Share وبالصلاحيات السابقة

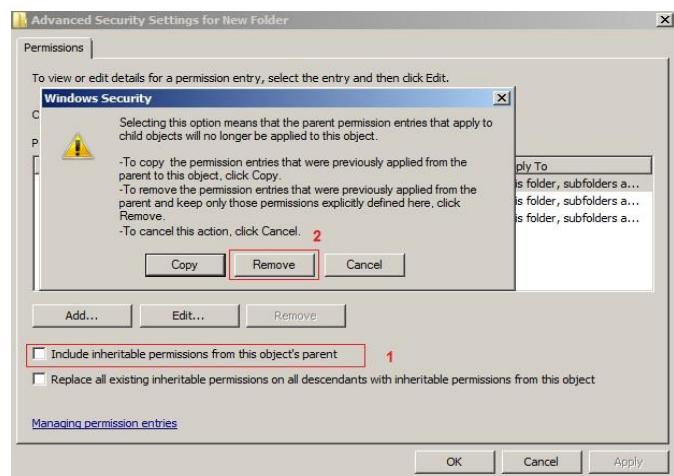


4. نضيف الصلاحيات المطلوبة من تبويبه security التي تمنح صلاحيات للمستخدم أقل من تغيير وفق المستوى المطلوب



ملاحظة : إذا كان نوع نظام الملفات على المخدم FAT فلا يوجد تبويب Security، لذلك من أجل تحقيق المشاركة الفعالة يجب أن يكون نوع نظام الملفات NTFS.

1. من تبويب Security نختار Advanced ومن ثم Edit ومن ثم نلغى خيار الوراثة ونزييل كامل خيارات الوراثة الافتراضية :



1. ومن ثم نضيف إلى قائمة المدير ونعطيه كامل الصلاحيـة Administrator: Full Control **الصلاحيـات المخصـصة:**

- a. صلاحيـة read: نستطيع فقط أن نقرأ الملف النصـي.
- b. صلاحيـة Read & execute : نستطيع فقط أن نقرأ الملف النصـي وكذلك تنفيـذ المـلف التنفيـذـي
- c. صلاحيـة Write: يستطيع المستخدم أن ينشـأ مجلـد وأن يكتب فيه ولكن لا يستطيع إعادة تسمـيـته ولا يستطيع أن يحـذـفـه
- d. صلاحيـة Modify : نستطيع أن نجري أي شيء على المـجلـد المـشارـك وهـي تـقـابـلـ فيـ المـشارـكـةـ changeـ . e. صلاحيـة Full control : أعلى صلاحيـة مـمـكـنةـ تعـنيـ التـحـكمـ الكـامـلـ f. صلاحيـة List content of folder : نستطيع فقط أن نفتحـ المـجلـدـ ولا نستطيع أن ننفذـ الأمرـ التنفيـذـيـ كماـ أنـناـ لاـ نستطيعـ أنـ نفتحـ المـملـفـ النـصـيـ

b. ماذا تختلف صلاحيـة التـحـكمـ الكـامـلـ عنـ صـلاـحيـةـ التـغـيـيرـ؟

الجواب : في التـحـكمـ الكـامـلـ يمكنـ أنـ أـضـيفـ أـشـخـاصـ إـلـىـ قـائـمةـ الصـلاـحيـاتـ وـحتـىـ يـمـكـنـ أنـ اـحـذـفـ Adminis~tratorـ منـ قـائـمةـ الصـلاـحيـاتـ،ـ بيـنـماـ فيـ تـغـيـيرـ لـيـمـكـنـهـ التـعـديـلـ أـبـدـاـ فـيـ الصـلاـحيـاتـ المـمـنـوـحةـ لـلـأـشـخـاصـ عـلـىـ المـجلـدـ المـشارـكـ،ـ سـوـاءـ إـضـافـةـ مـسـتـخـدـمـينـ أوـ حـذـفـ آخـرـينـ.

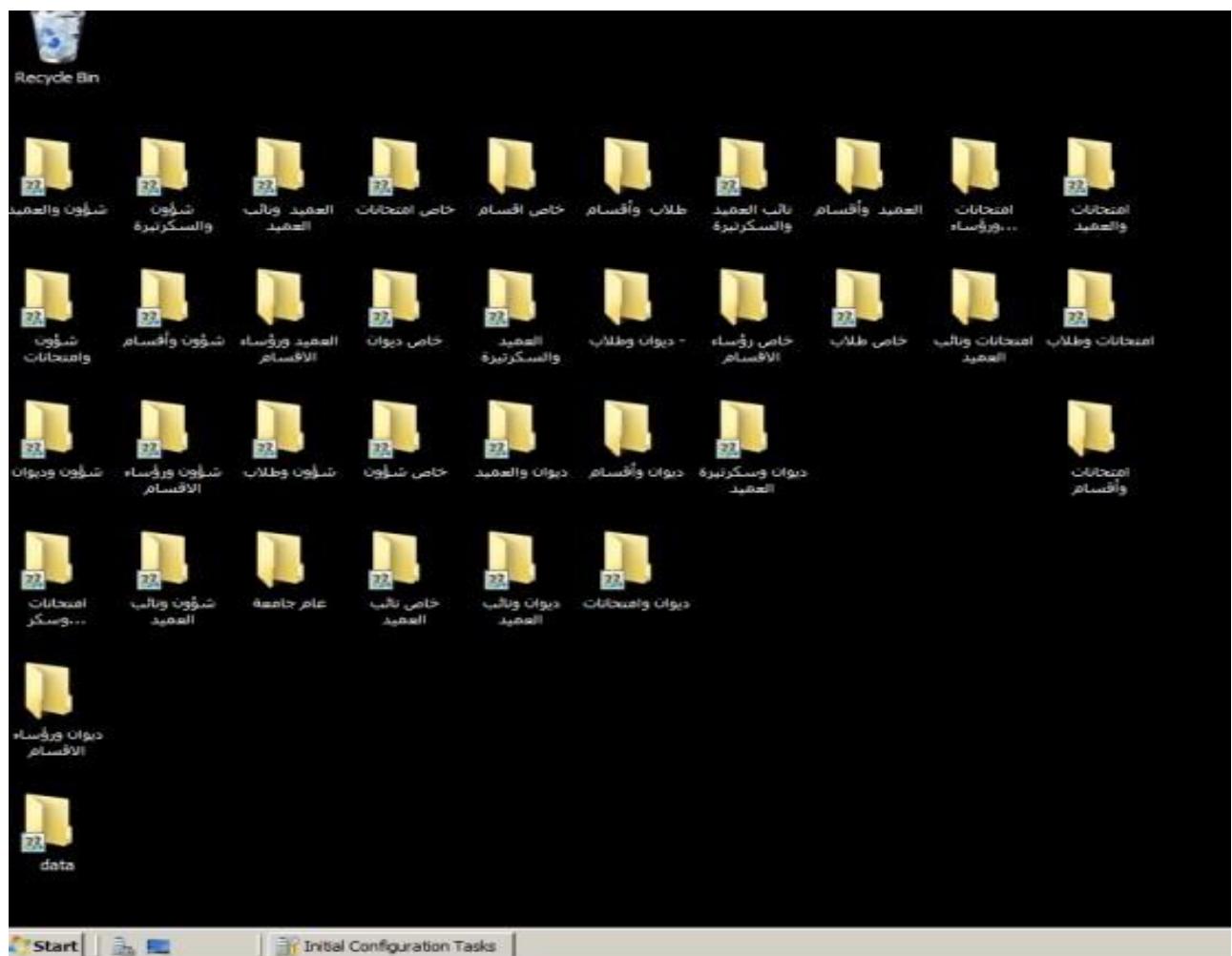
المـشارـكـةـ بـاـسـتـخـدـامـ Shareـ وـلـيـسـ Advanced Sharingـ : عند اختيار طريقة المـشارـكـةـ Shareـ يـفـعـلـ تـلـقـائـيـاـ إـعـدـادـاتـ المـشارـكـةـ لـSharingـ وـSecurityـ

إـذـاـ قـمـنـاـ بـعـمـلـيـةـ المـشارـكـةـ لـمـسـتـخـدـمـ معـيـنـ فـقـطـ مـنـ (Advanced Shareـ وـلمـ نـطـقـ Securityـ وـلاـ

طـرـيقـةـ المـشارـكـةـ) Shareـ ،ـ عـلـيـ 1ـ تـطبـقـ السـيـاسـةـ الـأـكـثـرـ تـقـيـداـ لـذـكـ لـنـ يـكـونـ المـجـلـدـ مـشـارـكـ عـبـرـ الشـبـكـةـ ،ـ لـحلـ هـذـهـ المشـكـلـةـ نـكـونـ أـمـامـ خـيـارـيـنـ:ـ

- ـ إـمـاـ الـذـهـابـ إـلـىـ تـبـوـيـبـ Securityـ وـإـضـافـةـ المـسـتـخـدـمـ بـالـصـلاـحيـاتـ الـمـحدـدةـ .ـ
- ـ أـوـ نـخـتـارـ Shareـ فـيـقـومـ تـلـقـائـيـاـ بـتـفـعـيلـ المـشارـكـةـ عـلـىـ Securityـ وـفقـ الصـلاـحيـاتـ الـمـحدـدةـ

وبـعـدـ تـطـبـيقـ الـخـطـوـاتـ السـابـقـةـ قـمـنـاـ بـتـشـكـيلـ مـجـمـوعـةـ مـنـ مـلـفـاتـ المـشارـكـةـ الـتـيـ تـضـمـنـ مـشـارـكـةـ الـمـوـارـدـ ضـمـنـ الشـبـكـةـ عـلـىـ أـكـمـلـ وـجـهـ مـمـكـنـ تـمـ أـنـشـاءـ مـجـمـوعـةـ المـجـلـدـاتـ التـالـيـةـ



ملفات المشاركة

وفق مجموعة مجلدات المشاركة السابقة فإن أي مكتب إداري سيكون بإمكانه مشاركة ملفاته مع أي مكتب إداري آخر ضمن الجامعة

تتم آلية المشاركة وفق التالي:

- لكل مكتب إداري مجلد خاص به مع كل مكتب إداري آخر ضمن الجامعة :

مثال: مكتب شؤون الطالب لديه المجلدات التالية:) شؤون وطلاب ، شؤون والعميد ، شؤون وامتحانات ، شؤون ورئيس الدائرة ، شؤون ونائب العميد ، شؤون وسكرتيرة العميد ، شؤون والديوان ()

نقصد بكل مجلد من هذه المجلدات أن بإمكان الشؤون تبادل ملفاتها مع أي مكتب آخر ضمن المجلد المخصص له ولن يظهر لدى المكتب الآخر سوا المجلد الخاص به بينما سيظهر لدى الشؤون كامل الملفات التي تربطه مع المكاتب الأخرى

وينطبق هذا المثال على كامل المكاتب الإدارية فهي أيضاً تمتلك مجلد مشاركة مع غيرها من المكاتب

- يمتلك كل مكتب مجلد خاص به :

مثال : لدينا مجلد يدعى خاص شؤون يظهر فقط للموظفين في مكتب شؤون الطلاب و الذين يمتلكون حساب خاص بهم

هذا المجلد لن يظهر إلا لموظفي الشؤون وذلك لتبادل الملفات بين موظفي الشؤون مع بعضهم

وينطبق هذا الأمر على كامل المكاتب الإدارية الأخرى فنحن لدينا (خاص ديوان، خاص امتحانات الخ)

موظفي المكتب صاحب المجلد يمتلكون صلاحية التعديل على الملفات المشاركة

- لتقليل كمية المجلدات ولأجل الحصول على أكبر قدر من الأمان للملفات المشاركة من التخريب

لجأنا إلى الاستفادة من مبدأ الوراثة فقمنا بوضع مجلدين داخل كل مجلد لكل طرف من الأطراف المشاركة في المجلد الأصلي)

مثال : لدينا مجلد شؤون ديوان كما ذكرنا سابقا

هذا المجلد يحوي على مجلدين صادر ديوان وصادر شؤون

نقصد بتصادير شؤون : أنني كموظف في مكتب شؤون الطلاب فأنا استطيع مشاركة ملفاتي مع الديوان ضمن هذا المجلد امتلك صلاحية التعديل على هذه الملفات بينما كموظف ديوان فسوف أمتلك صلاحية القراءة فقط.

أما بالنسبة إلى صادر ديوان بنفس المبدأ

أنا كموظف في مكتب الديوان فأنا استطيع مشاركة ملفاتي مع شؤون الطلاب ضمن هذا المجلد امتلك صلاحية التعديل على هذه الملفات بينما كموظف في شؤون الطلاب فسوف أمتلك صلاحية القراءة فقط.

وبالنسبة للمجلد الأصلي (الأب) فكلا المكتبين يمتلكان صلاحية القراءة فقط له .

وتنطبق هذه الآلية على كافة المكاتب الإدارية الأخرى

- لدينا أيضاً مجلد عام لـكلية يتم نشر فيه الملفات التي هي بمثابة إعلانات لكل المتواجدين في الكلية
- لم نكتفي فقط بوضع مجلدات للمكاتب الإدارية ولجعل المشاركة لأكثر تفصيلاً ودقة

أنشأنا مجلدات أيضاً لطلب مع كافة المكاتب التيمين المسوح لهم مشاركة الملفات معهم (الشؤون والديوان والامتحانات والأساتذة والدكتاترة ومع بعضهم البعض)

دخل هذا المجلد يوجد مجلد خاص بكل سنة من السنوات وذلك لجعل المشاركة أكثر دقة ولتسهيل الأمر للطالب للوصول إلى الملفات التي يريدونها.

وكذلك الأمر بالنسبة للدكتاترة والأساتذة أنشأنا لهم مجلدات تخولهم من مشاركة ملفاتهم مع المكاتب الإدارية ومع الطلب كل على حدا وبما أننا نملك أكثر من اختصاص في جامعتنا فلم ننسى ذلك أثناء تصميمنا لنظام المشاركة فقد أنشأنا مجلدات خاصة بكل قسم يمكن للدكتاترة والأساتذة المعينين به مشاركة ملفاتهم دون تدخل من الأقسام الأخرى بالاعتماد على آلية المشاركة الفتى تم شرحها في الأمثلة السابقة.

4. السياسات

تمكن السياسات مسؤولي النظام من الحصول على مستوى عالي من التحكم في المستخدمين وأجهزة الكمبيوتر المنضمة إلى شبكاتهم

وتعنى بالدرجة الرئيسية بالتحكم في ما يمكن للمستخدمين وما لا يمكنهم فعله على نظام الكمبيوتر وذلك من أجل توفير بيئة عمل أكثر أماناً وأكثر فعالية

يمكن وضع العديد من السياسات المختلفة وتهيئتها ، مثل إعدادات سطح المكتب والطبعات والبرامج النصية لتسجيل الدخول

حظر الوصول إلى أو تقييد الوصول إلى مجلدات معينة والعديد منها ولكن أهم السياسات التي يتوجب تطبيقها على معظم الشبكات هي:

4.5.1. الإشراف على الوصول إلى لوحة التحكم

من خلال لوحة التحكم ، يمكن لأي مستخدم التحكم في جميع جوانب جهاز الكمبيوتر. لذلك ، من خلال الإشراف على من لديه حق الوصول إلى الكمبيوتر ، يمكننا من الحفاظ على أمان البيانات وخلق بيئة عمل أكثر أماناً.

يمنع هذا الإعداد ملف برنامج لوحة التحكم من بدء التشغيل. نتيجة لذلك لا يمكن للمستخدمين بدء لوحة التحكم أو تشغيل أي عناصر لوحة التحكم.

يزيل هذا الإعداد أيضاً لوحة التحكم من قائمة بدأ.

يزيل هذا الإعداد أيضاً مجلد لوحة التحكم من مستكشف Windows.

إذا حاول المستخدمون تحديد عنصر لوحة التحكم من عنصر الخصائص في قائمة السياق ، تظهر رسالة توضح أن أحد الإعدادات يمنع الإجراء

متلا في حال قام أحد المستخدمين بالدخول إلى لوحة التحكم سيكون لديه الصلاحية في إلغاء تثبيت أي برنامج موجود على الحاسوب وهذا قد يؤدي إلى

أخطاء في نظام التشغيل أو حذف أحد برامج مضاد الفيروس مما يجعل الحاسوب أكثر عرضة للخطر

طريقة تفعيل السياسة بإتباع الخطوات التالية

In the left pane

In Group Policy Management Editor -> User Configuration -

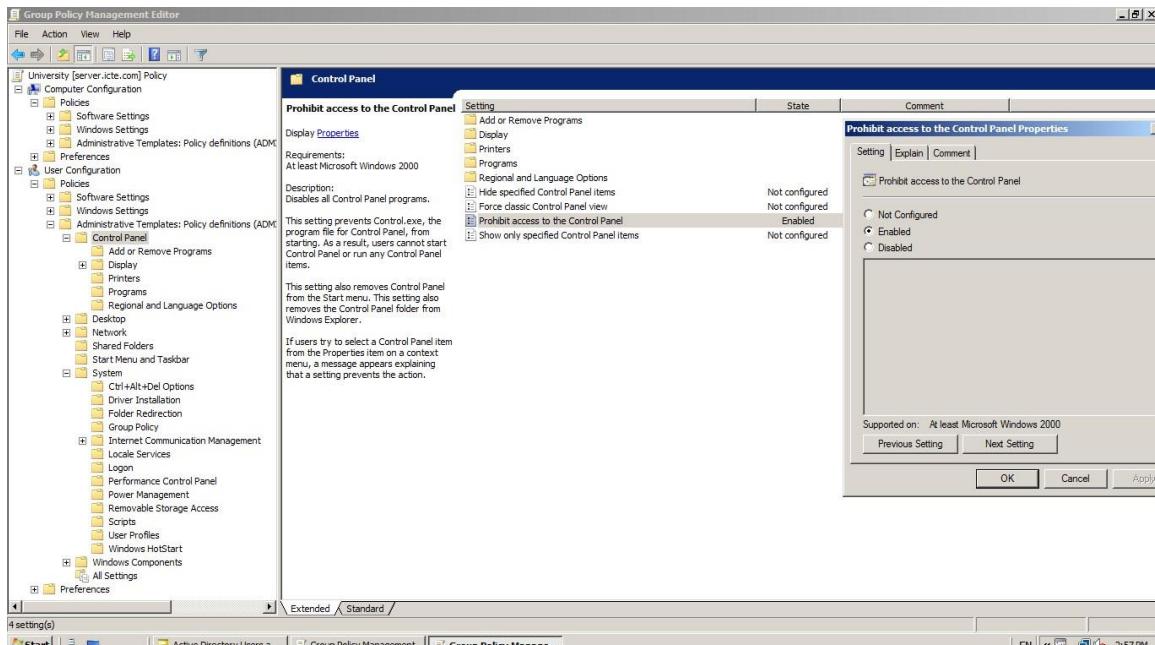
>Administrative Templates -> Control Panel In

the right pane:

Prohibit access to Control Panel and PC settings

Select Enabled

Apply and Ok



2_5_4. منع تخزين تجزئة LAN Manager

تحدد هذه السياسة ما إذا كان يتم منع LAN Manager من تخزين hash value لكلمة المرور الجديدة في المرة التالية التي يتم فيها تغيير كلمة المرور.

hash value هي تمثيل لكلمة المرور بعد تطبيق خوارزمية التشفير عليها . لفك تشفير hash value ، يجب تحديد خوارزمية التشفير ثم عكسها .

LAN Manager ضعيفة نسبياً وعرضه للهجوم .

نظراً لتخزين كلمات المرور على الجهاز المحلي في قاعدة بيانات الأمان ، يمكن اختراق كلمات المرور في حالة مهاجمة قاعدة بيانات الأمان من خلال

مهاجمة ملف إدارة حسابات الأمان (SAM) ، يمكن للمهاجمين الوصول إلى أسماء المستخدمين و كلمات المرور.

بعد حصولهم على هذه المعلومات ، يمكنهم استخدامها للوصول إلى الموارد على الشبكة عن طريق انتهاك خصوصية المستخدمين.

لن يؤدي تمكين إعداد السياسة هذا إلى منع هذه الأنواع من الهجمات ، ولكنه سيجعلها أكثر صعوبة .

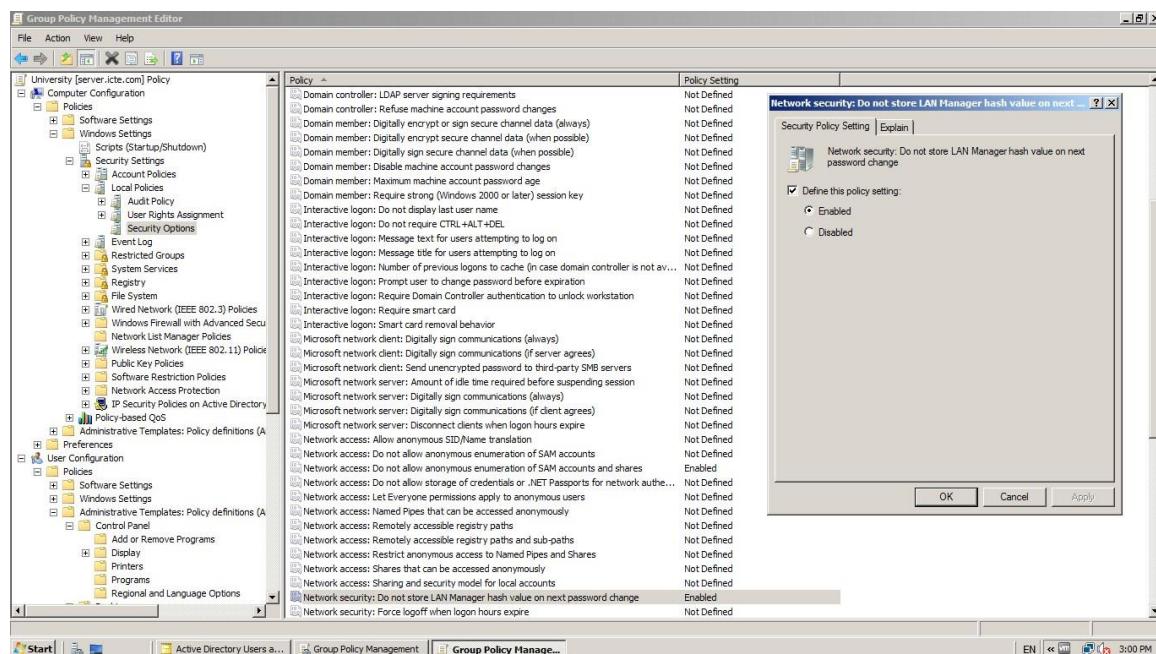
لتطبيق هذه السياسة :

: In the left pane

>-Security Settings >-Windows Settings >-Computer Configuration
.Security Options >-Local Policies

: In the right pane

Network security: Do not store LAN Manager hash value on next
.password change enable checkbox : Define
this policy setting
OK" and "Apply" Click



3_5_4 التحكم في الوصول إلى موجه الأوامر

يمكن استخدام "موجة الأوامر" لتشغيل الأوامر التي توفر وصولاً عالياً المستوى للمستخدمين وتجنب القيود الأخرى على النظام. لذلك، لضمان أمان موارد النظام، من الحكم تعطيل موجة الأوامر.

مثلاً في حال قام أحد المستخدمين بكتابة التعليمية `del *. *` في موجة الأوامر هذا سيؤدي إلى حذف جميع ملفات الكمبيوتر بما فيها ملفات النظام وبالتالي تلف النظام.

بعد قيامك بتعطيل "موجة الأوامر" ومحاوله شخص ما فتح نافذه اوامر ، سيعرض النظام رسالة تفيد بأن بعض الإعدادات تمنع هذا الإجراء لتطبيق هذه السياسة

يتم أتباع الخطوات:

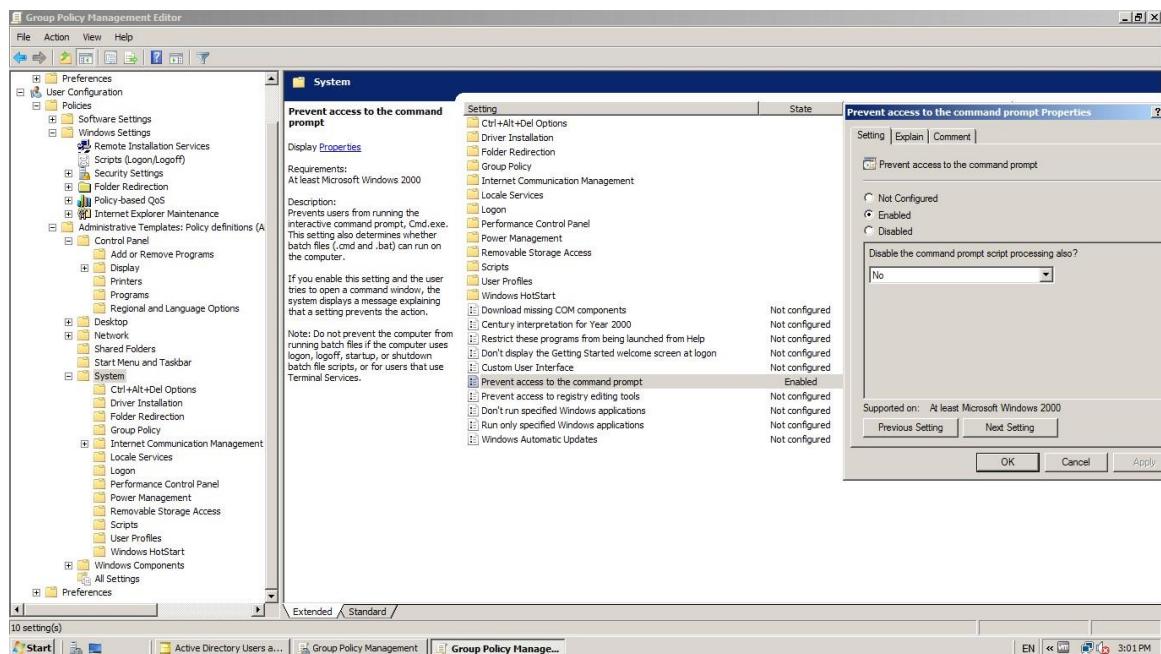
:in the left pane

Administrative >-Policies >-Windows Settings >-User Configuration .System >-Templates

:In the right pane

Prevent access to the command prompt
Enabled

."OK" and "Apply" Click



4_5_4. تعطيل إعادة تشغيل النظام القسري

عادة تشغيل النظام القسري شائعة. على سبيل المثال ، قد تواجهه موقفاً حيث كنت تعمل على جهاز الكمبيوتر الخاص بك ويقوم Windows بعرض رسالة تفيد بأن نظامك يحتاج إلى إعادة التشغيل بسبب وجود تحديث أمني.

في كثير من الحالات ، إذا فشلت في ملاحظة الرسالة أو استغرقت بعض الوقت للرد ، فسيتم إعادة تشغيل الكمبيوتر تلقائيا وتفقد العمل الهام غير المحفوظ.

إما في حال تشغيل هذه السياسة ستقوم بـ إخطار المستخدم بإعادة تشغيل جهاز الكمبيوتر ، وتنظر "التحديثات التلقائية" إعادة تشغيل جهاز الكمبيوتر من قبل أي مستخدم قام بتسجيل الدخول بدلاً من التسبب في إعادة تشغيل جهاز الكمبيوتر تلقائيا .

يجب الانتباه إلى ضرورة إعادة تشغيل الكمبيوتر حتى تصبح التحديثات نافذة المفعول .

لتعطيل إعادة التشغيل القسري من خلال GPO قم بتنفيذ الخطوات التالية :

:in the left pane

Windows >-Administrative Templates >-Computer Configuration

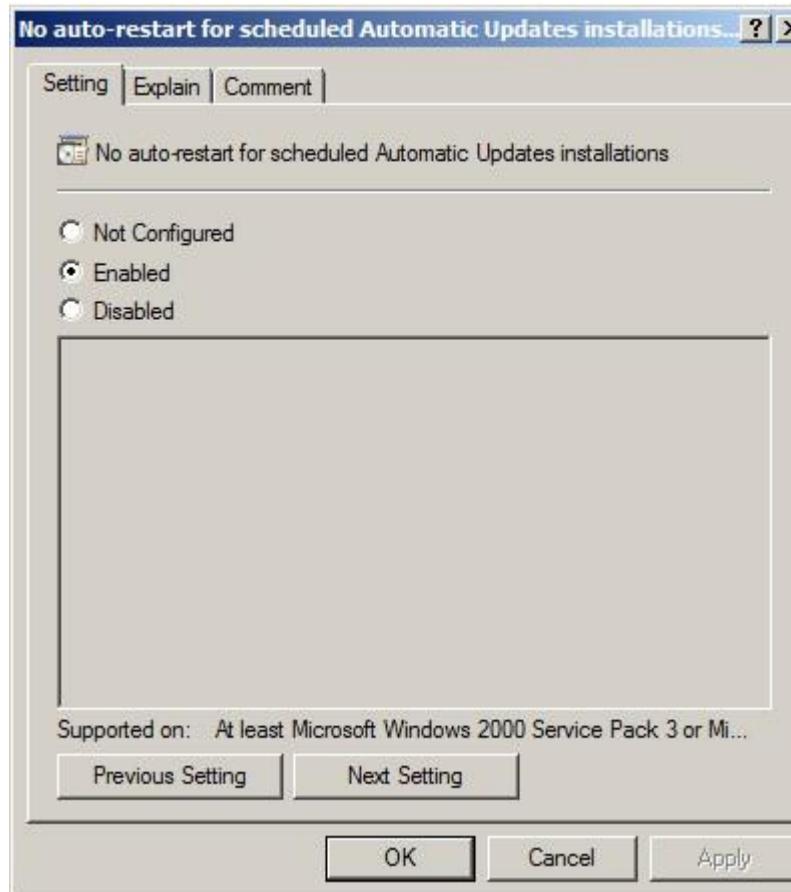
.Windows Update >-Component

:In the right pane

No auto-restart with logged on users for scheduled automatic

updates installations Click Enabled

."OK" and "Apply" Click



4_5_5. عدم السماح لمحركات الوسائط القابلة للإزالة وأقراص DVD والأقراص المدمجة ومحركات الأقراص المرنة

قد تحتوي محركات الوسائط القابلة للإزالء على فيروس أو برامج ضارة . إذا قام المستخدم بتوصيل محرك أقراص مصاب بجهاز كمبيوتر متصل بالشبكة ، فقد يؤثر ذلك على الشبكة بالكامل . وبالمثل ، تكون أقراص DVD والأقراص المدمجة ومحركات الأقراص المرنة عرضة للإصابة بالفيروسات .

لذلك من الأفضل تعطيل كل هذه الأقران بالكامل. قم بتنفيذ الخطوات التالية للقيام بذلك:

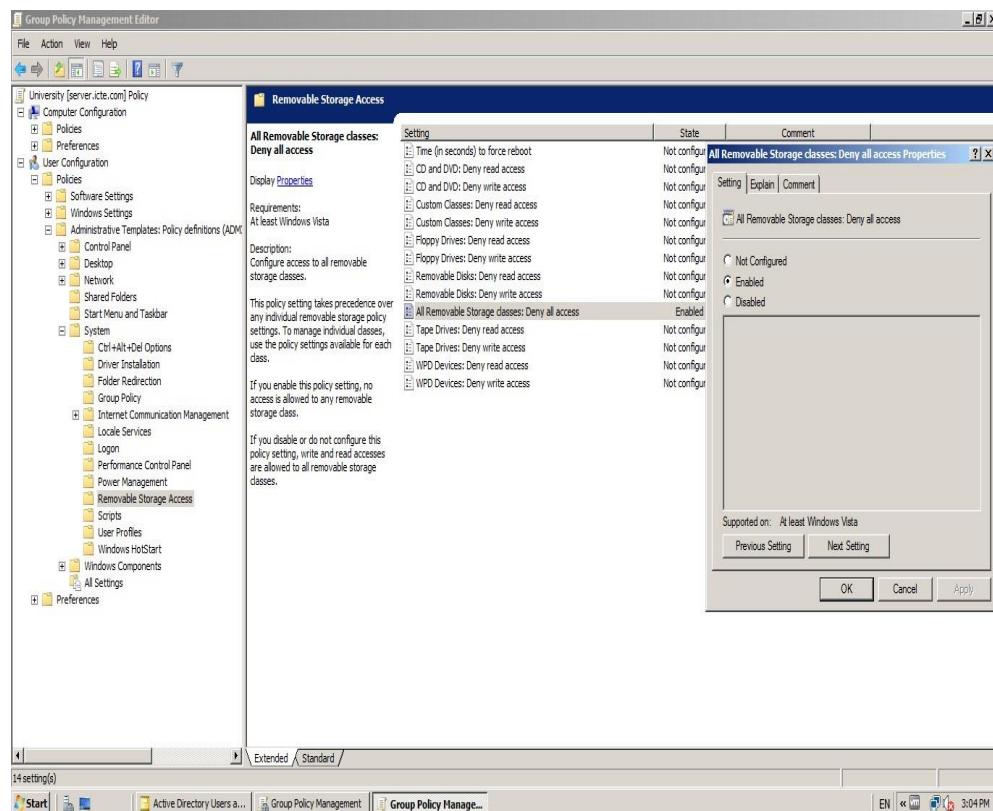
:int the left pane

:In the right pane All removable storage

classes: Deny all accesses

"Enabled" Click

."OK" and "Apply" Click



ملاحظة : هذا الإعداد للسياسة له الأسبقية على أي إعدادات سياسة تخزين فردية قائمة للازالة .

إذا قمت بتمكين إعداد النهج هذا ، فلنفلن يسمح بالوصول إلى أي فئة تخزين قابلة للإزالة .

٤_٥_٦. تقييد تثبيت البرامج

عندما تمنحك المستخدمين حرية تثبيت البرامج ، فقد يقومون بتثبيت العاب أو تطبيقات غير مرغوب فيها تعرضاً لخطره . عادة ما يتبعين على مسؤولي النظام إجراء صيانة وتنظيف هذه الأنظمة بشكل روتيني .

من المستحسن منع تثبيت البرامج من خلال :

:in the left pane

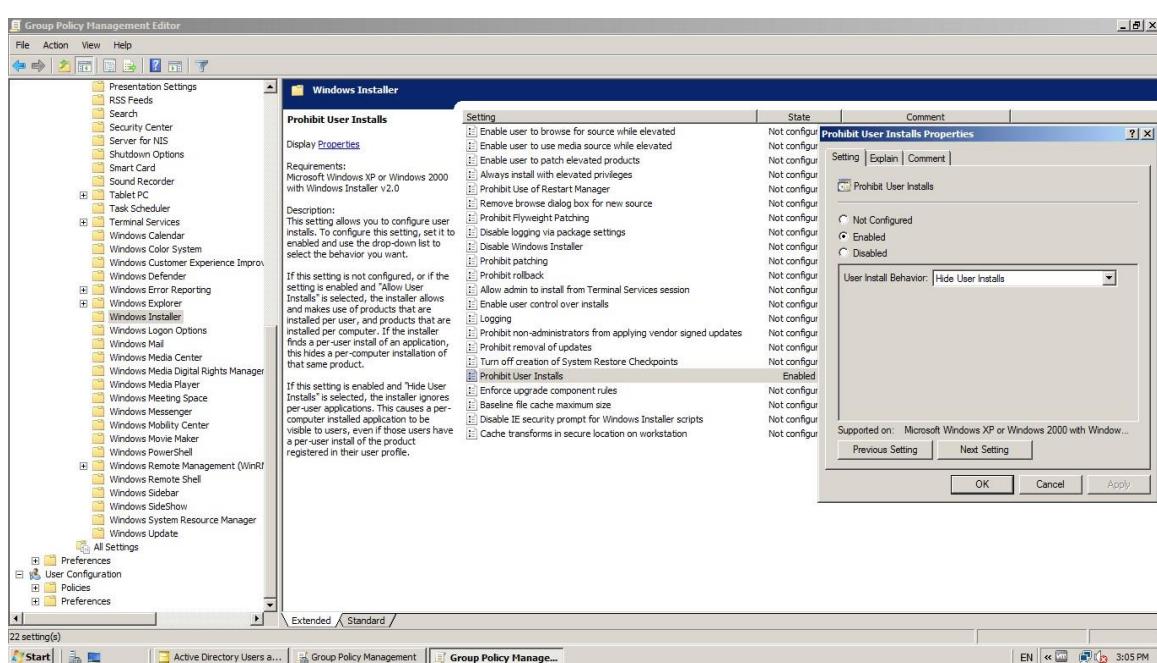
Windows >-Administrative Templates >-Computer Configuration
.Windows Installer >-Component

:In the right pane

Prohibit User Install

"Enabled" Click

."OK" and "Apply" Click



7_ تعطيل حساب الضيف

من خلال حساب الضيف ، يمكن للمستخدمين الوصول إلى البيانات الحساسة . تمنحك هذه الحسابات الوصول إلى جهاز كمبيوتر يعمل بنظام Windows ولا تتطلب كلمة مرور . يعني تمكين هذا الحساب أن أي شخص يمكنه إساءة استخدام نظام التشغيل وإساءة استخدامها .

لحسن الحظ ، يتم تعطيل هذه الحسابات بشكل افتراضي . من الأفضل التتحقق من أن هذا هو الحال في بيئة تكنولوجيا المعلومات لديك ، حيث إن تمكين هذا **الحساب في نطاقك فإن تعطيله سيمنع الأشخاص من إساءة استخدام الوصول** :

in the left pane:

>-Security Settings >-Windows Settings >-Computer Configuration
Security Options >-Local Policies

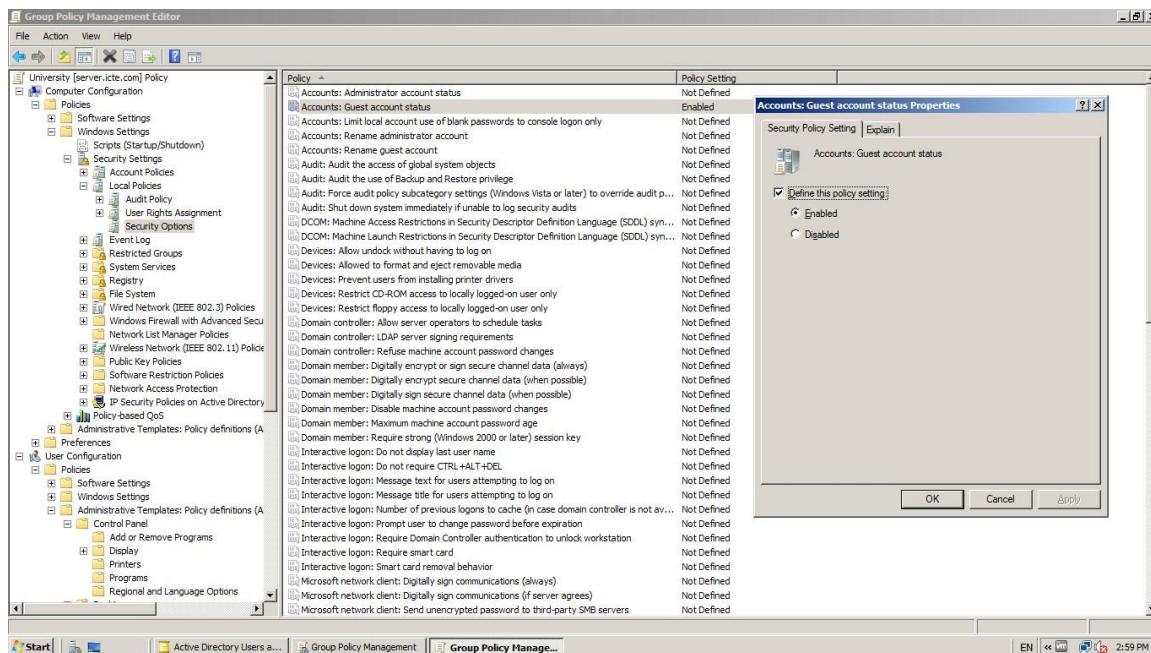
:In the right pane

Accounts: Guest Account Status

"Define this policy setting" Select

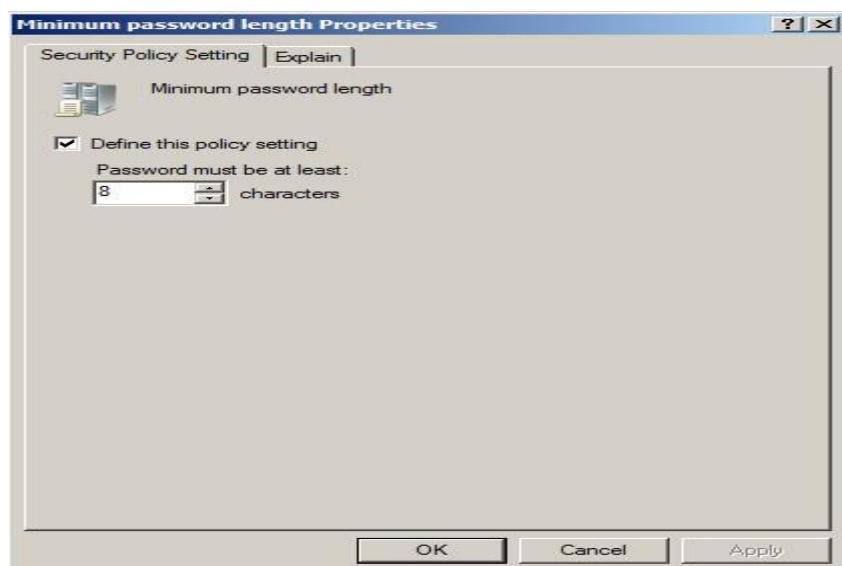
"Disabled"

."OK" and "Apply" Click



8_ تعيين الحد الأدنى لطول المرور إلى الحدود العليا

يحدد إعداد الأمان هذا أقل عدد من الأحرف التي قد تحتوي عليها كلمة مرور لحساب المستخدم . على سبيل **المثال** ، بالنسبة للحسابات المرتفعة ، يجب تعين كلمات المرور على 12 حرفا على الأقل ، وللحسابات العادية 8 حرفا على الأقل . يؤدي تحديد قيمة أقل لطول كلمة المرور الأدنى إلى إنشاء مخاطرة غير ضرورية . الإعداد الافتراضي هو الأحرف "0" -> Windows Settings >-Computer Configuration Password Policy >-Account Policies :In the right pane "Define this policy setting" Specify a value for the password length ."OK" and "Apply" Click



4_5_9. تعين الحد الأقصى لعمر كلمة المرور إلى الحدود الدنيا

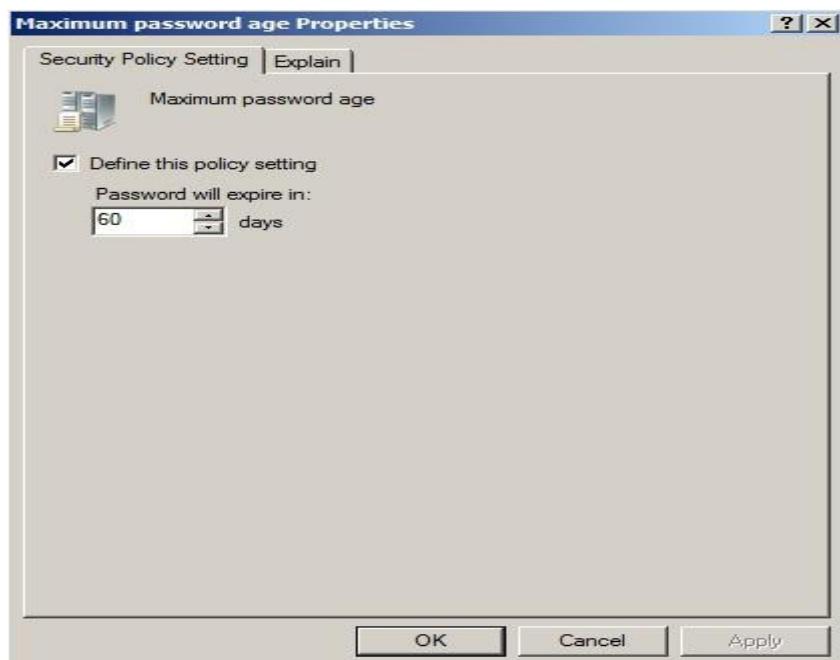
يحدد إعداد الأمان هذا الفترة الزمنية (بأيام) التي يمكن استخدام كلمة المرور قبل أن يطلب النظام من المستخدم تغييرها . يمكنك تعين كلمات المرور بحيث تنتهي صلاحيتها بعد عدد من الأيام بين 1 و 999 ، أو يمكنك تحديد كلمات المرور هذه لا تنتهي صلاحيتها أبداً بتعيين عدد الأيام على 0.

إذا قمت بتعيين عمر انتهاء صلاحية كلمة المرور على فترة زمنية طويلة ، فلن يضطر المستخدمون إلى تغييره كثيرا ، مما يعني أنه من المحتمل أن يتم سرقة كلمة المرور . يفضل دائماً فترات انتهاء صلاحية كلمة المرور الأقصر .

يتم تعين الحد الأقصى الافتراضي لعمر كلمة المرور لـ Windows إلى 42 يوما . تعرض لقطة الشاشة التالية إعداد السياسة المستخدم لتكوين "الحد الأقصى لعمر كلمة المرور . " قم بتنفيذ الخطوات التالية :

:in the left pane

>-Security Settings>-Windows Settings >-Computer Configuration
 Password Policy >-Account Policies
 :In the right pane
 "Define this policy setting" Select
 ."OK" and "Apply" Click



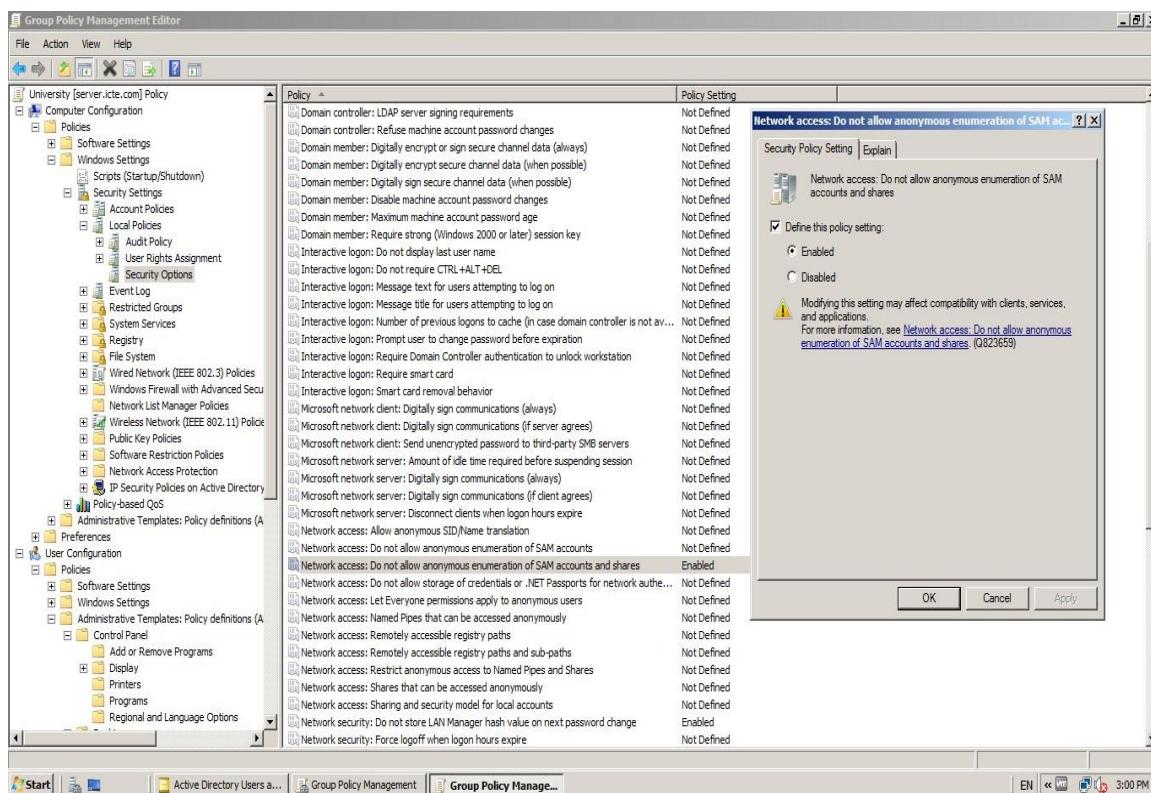
4_5_10. تعطيل تعداد SID مجهول

يقوم Active Directory بتعيين رقم فريد لكل كائنات الأمان في Active Directory ، بما في ذلك المستخدمين والمجموعات وغيرها ، وتسمى أرقام معرفات الأمان (SID). في إصدارات Windows الأقدم ، يمكن للمستخدمين الاستعلام عن معرفات الأمان لتحديد المستخدمين والمجموعات المهمة. يمكن استغلال هذا البند من قبل المتسللين للحصول على وصول غير مصرح به إلى البيانات. افتراضياً ، يتم تعطيل هذا الإعداد ، وتأكد من بقائه على هذا النحو. قم بتنفيذ الخطوات التالية:

:in the left pane
 Security >-Windows Settings >-Policies >-Computer Configuration
 Security Options >-Local Policies >-Settings

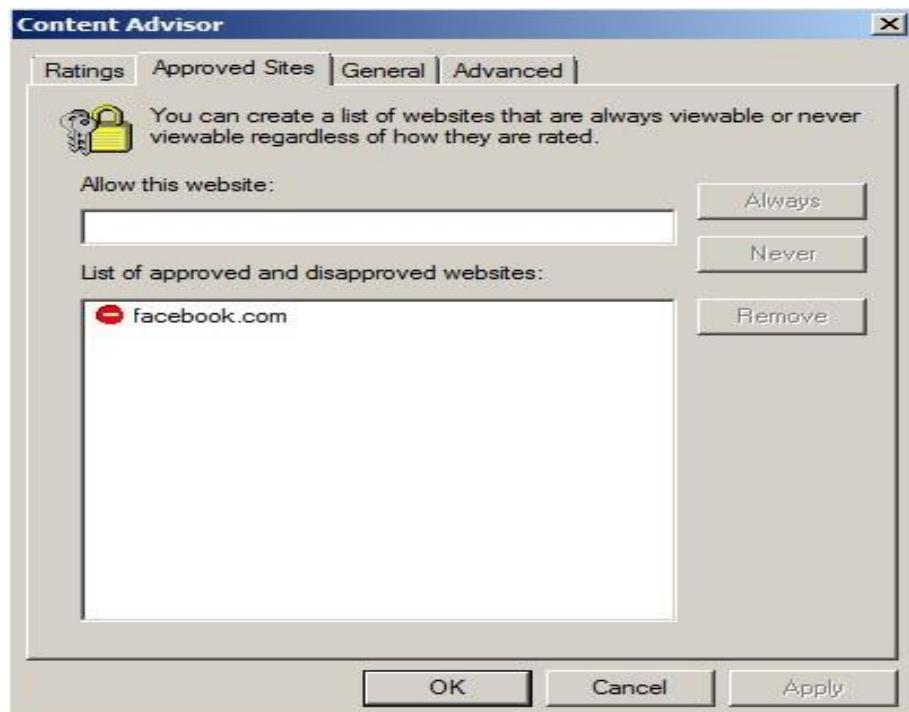
:In the right pane
 Network Access: Do not allow anonymous enumeration of SAM accounts and shares
 'Enabled' Choose

.Apply and OK



4_5 منع استخدام موقع الويب

يمنح هذا الإجراء القدرة لاختيار موقع الويب المسموح بالدخول إليها بالإضافة إلى الفرصة لحظر بعض المواقع الأخرى
ففي الصورة أدناه قمنا بحظر استخدام موقع face book

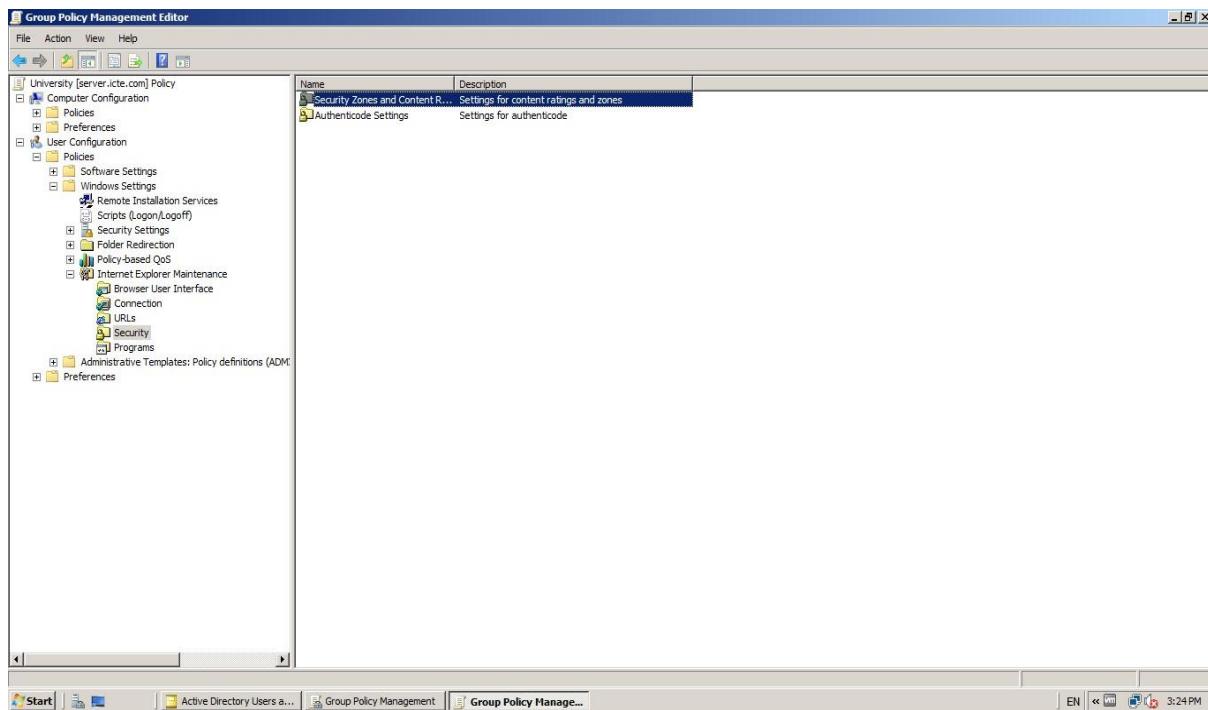


يمكنا كذلك منح سماحية وصول لموقع محدد مثل Google بالإضافة لذلك نستطيع اختيار إجراء لجميع المواقع الأخرى الغير محددة إما سماح الدخول إليها أو حظرها

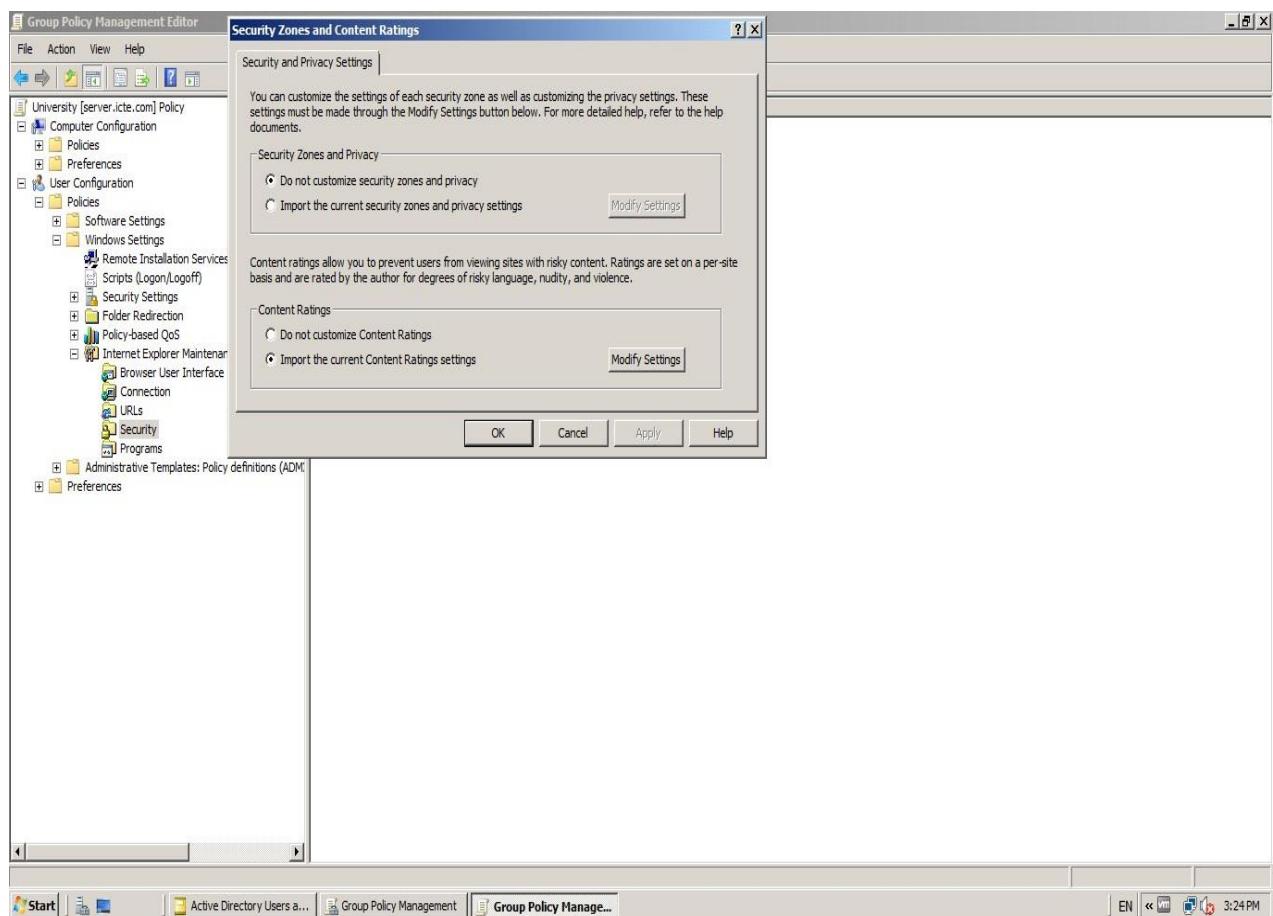
في حال حاول أحد المستخدمين تسجيل الدخول لأحد هذه المواقع ستظهر رسالة تؤكد حظر وصول لهذا الموقع المحدد

group policy management - user configuration - windows setting - internet explorer management - security zones and content

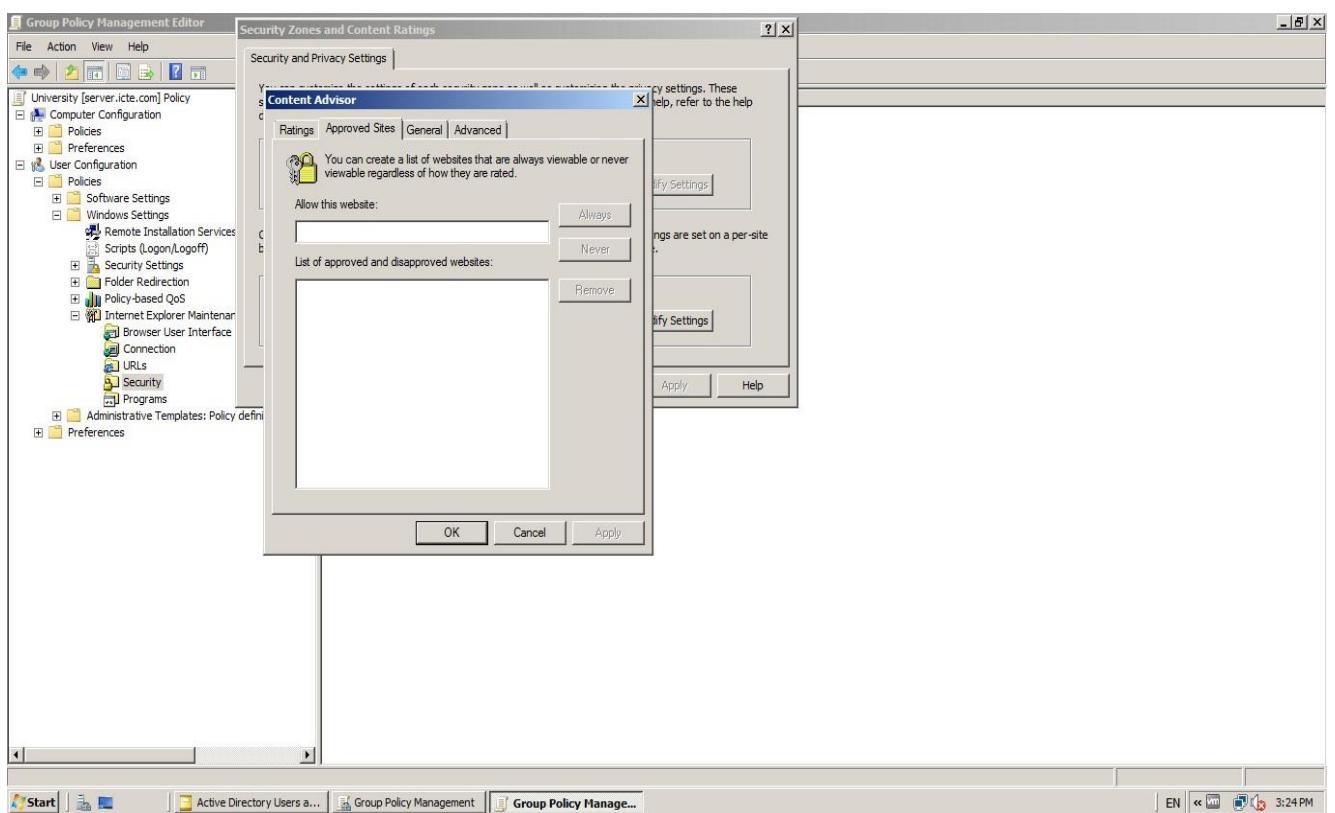
الجانب اليمين في



نضغط عليها في القسم السفلي من الواجهة المنبثقة نختار
import the current content setting – modify setting

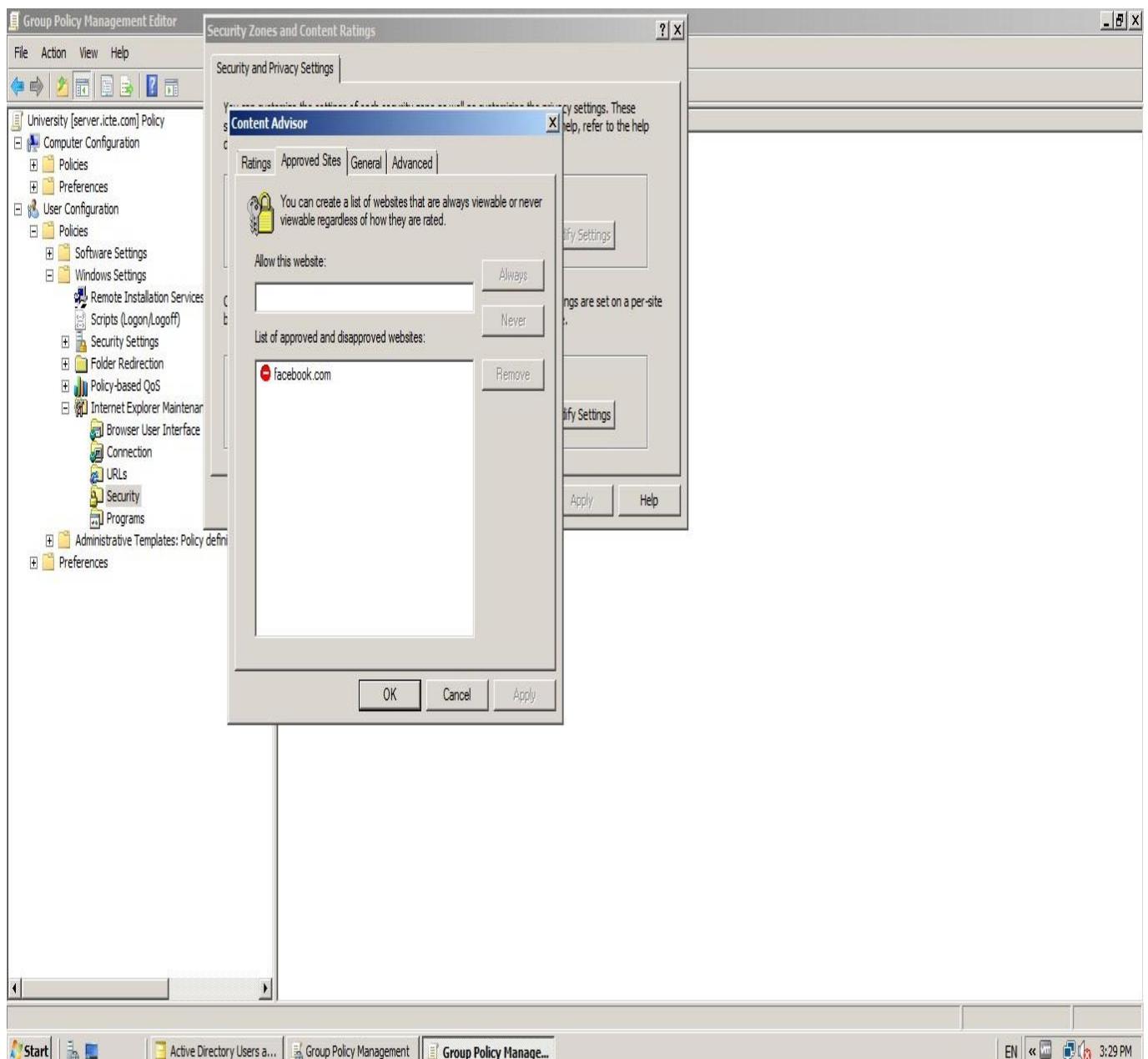


نختار approved sites



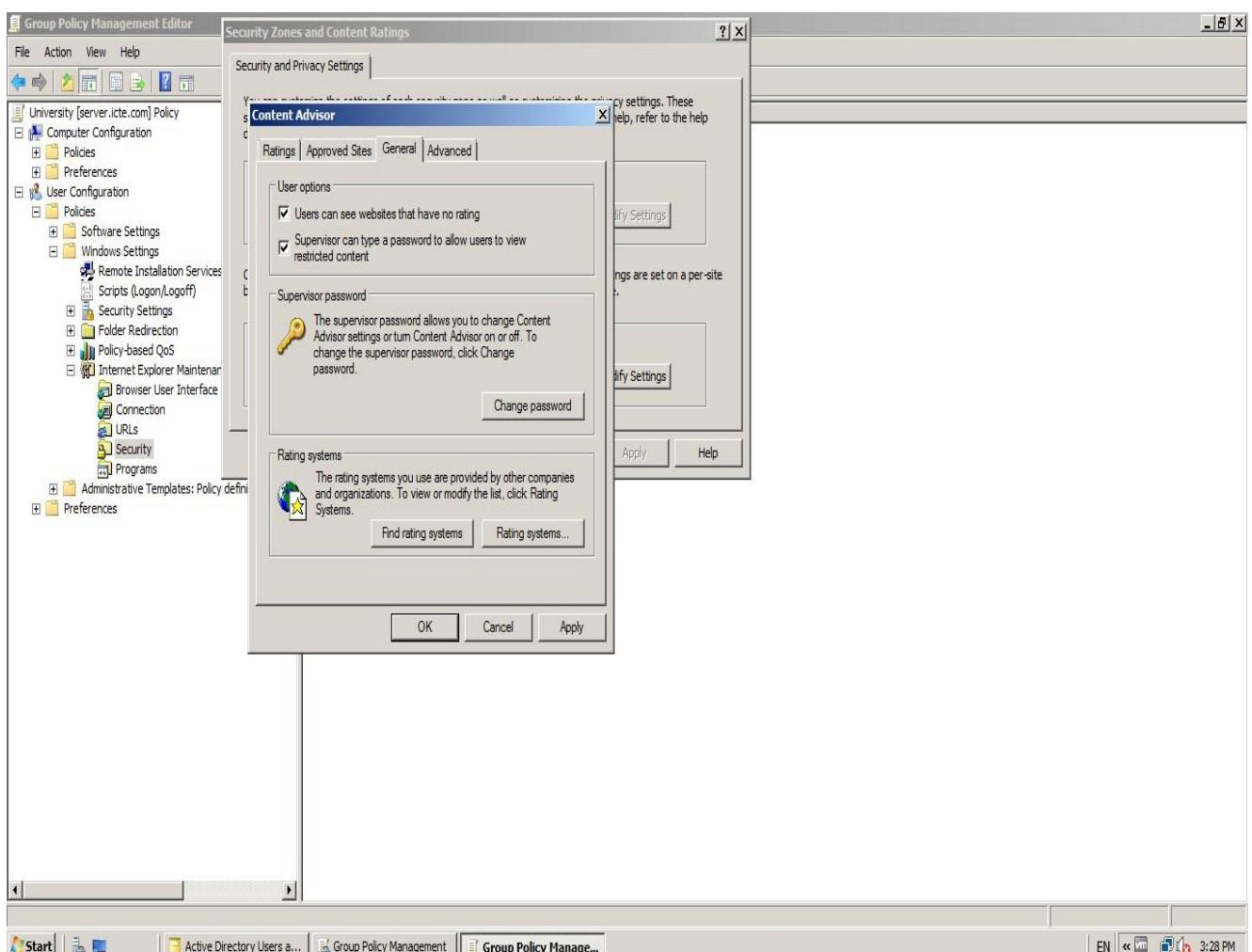
نكتب رابط الموقع ونختار never

ثم ok يطلب password لمرة واحدة فقط ندخل password نجد ها أمنة ثم نقوم بتأكيد الـ ok ثم password



في حال أحبنا حظر فقط موقع واحد والسماح للمستخدمين بتسجيل الدخول لجميع المواقع الأخرى نذهب إلى general نفعل الخيار websites that has no rating

وإلا في الحالة الافتراضية لن يستطيع المستخدم تسجيل الدخول لـ 'Always' المواقع التي نقوم باختبار لها



ملاحظة : هذه السياسة تطبق على برنامج Internet Explorer فقط

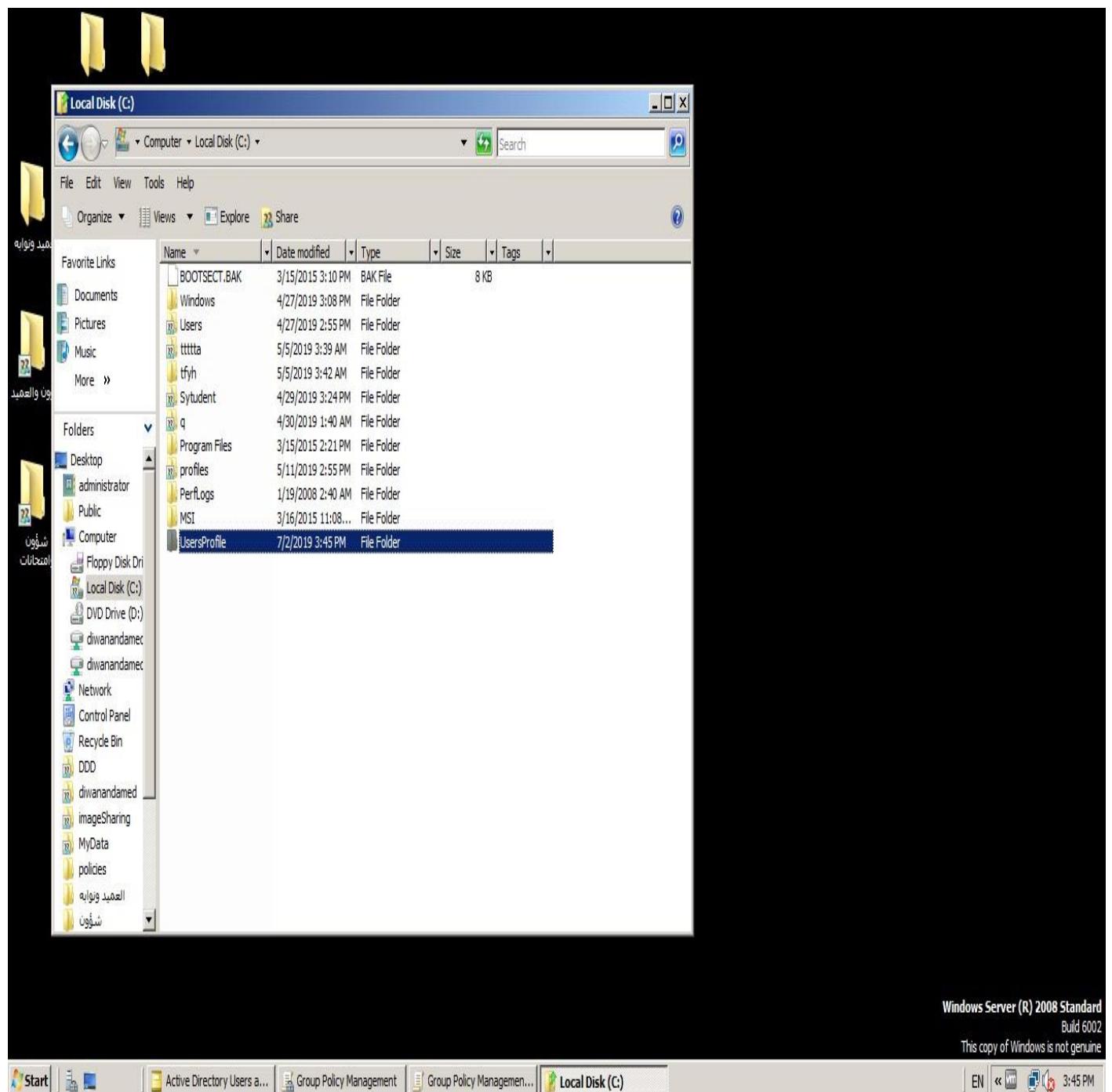
Local Roaming Profile . 12_5_4

في أي مركز عمل نلاحظ وجود عدد محدود من الحواسيب ولا يمكن تخصيص حاسوب محدد لكل موظف لذلك هنا يأتي دور هذه السياسة التي تعمل على نسخ جميع ملفات المستخدم الضرورية إلى جانب السيرفر والاحتفاظ بها ضمن مجلد محدد بحيث في حال قام المستخدم بتسجيل الدخول إلى أي حاسوب متصل بالشبكة يستطيع قراءة ملفاته الشخصية أو في حال حدوث إيه خلل في أحد الحواسيب فيستطيع تسجيل الدخول عبر حاسوب آخر ومتابعة العمل.

من أجل ذلك نلاحظ وجود قرص جديد باسم كل مستخدم في جهاز الحاسوب يحتفظ بها بملفاته الضرورية **لتطبيق هذه السياسة :**

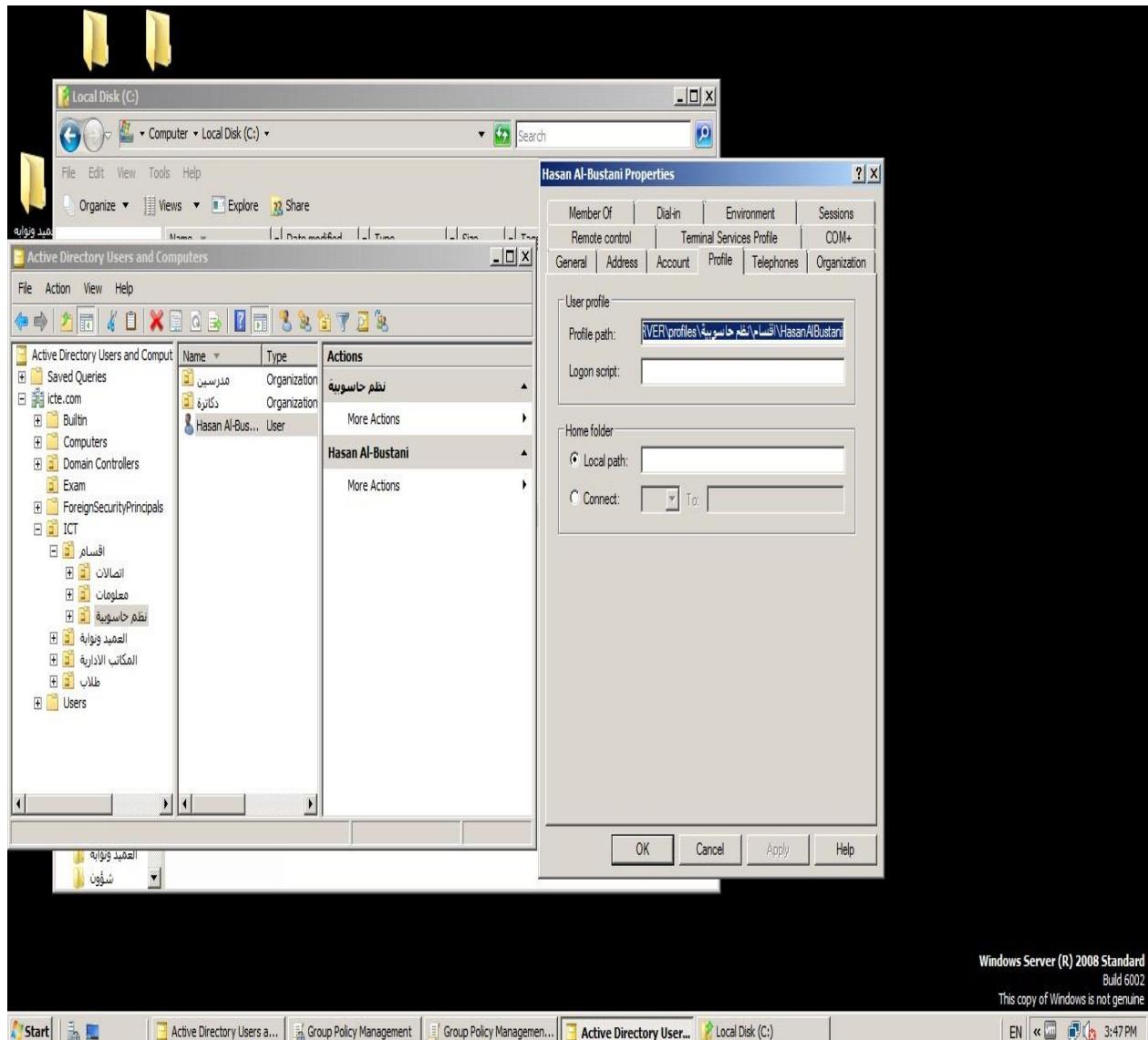
نشئ مجلد جديد في القرص C مثلا user Profile نقوم بوضع مشاركة متقدمة للمجلد

في إعدادات المشاركة نختار جميع الصلاحيات لeveryone نقوم بوضع مجلد جديد باسم user مثلا مجلد باسم YAZAN



نذ هب إلى ال directory users and computers active ننسخ رابط ملف المشاركة للمجلد الأساس user Profile

إلى المستخدم الذي نريد إجراء نسخ للملفات الخاصة به على جانب السيرفر
properties- profile



يوجد مجال فارغ يدعى profile path

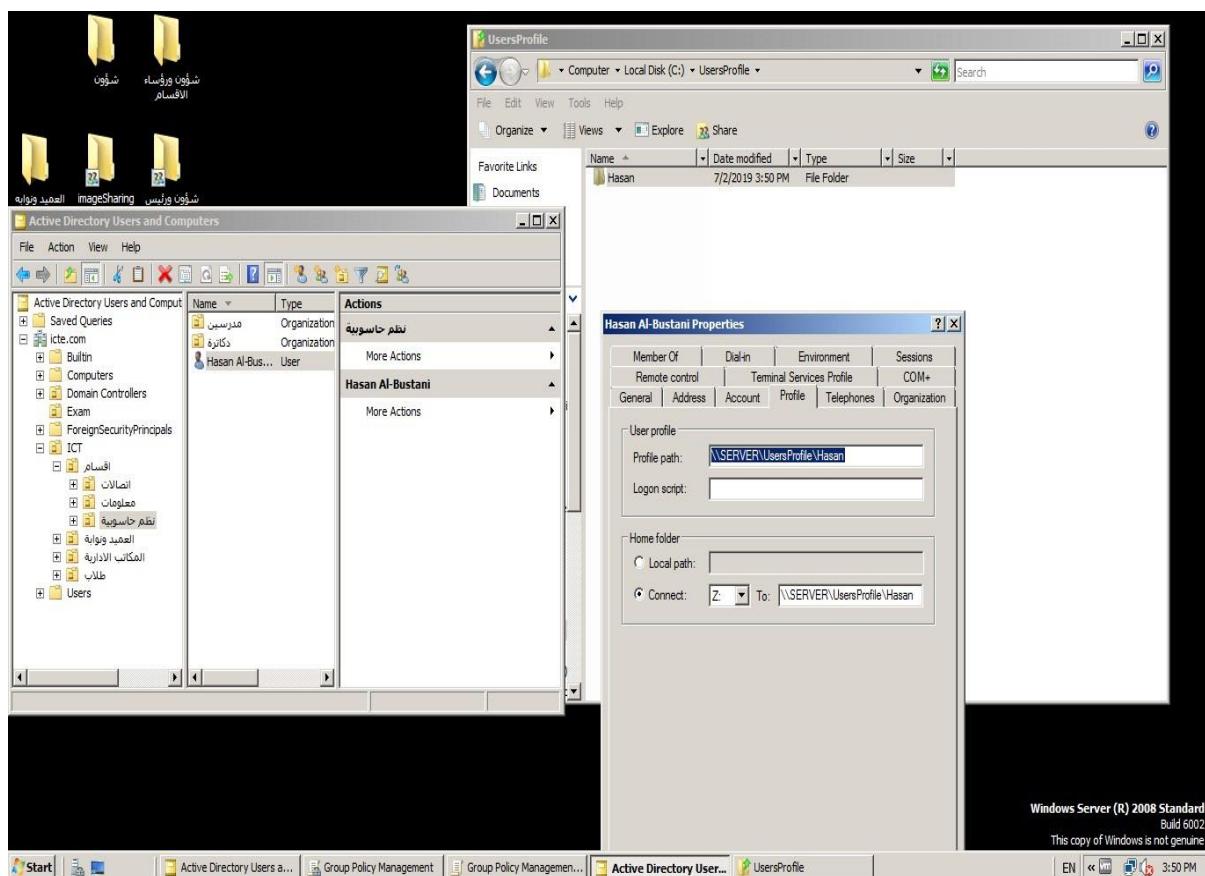
تلصق به رابط المشاركة للمجلد user Profile ليكون بالشكل
 SERVER/user Profile// نضيف إليه اسم المجلد الذي انشأناه لهذا
 user فيصبح بالشكل

SERVER/user Profile/YAZAN// Home

في النافذة نفسها يوجد خيار connect
نختار connect

في الفراغ to ننسخ رابط المشاركة ذاته ونلصقه هنا

أي الرابط // SERVER/user Profile/YAZAN /



باتالي يظهر لدينا قرص جديد في جهاز الكمبيوتر لدى المستخدم يضع بداخلة الملفات التي يرغب بالاحتفاظ بها



4_5_13. منع استخدام الأجهزة القابلة للإزالءة

إذا قمت بتمكين هذا الإعداد ، فقد لا يتم تثبيت الأجهزة القابلة للإزالءة ، ولا يمكن للأجهزة القابلة للإزالءة الموجودة تحديث برامج التشغيل الخاصة بها .

من المؤكد أنه ليس من المستغرب انتشار الأجهزة المحمولة مثل محركات أقراص USB المحمولة والأقراص الصلبة USB و الهواتف المحمولة وحتى الكاميرات التي يجب توخي الحذر الشديد الآن لمنع سرقة البيانات.

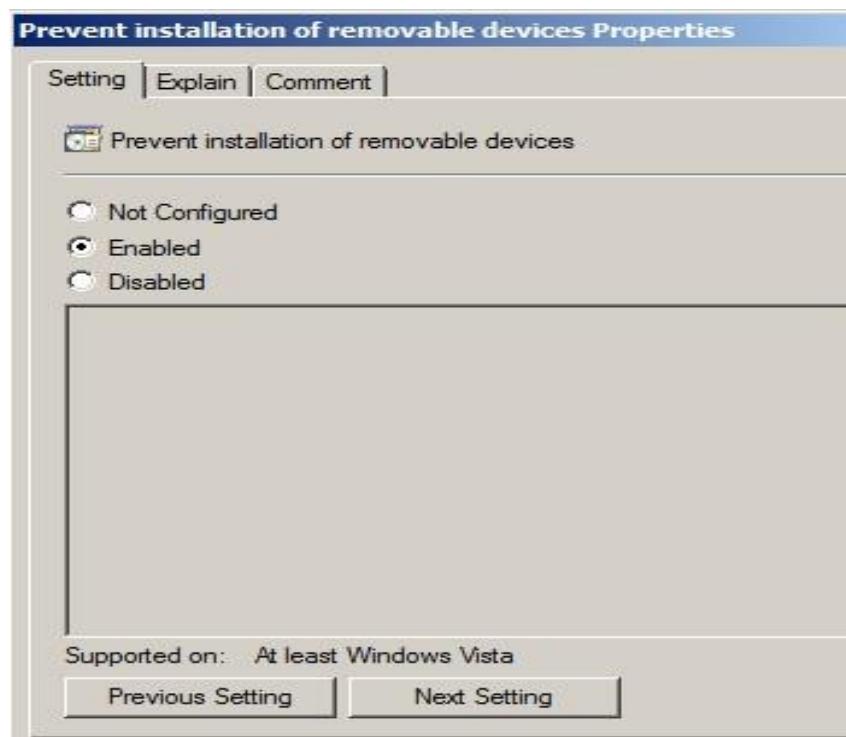
لتطبيق هذه السياسة :

: In the left pane

>-Administrative Templates >-Policies >-Computer Configuration
.Device Installation Restrictions >-Device Installation >-System

In the right pane

Prevent Installation of Removable Devices



في حال تم وصل أي عنصر بجهاز الحاسب ستظهر الرسالة التالية



4_5_4. منع الوصول إلى قرص النظام C

هذه السياسة تستخدمن لمنع وصول المستخدمين المحليين إلى قرص النظام والقيام بأية محاولة تعديل عليه لذلك تطبيق هذه السياسة سيؤدي إلى تجنب مواجهه الكثير من المشكلات ومن أمثلتها حذف أحد ملفات النظام التي بدورها تؤدي إلى تعطيل النظام بشكل كامل

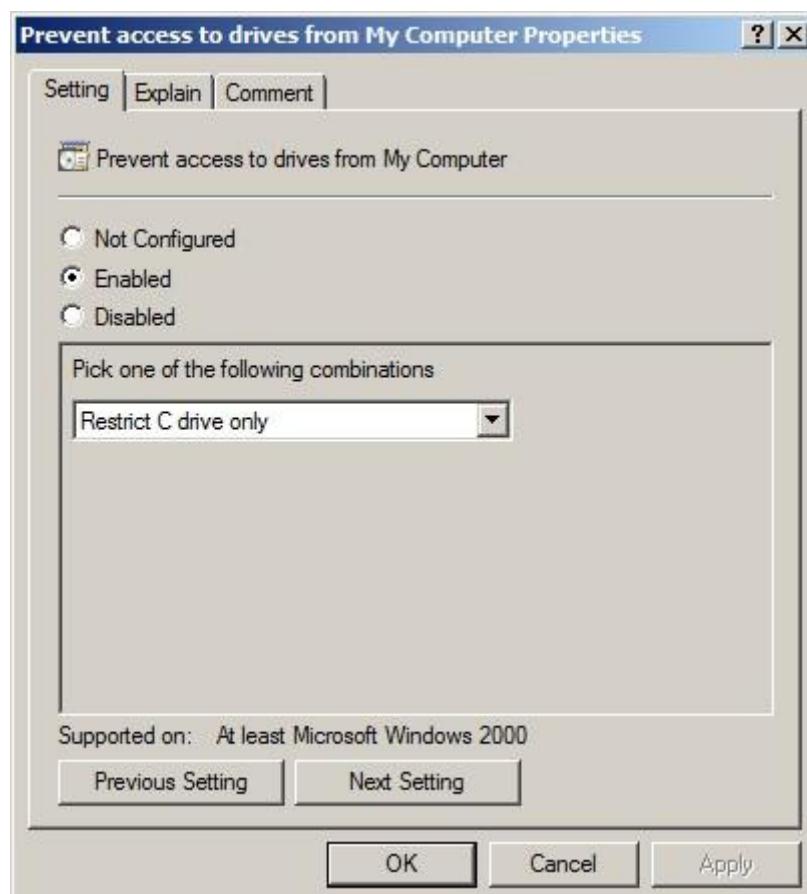
لتطبيق السياسة نتبع الخطوات

In the left pane:

User Configuration->polices-> Administrative Template -> Windows Component ->Windows Explorer

In the right pane :

Prevent access to drives from my computer



وعند القيام بمحاولة الدخول إلى القرص C ستظهر الرسالة التالية



4_15_5 منع تغيير صورة سطح المكتب

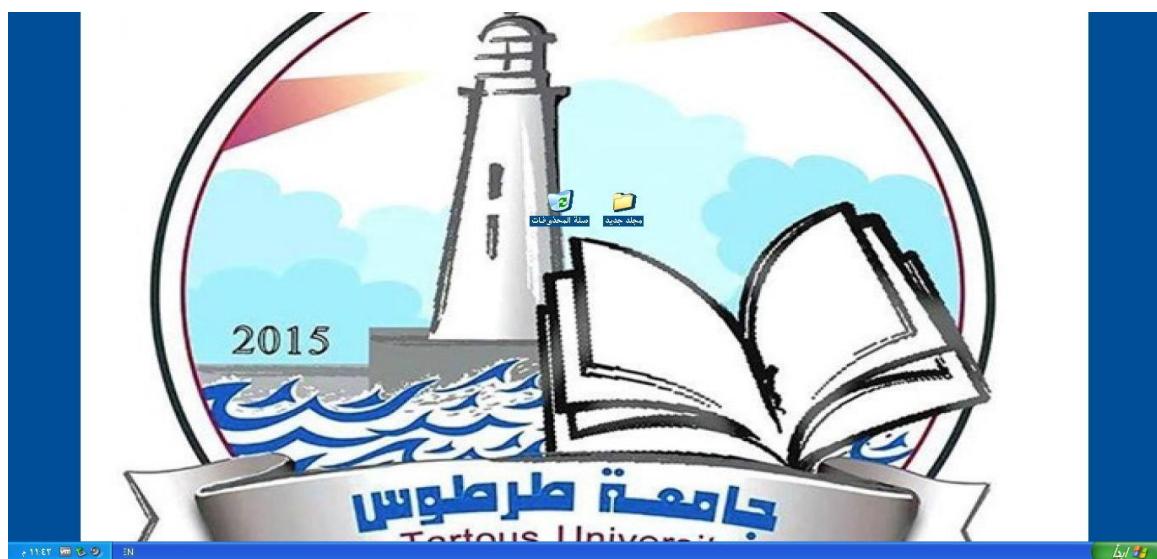
تستخدم هذه السياسة من أجل الحفاظ على وجود شعار الشركة او المؤسسة او الجامعة كخلفية سطح المكتب على الحواسيب الموجودة ضمن الشركة الواحدة لتحديد الصورة المختارة كخلفية يجب أن تكون مشاركة لكل المستخدمين في

الشبكة لذلك ننشئ مجلد جديد نضع بداخله الصورة ونقوم بمشاركته بمستوى قراءة لجميع المستخدمين

ثم نأخذ مسار المشاركة للمجلد بالإضافة إلى اسم الصورة ولاحقتها ونضعه في Wallpaper Name كما في الصورة



عند تطبيق السياسة :



4_5_16. الإشراف على الوصول إلى لوحة التحكم

من خلال لوحة التحكم ، يمكن لأي مستخدم التحكم في جميع جوانب جهاز الكمبيوتر. لذلك ، من خلال الإشراف على من لديه حق الوصول إلى الكمبيوتر

، يمكننا من الحفاظ على أمان البيانات وخلق بيئة عمل أكثر أمانا .
 يمنع هذا الإعداد ملف برنامج لوحة التحكم من بدء التشغيل . نتيجة لذلك
 لا يمكن للمستخدمين بدء لوحة التحكم أو تشغيل أي عناصر لوحة التحكم .
 يزيل هذا الإعداد أيضا لوحة التحكم من قائمة ابدأ .
 يزيل هذا الإعداد أيضا مجلد لوحة التحكم من مستكشف Windows .
 إذا حاول المستخدمون تحديد عنصر لوحة التحكم من عنصر الخصائص في قائمة
 السياق ، تظهر رسالة توضح أن أحد الإعدادات يمنع الإجراء

مثلا في حال قام أحد المستخدمين بالدخول إلى لوحة التحكم سيكون لديه
 الصلاحية في إلغاء تثبيت أي برنامج موجود على الكمبيوتر وهذا قد يؤدي إلى
 أخطاء في نظام التشغيل أو حذف أحد برامج مصاد الفيروس مما يجعل الكمبيوتر
 أكثر عرضة للخطر

طريقة تفعيل السياسة بإتباع الخطوات التالية

In the left pane

In Group Policy Management Editor -> User Configuration -> Administrative Templates -> Control Panel

In the right pane:

Prohibit access to Control Panel and PC settings

Select Enabled

Apply and Ok -



4_5_17. التحكم في الوصول إلى موجه الأوامر

يمكن استخدام "موجه الأوامر" لتشغيل الأوامر التي توفر وصولاً عالياً المستوى للمستخدمين وتجنب القيود الأخرى على النظام. لذلك، لضمان أمان موارد النظام، من الحكم تعطيل موجه الأوامر.

مثلاً في حال قام أحد المستخدمين بكتابة التعليمية (`*.*.del`) في موجه الأوامر هذا سيؤدي إلى حذف جميع ملفات الكمبيوتر بما فيها ملفات النظام وبالتالي تلف النظام.

بعد قيامك بتعطيل "موجه الأوامر" ومحاولة شخص ما فتح نافذة أوامر، سيعرض النظام رسالة تفيد بأن بعض الإعدادات تمنع هذا الإجراء **لتطبيق هذه السياسة**.
يتم إتباع الخطوات:

in the left pane:

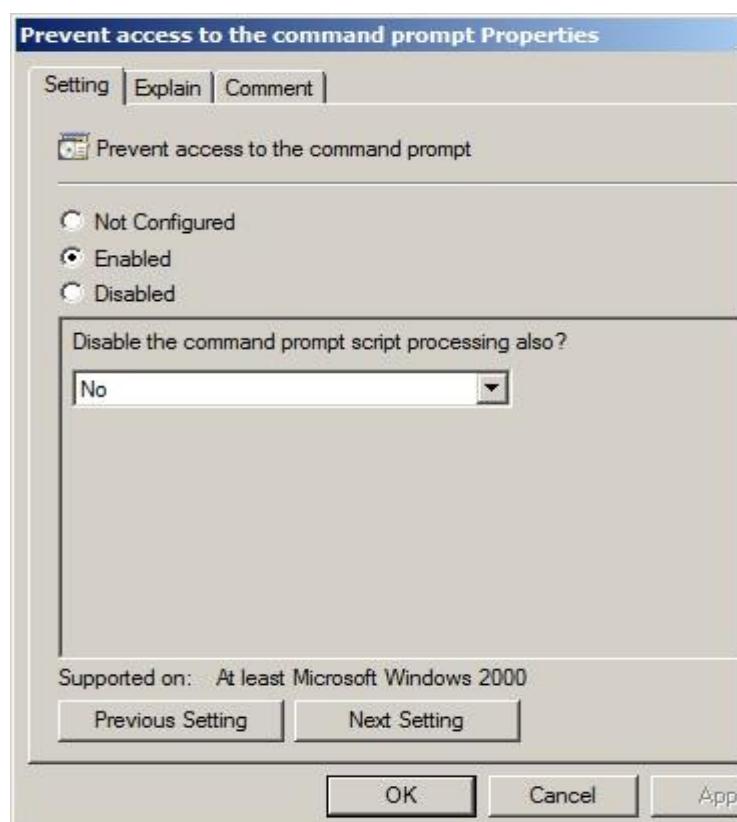
User Configuration-> Windows Settings-> Policies-> Administrative Templates-> System

In the right pane:

Prevent access to the command prompt

Enabled

."and"OK "Apply"Click

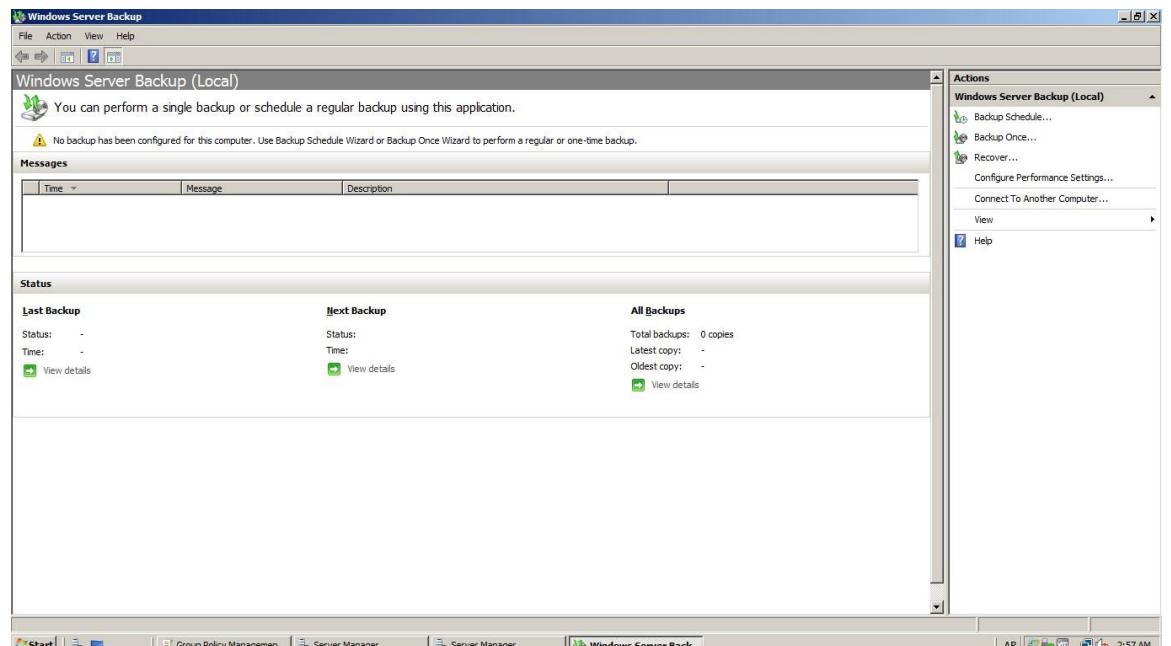


18_5_4**Windows Server Backup (WSB)**

هي ميزة توفر خيارات النسخ الاحتياطي والاسترداد لملفات المستخدمين. يمكن للمسؤولين استخدام إجراء نسخ احتياطي لجميع الملفات بشكل كامل أو حالة النظام أو وحدات تخزين محددة أو ملفات أو مجلدات محددة ، طالما أن حجم البيانات أقل من 2 تيرابايت.

توفر هذه الخدمة القدرة على استعادة ملفات المستخدمين إلى أجهزة مختلفة ندخل إليها من خلال :

Start -> Administrative tool -> Windows server backup



طبعاً تمكنا الخدمة من تحديد وقت معين للقيام بعملية النسخ الاحتياطي بحيث أنها لا تتعارض مع أوقات عمل الموظفين حيث إننا فمنا باختيار وقت عملية النسخ الساعة التاسعة مساء وبشكل يومي



٤_٥_١٩. تحويل مجلد المشاركة إلى قرص على جهاز الكمبيوتر

هذه الخدمة تتيح لنا إظهار مجلدات المشاركة لكل مستخدم مع الأطراف التي يشارك معها المعلومات على شكل أقراص في جهاز الحاسوب وذلك من خلال:

نقوم بتحديد المجلد المراد مشاركته ولتكن sharing



نقوم بمشاركة المجلد على مستوى المستخدمين
ثم نذهب إلى

Group Policies Management

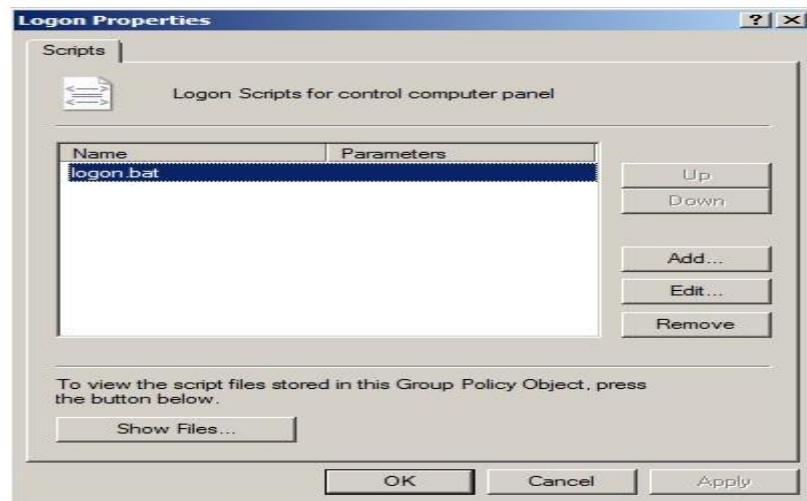
ونطبق السياسة على الوحدة التنظيمية التي ستشارك هذه المجلد وذلك من خلال

User Configuration-> Windows setting -> Scripts -> logon

نختار خصائص ثم نقوم بإضافة الملف

والذي يحتوي على التعليمية

Net use o: \\\WIN-M20W08FS89X\sharing



طبعاً التعلمية

WIN-M20W08FS89X\sharing

تمثل رابط المشاركة للمجلد

cmd ثم نقوم بتشغيل sharing

وكتابة التعلمية

```
C:\Users\Administrator>net use o: \\\WIN-M20W08FS89X\sharing
The command completed successfully.
```

وبذلك عند تسجيل الدخول من احد الموظفين سيظهر له القرص
ضمن جهاز الكمبيوتر

٤_٥_٢. تثبيت برامج على أجهزة المستخدمين من طرف السيرفر

تتيح هذه السياسة توزيع البرامج تلقائياً على أجهزة الكمبيوتر
المستخدمين.

ولدينا طريقتين للقيام بذلك:

a. تخصيص البرامج

يمكنك تعيين توزيع برنامج للمستخدمين أو أجهزة الكمبيوتر
إذا قمنا بتعيين البرنامج لمستخدم ، يتم تثبيته عندما يقوم المستخدم
بتسجيل الدخول إلى الكمبيوتر .

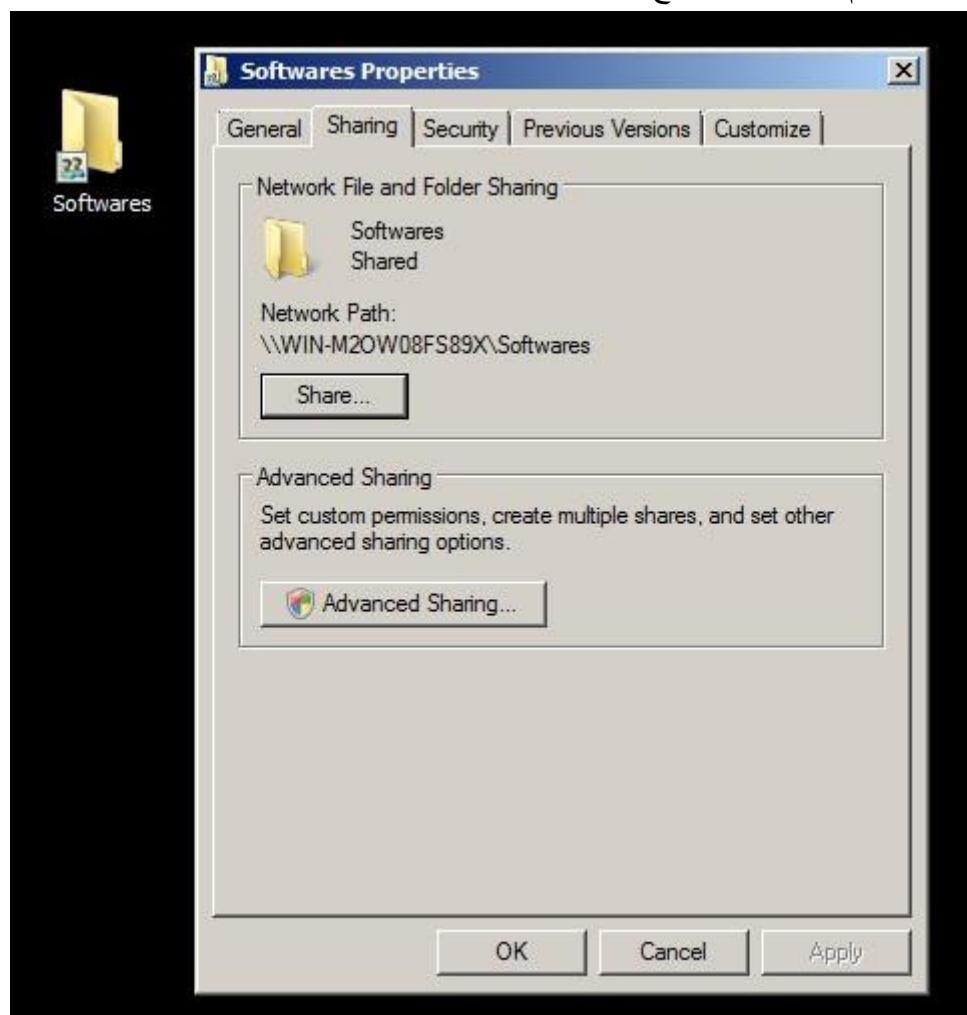
إذا قمت بتعيين البرنامج لجهاز كمبيوتر ، يتم تثبيته عند بدء تشغيل الكمبيوتر ، وهو متاح لجميع المستخدمين الذين يقومون بتسجيل الدخول إلى الكمبيوتر .

٦. نشر البرمجيات

يمكننا نشر توزيع برنامج للمستخدمين . عندما يقوم المستخدم بتسجيل الدخول إلى الكمبيوتر ، يتم عرض البرنامج المنشور في مربع الحوار إضافة أو إزالة البرنامج ، ويمكن تثبيته من هناك .

إضافة برنامج ما إلى جميع الحواسيب أو مجموعة محددة من المستخدمين تقوم بإجراءات التالية

نقوم بوضع البرنامج ضمن مجلد ونقوم بمشاركة هذا المجلد مع المستخدمين الذين سنضيف لديهم البرنامج المحدد

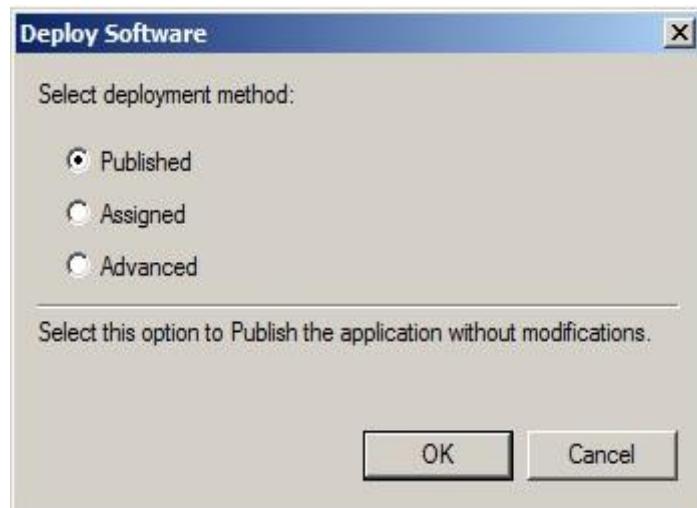


ثم ندخل ال Group Policy Management

User Configuration-> Software Setting -> Software installation->New-> Package.

في الواجهة المنبثقة نقوم بوضع رابط مشاركة المجلد ونحدد البرنامج

المراد نشرة



نختار نشر ثم موافق
من أجل تثبيت البرنامج في طرف المستخدم نسجل
دخول من حساب احد المستخدمين نذهب إلى
لوحة التحكم -> إضافة أو إزالة برنامج -> إضافة برنامج جديدة ونضغط إضافة



5. المشاكل أثناء العمل :

بعد التوصيف الكامل لشبكة الكلية الذي استغرق حوالي شهر كامل من الفحص والتوثيق بأوقات الدوام وخارج أوقات الدوام وخارج أوقات الدوام وقد واجهتنا العديد المعوقات منها: مشغولية القاعات وبعض المكاتب المقفلة وبعد الانتهاء من فحص كامل النقاط والأجهزة وتوثيقها وجدنا بعض المشاكل واقتربنا حلول لها كما ذكرنا سابقا في الفقرة [1_4](#) [Ba la3afat ilay An sisirferr al-khamis b-al-kalayah kan yeani min b3es mashaikh wakan min al-suuobia ttabiq kafa3a al-3amli3 lihi .](#)

6. المراجع

<https://www.lepide.com/blog/top-10-most-important-group-policy->

/settings-for-preventing-security-breaches

<https://www.lifewire.com/wlan-816565>

<https://www.sans.edu/cyber-research/security-laboratory/article/401-tnetwork-types>

<http://abuelfateh.com>