

الباب الثالث

(Active Directory)

❏ (١) ما هو الدليل النشط ؟

❖ **الدليل النشط** : عبارة عن خدمة موجودة داخل نظام تشغيل الخادم، و تتكون من مجموعة كبيرة من العناصر، و تم تقسيمها في شكل هرمي لتسهيل التعامل مع الدليل و تصحيح أي أخطاء و مشاكل قد تحدث .

❏ (٢) ما هي وظائف الدليل النشط في شبكة الإتصال ؟

- ❶ توفير دليل يحتوي على قائمة هيكلية بكل الكائنات الموجودة في الشبكة، **مثل** : المستخدمين (Users) و المجموعات (Groups) و الأجهزة (Devices) .
- ❷ توفير نقطة واحدة لإدارة الكائنات من المستخدمين و أجهزة الكمبيوتر و الموارد .
- ❸ توفير خدمة التوثيق و الأمن التي توفر إمكانية الوصول إلى موارد الشبكة و التحكم بها .
- ❹ تفويض من الإدارة للسماح بالإدارة الغير مركزية لكائنات الدليل النشط (Users and Groups) .

❏ (٣) اذكر ما هو تخطيط الدليل النشط ؟

- ❶ تخطيط الدليل النشط على عدة مستويات، بحيث يتضمن كل مستوى مجموعة من الكائنات يسهل التحكم بها.
- ❷ تقسيم عناصر الدليل النشط في شكل هرمي لتسهيل التعامل معها و لتسهيل تصحيح الأخطاء .

(مكونات الدليل النشط)

❏ (٤) ما هي عناصر البنية الهرمية للدليل النشط ؟

- ❶ المجال (Domain) و الوحدات التنظيمية (OU) .
- ❷ التفرعات (Tree) و مجموعات التفرع (Forest) .
- ❸ خادم الكتالوج العام (Global Catalog) .

(مكونات الدليل النشط)

❏ (٥) اشرح البنية الهرمية للدليل النشط ؟

- ❶ المجال (Domain) و الوحدات النمطية (OU) :
 - ❶ كائنات الدليل النشط : كلمة كائن تطلق على أي عنصر من موارد الشبكة، **مثل** : المستخدم (User) و المجموعة (Group) و الجهاز (Device) .
 - ❷ وحدات تنظيمية (Organizational Unit) : عبارة عن تجمع تنظيمي لبعض الكائنات داخل (Active Directory Domain) و يكون لها قاسم مشترك معين .
 - ❸ المجال أو النطاق (Domain) : عبارة عن مجموعة من أجهزة و مستخدمين و مجموعات تربط بينها علاقة ثقة من نوع ما و تتشارك في بعض الخصائص المشتركة و لها قاعدة بيانات واحدة .
- ❷ التفرعات (Tree) و مجموعات التفرع (Forest) :
 - ❶ التفرع (Tree) : هو مجموعة من مجال (Domain) و التي تربط بينها علاقة ثقة متعددة ذات اتجاهين، و غالباً ما تكون من : (Parent Domain, Child Domain and Sub Domain) .
 - ❷ علاقة الثقة المتعدية : عبارة عن علاقة ثقة تربط بين اثنين Domain مختلفين عن بعضهما البعض، و تسمح بدخول أي مستخدم من أحد الـ Domain إلى الـ Domain الآخر .
 - ❸ مجموعة التفرع (Forest) : هي مجموعة من الأشجار (Tree) مرتبطة مع بعضها البعض عن طريق علاقات الثقة المتبادلة بينهم .
- ❸ خادم الكتالوج العام (GC) : هو عبارة عن نوع جديد من قواعد البيانات يحتوي على قائمة بالخدمات التي يمكن الوصول إليها من داخل شبكة الإتصال و يتم تثبيته على وحدة تحكم واحدة DC .
❖ **مميزاته** : تسجيل الدخول - الإستعلام و البحث عن موارد محددة .

❏ (٦) ما هو مخطط البيانات ؟ و ما هي أهميته ؟

❏ **مخطط البيانات (Schema) :** عبارة عن تعريف لجميع الكائنات و خصائصها الموجودة و المخزنة في قاعدة بيانات الدليل النشط، أي تقديم المعلومات المخزنة التي يوفرها الدليل بصورة متتابعة لجميع كائناته، و ذلك عن طريق دليل (Guide) : و هو عبارة عن رقم عشري خاص بالكائن و يسمح بتغيير اسم الكائن دون التأثير على الأمن .

❏ **أهمية مخطط البيانات :**

- ① يحدد المعلومات المخزنة و التي يوفرها الدليل النشط بصورة متتابعة لكل كائناته .
- ② إنشاء الحقول المحددة لكل كائن من قبل مدير الشبكة .
- ③ يوفر أدوار لكل الكائنات الموجودة في الدليل النشط، كذلك أدوار الوحدات التنظيمية في شبكة الإتصال .

❏ (٧) ما المقصود بنشر عناصر إلى الدليل ؟ و ما هي أهميته ؟ مع ذكر العيوب الناتجة عنه ؟

❏ **نشر عناصر إلى الدليل :** هي عملية توزيع معلومات عن الكائنات المستضافة على خوادم المستخدمين الموجودة في أنحاء شبكة الإتصال .

❏ **أهميته :**

- ① الوصول إلى الكائنات بمنتهى السهولة في جميع الشبكة .
- ② السماح للشبكات الكبيرة التي عليها موارد تستضيفها خوادم في مواقع متعددة من نقطة مركزية على شبكة الإتصال .

❏ **عيوبه :** نشر الكائنات في الدليل يؤدي إلى زيادة تدفق تكرار المجال .

❏ (٨) ما هو متحكم الميدان ؟

❏ **متحكم الميدان :** هو عبارة عن جهاز يعمل على ويندوز سيرفر تم تثبيت Active Directory فيه، و هو المسئول الرئيسي عن عمليات التحقق من الصحة لجميع المستخدمين و الأجهزة و عمليات تسجيل الدخول و الوصول لكثير من الموارد المشاركة على الشبكة .

❏ (٩) ما هو التكرار ؟ و ما متطلباته في مجال الدليل النشط ؟

❏ **التكرار :** عبارة عن نسخ معلومات الدليل بين وحدات التحكم في الشبكة حتى يكون لديها نفس المعلومات، و يمكن استعلام أيًا من وحدات التحكم عن جهاز أو مستخدم معين .

❏ **يتطلب 4 فئات أساسية من المعلومات للتكرار، هم :**

- ① التوصيف .
- ② مخطط البيانات (Schema) .
- ③ المجال (Domain) .
- ④ معلومات عن الكتالوج العام (معلومات عن كل كائنات الدليل) .

❏ (١٠) ما هي أسباب استخدام مجالات متعددة في شبكة الإتصال ؟

- ① توفير بيانات شبكة الإتصال .
- ② الأمن و الإدارة .
- ③ تفويض الإدارة .
- ④ التكرار، و ذلك نتيجة لوجود خوادم كتالوج عام يقوم بنشر المعلومات بين المجالات من أجل وصول المستخدمين إليها .

❏ (١١) ما هي المعلومات التي يقوم الدليل النشط بتخزينها لإدخال دليل معين ؟ (خدمات الدليل)

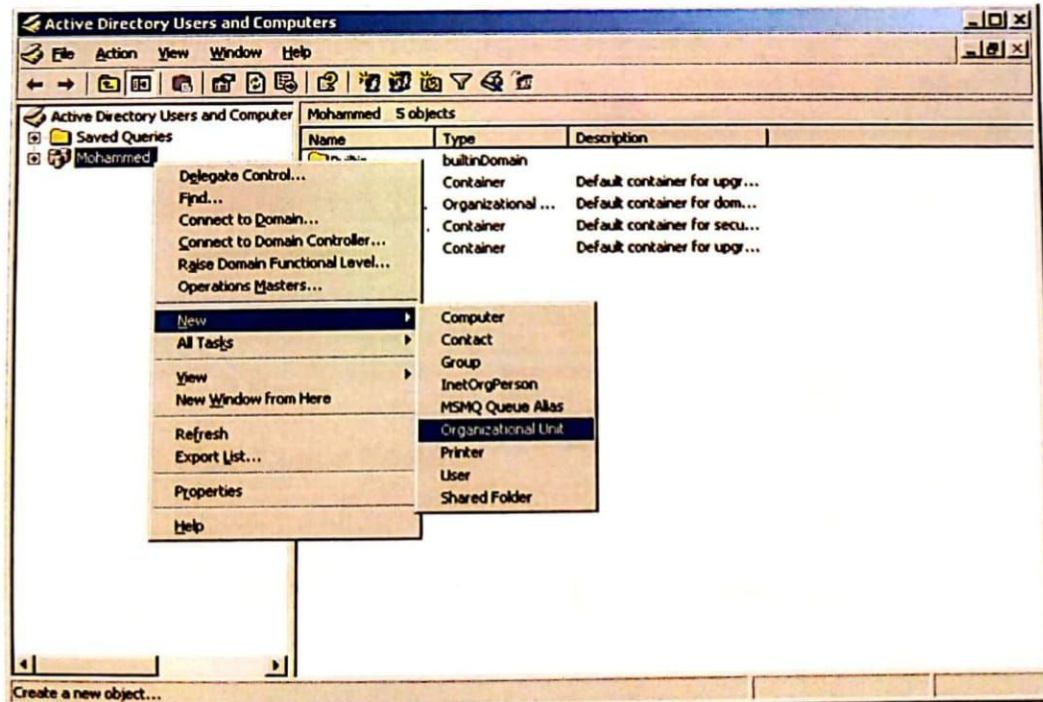
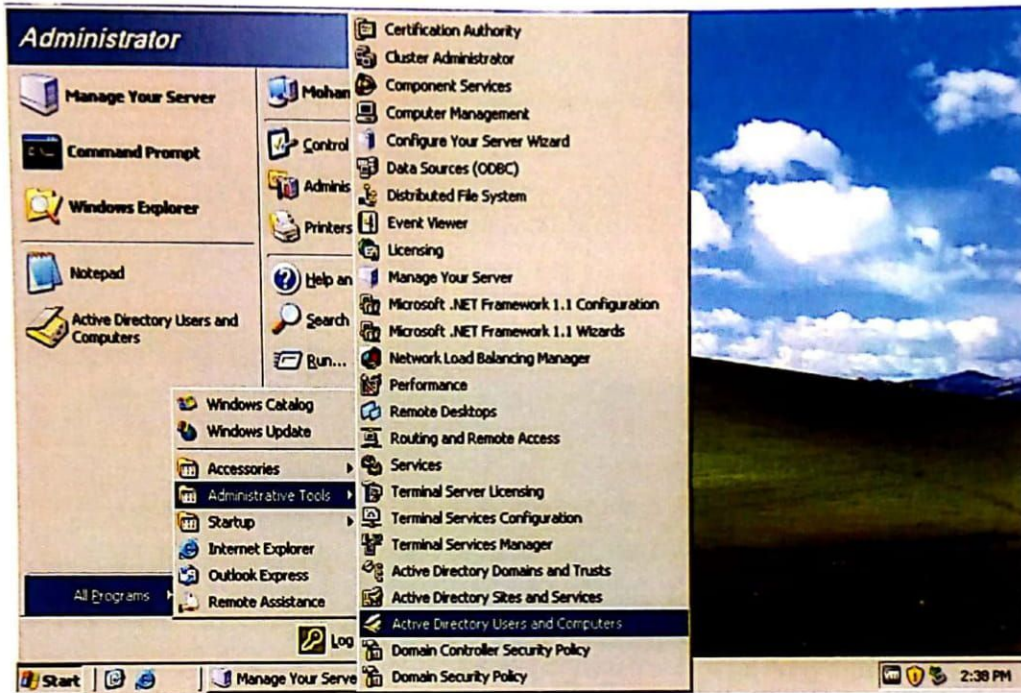
❏ اسم المستخدم و معلومات جهات الإتصال، **مثل :**

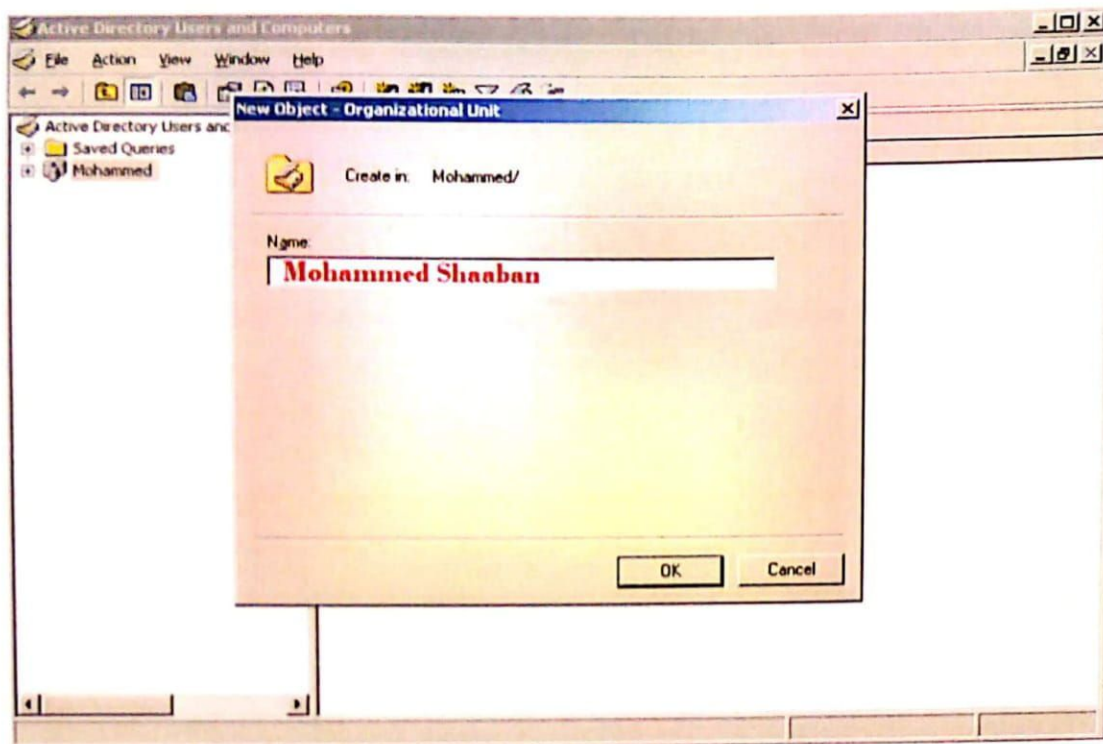
(العنوان المادي - أرقام الهاتف - البريد الإلكتروني - جهات الإتصال الإدارية و الملكيات - سمات الكائنات) .

إدارة المستخدمين و التحكم في موارد الشبكة :

① إنشاء وحدة تنظيمية :

- ① افتح قائمة **Start** .
- ② اختر منها **All Programs** ثم **Administrative Tools** .
- ③ اختر منها **Active Directory Users and Computers** .
- ④ اضغط كليك يمين على اسم المجال (**Mohammed**) و اختر (**New**) ثم (**Organizational Unit**) .





② إنشاء حساب لمستخدم و ضبط الصلاحيات :

- ① افتح قائمة **Start** .
- ② اختر منها **All Programs** ثم **Administrative Tools** .
- ③ اختر منها **Active Directory Users and Computers** .
- ② اضغط بالزر الأيمن على المجال (إسم المجال المُعطى في السؤال)، فتظهر قائمة مختصرة، اختر منها **New**، و من القائمة المنسدلة اضغط على **User** .
- ③ تظهر قائمة بإسم **New Object - User** :

New Object - User
X

First Name	الإسم الأول المُعطى في السؤال
Last Name	الإسم الأخير المُعطى في السؤال
Full Name	الإسم بالكامل (الإسم الأول + الإسم الثاني)
User Logon Name	<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 1px solid black; padding: 2px; width: 40%;">إسم الدخول المُعطى في السؤال</div> <div style="border: 1px solid black; padding: 2px; width: 55%;">.Com. إسم المجال المُعطى في السؤال @</div> </div>

< Back
Next >
Cancel

- ④ اضغط **Next**، فتظهر قائمة أخرى لإنشاء كلمة السر :

- 5 **نضغط Next، ثم نضغط Finish،** فتظهر أيقونة باسم (إسم المستخدم المُعطى في السؤال)، اضغط بالزر الأيمن للفأرة على أيقونة المستخدم، ثم اختر **Properties** .
- 6 تظهر قائمة باسم (**Properties** + إسم المستخدم المُعطى في السؤال)، اختر منها **Logon Hours** للتحكم في الأوقات .
- 7 تظهر قائمة باسم (**Logon Hours For** + إسم المستخدم المُعطى في السؤال) :

8 اضغط OK، ثم اختر أيقونة باسم Log On To، للسماح بالدخول على الأجهزة :

9 اضغط **Add**، ثم اضغط **OK**.

مثال :

قم بإنشاء حساب لمستخدم اسمه بالكامل **Mohammed Shaaban** في مجال **engineers.server** و اسم الدخول **eng.mohammed** و له الصلاحيات الآتية
 كلمة السر **MSHbn96%** ولا يستطيع المستخدم تغيير كلمة السر ولا تنتهي صلاحية كلمة السر .
 السماح للمستخدم بالدخول من الساعة 8 ص حتى الساعة 9 م . جميع الأيام عدا يومي الجمعة و السبت .
 الدخول على الأجهزة **PC1,PC7** .

- ① افتح قائمة Start .
- ② اختر منها **All Programs** ثم **Administrative Tools** .
- ③ اختر منها **Active Directory Users and Computers** .
- ④ اضغط بالزر الأيمن على المجال (**engineers.server**)، فتظهر قائمة مختصرة، اختر منها **New**، و من القائمة المنسدلة اضغط على **User** .
- ⑤ تظهر قائمة باسم **New Object - User** :

New Object - User
✕

First Name	Mohammed
Last Name	Shaaban
Full Name	Mohammed Shaaban
User Logon Name	<div style="display: flex; justify-content: space-between; border: 1px solid black; padding: 5px;"> <div style="border: 1px solid black; padding: 5px; width: 45%;">eng.mohammed</div> <div style="border: 1px solid black; padding: 5px; width: 45%;">@engineers.server .Com</div> </div>

< Back
Next >
Cancel

- ④ اضغط **Next**، فتظهر قائمة أخرى لإنشاء كلمة السر :

New Object - User [X]

Password
Confirm Password

☐ User must Change Password at next Logon .
☒ User Can not Change Password .
☒ Password Never expired .
☐ Account is disabled .

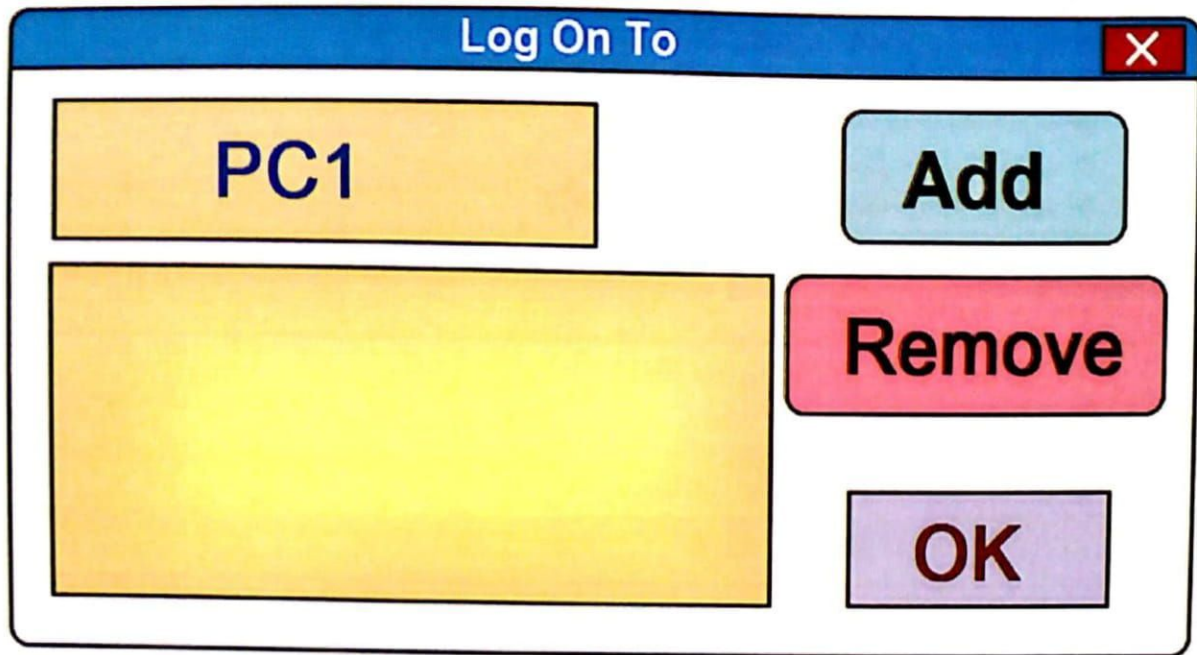
- 5 نضغط **Next**، ثم نضغط **Finish**، فتظهر أيقونة بإسم (Mohammed Shaaban)،
 اضغط بالزر الأيمن للفأرة على أيقونة المستخدم، ثم اختر **Properties** .
 6 تظهر قائمة بإسم (Mohammed Shaaban Properties)، اختر منها **Logon Hours** للتحكم في الأوقات .
 7 تظهر قائمة بإسم (Logon Hours For Mohammed Shaaban)

Logon Hours For Mohammed Shaaban [X]

	12	2	4	6	8	10	12	2	4	6	8	10	12
All													
Sunday													
Monday													
Tuesday													
Wednesday													
Thursday													
Friday													
Saturday													

☒ Logon Permitted
☐ Logon Denied

- 8 اضغط **OK**، ثم اختر أيقونة **Log On To**، للسماح بالدخول على الأجهزة :



Log On To

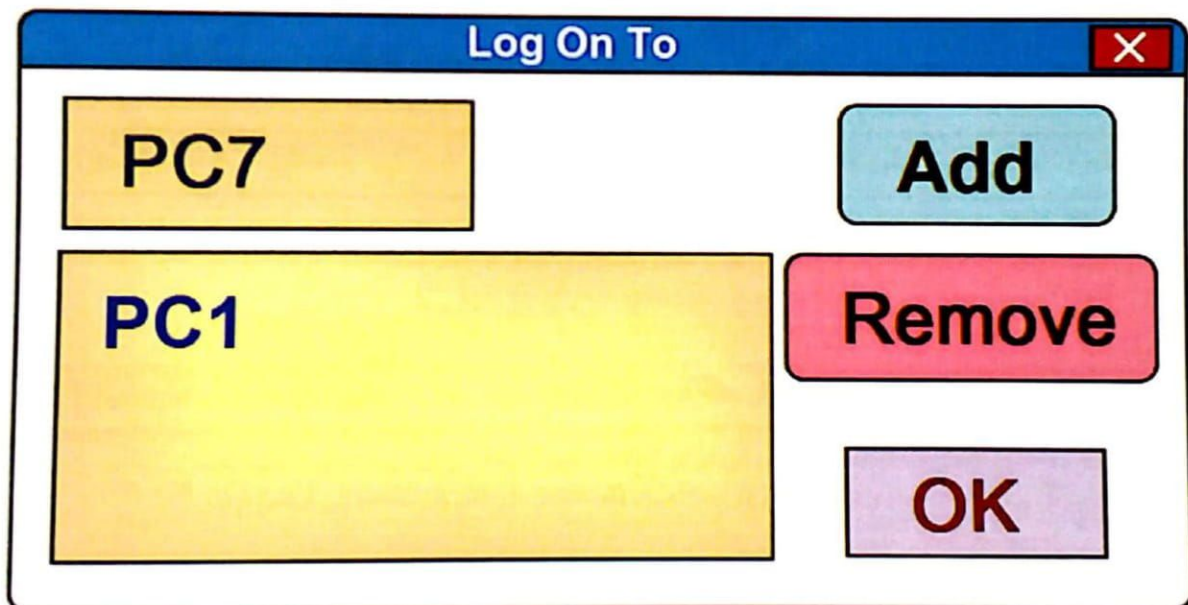
PC1

Add

Remove

OK

9 أكتب اسم الجهاز ثم اضغط Add :



Log On To

PC7

PC1

Add

Remove

OK

10 أكتب اسم الجهاز ثم اضغط Add، ثم بعد ذلك اضغط OK .

ملحوظة : يمكن إنشاء حساب لمستخدم على وحدة تنظيمية (OU) أو على المجال مباشرة .

(القواعد التي تجعل كلمة السر قوية)

١٢) ما هي الشروط المقترحة لكلمة السر ؟

- ١ يجب أن يبلغ طولها 7 أحرف أو أكثر على أقل تقدير .
- ٢ يجب أن تكون مزيجاً من الأحرف و الأرقام .
- ٣ يجب أن تشتمل على أحرف كبيرة و صغيرة (M,m) .
- ٤ يجب أن تشتمل على رمز خاص واحد أو أكثر (& , \$, %) .
- ٥ يجب ألا تمثل كلمة محجوزة، مثل : (Administrator) .
- ٦ يجب ألا تكون الأحرف و الأرقام مرتبطة .

١٣) ما هي حالات كلمة السر ؟

- ١ إلزام المستخدم بتغيير كلمة السر في المرة القادمة لدخوله إلى الـ Domain .
- ٢ لا يستطيع المستخدم تغيير كلمة السر .
- ٣ كلمة المرور لا تفقد صلاحيتها بمرور الوقت .
- ٤ تم إنشاء حساب لمستخدم و لكنه غير مفعل لحين استخدامه .

١٤) ما هي طريقة إلغاء كلمة السر ؟

- ١ افتح قائمة Start .
 - ٢ اختر منها All Programs ثم Administrative Tools .
 - ٣ اختر منها Domain Security Policy .
 - ٤ اختر منها Account Policies .
 - ٥ اختر منها Password Policy .
 - ٦ قم بتقليل طول كلمة السر و إلغاء تعقيدها :
- Minimum Password Length (0 Characters) .
- Passwords must meet complexity requirements met (Disable) .

١٥) اذكر فقط بعض عناصر التحكم في صلاحيات المستخدم ؟ (استنتج من المثال السابق)

- ١ تحديد ساعات الدخول .
- ٢ السماح لأجهزة الحاسب أو السماح لجهاز معين بالدخول و العمل أو عدم السماح .
- ٣ تحديد موعد إنتهاء المدة المتاحة لحساب المستخدم .
- ٤ صلاحيات المستخدم (حالات كلمة السر) .

(Domain Name Server)

١٦) اذكر ما تعرفه عن خدمة ترجمة العناوين DNS ؟

- يستخدم الدليل هذه الخدمة للوصول إلى مواقع الكائنات على الشبكة، أي أن أي اسم في الدليل لابد أن يتبع هذه الخدمة، و يقوم DNS بترجمة أسماء النطاقات و كل كائن من كلمات إلى أرقام تعرف باسم (IP Address) .
- مكوناته أو مستوياته :
- ١ النطاق الجذري (Root Domain) : يمثل أعلى مستوى و يشار إليه بنقطة .
 - ٢ مستوى القمة للنطاقات (Top Level Domain) : يمثل من رمزين إلى ثلاثة رموز (org,net,com) .
 - ٣ المستوى الثاني للنطاقات (Second Level Domain) : تمثل Sub Domain يحتوي على مستخدمين .
 - ٤ أسماء المضيفين (Host Names) : إشارة إلى أجهزة الكمبيوتر الموجودة على الإنترنت .
- ملاحظات هامة :
- ١ (AD , DNS) لابد أن يشتركا في نفس الوحدة التنظيمية المركزية (Domain) .
 - ٢ DNS لا يقوم بتخزين كائنات و لكنه يقوم بتخزين مجالات و معلومات .
 - ٣ DNS يقوم بتخزين FQDN و عنوان الـ IP المرتبط به .
 - ٤ DNS لا يتطلب وجود خدمة AD و لكن العكس صحيح .

تعد مزيجًا من اسم الكمبيوتر الخاص بالكمبيوتر المثبت عليه ويندوز سيرفر 2003 ، و اسم المجال الذي يوجد عليه حاليًا، على سبيل المثال : اسم الكمبيوتر الذي يستخدمه ويندوز سيرفر 2003 في مجال Server اسم الكمبيوتر المكافئ هو (Computer.server.com)، وإذا كان هذا الكمبيوتر عضوًا في مجال فرعي (Sales.server.com)، في هذه الحالة سيكون FQDN للكمبيوتر هو : (Computersales.server.com).

هي خدمة تسمح لكل وحدات التحكم في المجال باستخدام نفس قاعدة البيانات التي يتم تحديثها تلقائيًا عند إضافة أجهزة كمبيوتر جديدة إلى شبكة الاتصال وإزالتها منها، أي يقوم DDNS بربط (DNS , DHCP) معًا .
و بالتالي عندما يقوم DHCP بإجراء تغيير فإنه يقوم بإرسال المعلومات إلى المنطقة المناسبة في DNS الذي يقوم بعد ذلك بعكس التغيير، أي يسمح لأجهزة الزبائن بالشبكة أن تقوم بتسجيل بياناتها في DNS بشكل تلقائي بدون تدخل من المدير أو المستخدمين .

- 1 يرسل Resolver من العميل إلى DNS Local استعلام عن كيفية الوصول إلى العنوان (www.yahoo.com) ، إذا كان الاسم موجود لديه يُعطى وإذا لم يجده يذهب إلى خادم آخر .
- 2 يقوم الخادم المحلي بإرسال طلب العميل إلى الخادم الجذري (Root) وهو (Top Level) .
- 3 يبحث Root DNS عن الخادم المسنول عن com من القوائم عنده ويرسلها إلى Local DNS .
- 4 يرسل DNS Local إلى DNA.com استعلام عن (www.yahoo.com) .
- 5 يراجع قوائم العناوين الموجودة لديه المسنولة عن (yahoo.com) ويرسلها إلى DNA Local .
- 6 يرسل Local DNA الخادم المسنول عن (yahoo.com) و يطلب استعلام عنه .
- 7 يرسل (DNA Server yahoo.com) يرسل (Ip addressing) إلى (DNA Local) .
- 8 يرسل DNS Local العنوان الخاص بـ (www.yahoo.com) إلى العميل .
- 9 يقوم Resolver باستقبال العنوان و يقوم الجهاز بتخزينه في الذاكرة المحلية لحين طلبه مرة أخرى .

- 1 الإسم الأول .
- 2 أول حرف في الإسم الأوسط للمستخدم .
- 3 الإسم الأخير .
- 4 الإسم الكامل للمستخدم .
- 5 اسم دخول في المجال للمستخدم .
- 6 اسم دخول غير متكرر في المجال للإصدارات السابقة .



أسئلة الباب الثالث

- ① عرف الدليل النشط مع ذكر وظيفته في شبكة الإتصال ؟
- ② اذكر تخطيط الدليل النشط ؟
- ③ اذكر تقسيم الدليل النشط في ويندوز سيرفر 2003 ؟
- ④ عرف مخطط البيانات و ما أهميته ؟
- ⑤ عرف المجال و متحكم الميدان و أسباب استخدام مجالات متعددة في شبكة الإتصال ؟
- ⑥ عرف التفرع مع تفرع العلاقة المتعدية ؟
- ⑦ عرف مجموعة التفرع و خادم الكتالوج ؟
- ⑧ ما المقصود بالتكرار للدليل النشط بين المواقع ؟
- ⑨ ما المقصود بنشر عناصر الدليل و ما أهميته مع ذكر عيوبه ؟
- ⑩ اذكر ما تعرفه عن DNS و مكوناته و علاقته بالدليل النشط ؟
- ⑪ اذكر ما تعرفه عن FQNS و DDNS ؟
- ⑫ ما هي الشروط لإنشاء كلمة سر و حالات كلمة المرور و إلغاء كلمة السر ؟
- ⑬ ما هي عناصر إنشاء المستخدم ؟
- ⑭ قم بإنشاء حساب مستخدم بإسم أول **Mohammed Shaaban** و اسم دخول على المجال **BNS** في وحدة تنظيمية **Sales** و اسم الدخول **Eng-Mohammed** و له الصلاحيات الآتية :
 - ① كلمة السر %4YK2ms و لابد من تغيير كلمة السر .
 - ② يدخل على الأجهزة (PC1 , PC2 , PC7) فقط .
 - ③ السماح بالدخول من 9 صباحاً حتى 2 مساءً، جميع الأيام عدا يوم الأحد .
- ⑮ قم بإنشاء حساب بإسم أول **Islam** و له الصلاحيات الآتية :
 - ① كلمة السر **Islamsh20** و الحساب ملغي مؤقتاً .
 - ② الدخول على جهازي (Lab5 – Lab6) .
 - ③ السماح للمستخدم بالدخول يومي الإثنين و الخميس فقط من كل أسبوع .
- ⑯ قم بإنشاء حساب بإسم دخول **Ahmed** و له الصلاحيات الآتية :
 - ① كلمة السر **ab** ولا يستطيع المستخدم تغييرها .
 - ② الدخول على جهاز **PC1** .
 - ③ السماح للمستخدم بالدخول يومي الإثنين و الثلاثاء فقط .
- ⑰ قم بإنشاء حساب بإسم دخول **engineering** :
 - ① كلمة السر **AAA** مع إمكانية تغييرها في المرة التالية للدخول .
 - ② الدخول على جهازي (Lab7 – Lab9) فقط .
 - ③ السماح للمستخدم بالدخول يومي الإثنين و الجمعة فقط من كل أسبوع .