

### *TCP/IP Introduction – Arabic Paper*

ASK PC "The Largest Arabic Technical Support Community Online"

Sponsored by "Culminis"

Published: May 24, 2007

Author: Abdelrauf Hafiz Mohamed Basheer

Email: [abdu\\_r2001@hotmail.com](mailto:abdu_r2001@hotmail.com)

Supervision: Mohamed N. El-Guindy, ASK PC Community Leader

## البروتوكولات

### ما هي البروتوكولات ؟

إن كل نوع من أنواع الشبكات له البروتوكولات الخاصة به وهي مجموعة من المواصفات والقواعد التي تمكن رزم البيانات من التنقل عبر الشبكة ، وفي الويندوز 2000 الـ ( TCP/IP ) هو البروتوكول الأساسي ، ويدعم الويندوز عدد من البروتوكولات التي تمكنه من التعامل مع التطبيقات المختلفة ، والتواصل مع غيره من أنظمة التشغيل الشبكي الأخرى ، وفهم طريقة عمل البروتوكولات ووظائفها وفوائدها هي نصف المشوار الأول إلى عالم الشبكات . خاصة بعد ظهور الأجيال الجديد من البروتوكولات التي تمكن مجموعة من الأنظمة المختلفة من الاتصال مع بعضها البعض ، لذلك كان من المهم التعرف على طريقة تعايش البروتوكولات المختلفة على نفس نظام التشغيل الواحد ، وأبسط التعاريف للبروتوكول هو أنه اللغة التي تشبه لغة الإنسان ، والحواسيب ذات اللغات المختلفة لا يمكن أن تتصل مع بعضها البعض .

## تي سي بي / آي بي ( TCP/IP )

لقد تم تطوير هذا البروتوكول من أجل ( الآربانت أنت ) ؛ ولكن مع مرور الوقت وتوسع شبكة الإنترنت أصبح بروتوكولا ساخناً ، وهو أحد أهم البروتوكولات المستخدمة هذه الأيام لجميع أنواع الشبكات . ويعود ذلك إلى كون هذه البروتوكول :

1 - فعال .

2 - ليس تابعاً أو مكتوباً من قبل شركة واحدة ، ولقد أقرت جمعية الإنترنت بكاملها استخدام هذا البروتوكول .

3 - يسمح بالاتصال بين الأنظمة المختلفة .

4 - الدخول إلى الإنترنت ، حيث يعتبر البروتوكول الرئيسي لشبكة الإنترنت . سنتعرف على الطبقات الأربع المكون منها هذا البروتوكول العجيب وترتيبها ، وعمل كل منها ،

وسنلقي نظرة على أدوات الفحص ، وتتبع الأخطاء أثناء الإرسال .

### الطبقات الأربع وبنية الشبكة :

الطبقات : عبارة عن مجموعة من التوصيات التي تستخدم عند تصميم بيئة الشبكة ، وتعتمد كل المصانع عند تصميم عتاد الشبكات على هذه الطبقات للقيام بأمرين وهما :

1 - اتصال كل طبقة مع الأخرى .

2 - اعتماد كل طبقة على الطبقات الأخرى بدون أن يكون هناك تعامل حقيقي مع طريقة عمل كل طبقة .

ولتوضيح الطبقات : عبارة عن مجموعة من البروتوكولات الموجودة في عدد مستويات كل طبقة تقوم بخدمة ما تقدمها للطبقة التي فوقها ، وتتطلب هي الخدمة من الطبقة التي تحتها ، والبروتوكول TCP/IP مكون من أربع طبقات وهي :

1 - Application

2 - Transport

3 - Internet

4 - Network Interface

وكل طبقه تتكون من عدد بروتوكولات .  
وتقوم بعمل محدد لخدمة الحواسيب في الشبكة ،  
وتمكنها من الاتصال عبر الشبكة .

1 - ويبدأ الترتيب في الطبقات  
من تحت إلى أعلى ، وتكون طبقة  
Network Interface هي أول طبقة تتعامل  
مع الشبكة ؛ إذ تلخص مهمتها في  
معرفة البنية المستخدمة في الشبكة  
هل هي Ethernet أو Token-Ring .

2 - أما طبقة Internet فهي مسؤولة  
عن عنونة الرزم من البيانات بواسطة  
IP .

3 - وطبقة Transport فهي المسؤولة  
عن وصول الرزم المرسله بواسطة طبقة  
Internet وتستخدم إما بروتوكول TCP أو  
UDP .

4 - وتبقى طبقة Application هي  
الطبقة المسؤولة عن التأكد من الترميز  
المرسل عبر الشبكة يستخدم نفس الأبجدية .  
فمعظم الحواسيب تستخدم الترميز ASCII ؛  
ولكن يوجد بعض الحواسيب التي تستخدم  
الترميز EBCDIC لأجهزة IBM ، وأيضا هذه  
الطبقة مسؤولة عن البرامج المستخدمة في

التعامل عبر الشبكة ، مثل : البريد الإلكتروني ، وبرامج قواعد البيانات . إذا كما نلاحظ أن كل طبقة تقوم بخدمة مختلفة عن الأخرى ، وتقوم بعمل مهم يخدم مهمة الإرسال

### مكونات البروتوكول TCP/IP :

#### 1 - البروتوكول Transmission (TCP) Control Protocol :

كما نعلم أن البروتوكول TCP/IP مكون من بروتوكولات مختلفة ، كل منها له عمل أو خدمة يقدمها من أجل الإرسال عبر الشبكة . وأول بروتوكول هو TCP : وهو عبارة عن بروتوكول يتحقق من وصول الإرسال ، وهو من نوع Connection-based ، ويحتاج إلى إنشاء جلسة عمل قبل إرسال البيانات بين الحواسيب ، كما يتأكد من أن جميع الرزم التي أرسلت قد تم استقبالها من الجهاز الآخر ، وإذا لم تصل هذه الرزم يقوم TCP بإرسالها مرة ثانية ، وإذا تم الاستلام يأخذ شهادة مصادقة ويقوم بإرسال الدفعة التالية ... وتتم عملية Connection Based كما يلي :

يتفق الحاسبان على الطريقة الأصلح ، لتحديد كمية البيانات التي سوف يتم إرسالها في وقت واحد ، وعلى أرقام المصادقة التي سيتم إرسالها عند استلام البيانات وما هو الوقت المناسب لقطع الاتصال ... هذا ما يسمى إنشاء جلسة عمل . وكما ترى فإن هذا البروتوكول قد يسبب حملاً زائداً عند إرسال كمية كبيرة من البيانات .

#### 2 - البروتوكول User Data ( UDP ) gram Protocol :

وهذا البروتوكول هو من نوع -No connection Based بمعنى الاتصال غير الموثق ، وهو لا ينشئ جلسة عمل بين الحواسيب أثناء الاتصال ، وهو لا يضمن وصول البيانات مثل ما أرسلت به ، وهو عكس TCP ؛ ولكن هذا البروتوكول له مميزات تجعل يستحب استخدامه في بعض الحالات . مثلاً : عند إرسال بيانات جماعية عامة ، وعند الحاجة إلى السرعة ، وسرعته من عدم حاجته إلى التحقق من دقة الإرسال . يستخدم في نقل الوسائط المتعددة ، مثل : الصوت ، والفيديو ، لأن الوسائط لا تحتاج إلى دقة الوصول ، ونستطيع أن نقول أن هذا البروتوكول ذو فاعلية كبيرة وسريع الأداء .

ومن أهم الأسباب التي أدت إلى إنشاء البروتوكول UDP :

أن الإرسال عبر هذا البروتوكول لا يتطلب إلا القليل من الحمل والوقت ، إذ أن رزمة UDP لا تحتوي على كل المعطيات التي ذكرت مع البروتوكول TCP لمراقبة الإرسال .. لذلك سمي بروتوكول الاتصال غير الموثق .

### 3 - البروتوكول Internet Protocol ( IP ) :

وهو يعد من أهم البروتوكولات لوجود عنصر العنوان الذي يستخدمه لإعطاء كل حاسب على الشبكة رقماً خاصاً به ، ويسمى عنوان إنترنت IP Address ، وهو عنوان متفرد ليس له شبيه في النطاق الشبكي ، ويتميز IP بميزتين مهمتين وهي : التوجيه وشرط الرزم ، وإعادة الرزم . فالتوجيه يقوم بفحص العنوان الموجود على الرزمة ويعطيه تصريح تجول في أرجاء الشبكة ، وهذا التصريح له مدة محددة ، فإذا انتهت هذه الفترة الزمنية ذابت تلك الرزمة ، ولم تعد تسبب ازدحام داخل الشبكة .. وعملية التشطير تستخدم في التوليف بين بعض أنواع الشبكات

المختلفة ، مثل : شبكة Token-Ring و Ethernet بسبب ما لشبكة ( توكن رنغ ) من سعة في نقل الإشارات لذلك وجب تشطيرها ثم إعادة التجميع مرة أخرى .

#### 4 - البروتوكول Internet ( ICMP ) : Control Message Protocol

وهو مسؤول عن رسائل الأخطاء التي تتعلق بتأمين وصول IP ، ويحتوي على رسائل من أشهرها التي تأتي مع الأداة Ping ، وهي رسالة Echo Request و Echo Reply .

#### 5 - البروتوكول Address Resolution Protocol ( ARP )

يقوم هذا البروتوكول بعمل جداً مهم وهو : وصف وإرشاد خدمة IP عن العنوان الفيزيائي للعنوان المطلوب ، إذ يقوم IP عند استلام طلب الاتصال بحاسب ما مثلاً : ( X ) يتوجه فوراً إلى خدمة ARP ويسأله عن مكان هذا العنوان على الشبكة ، ثم يقوم البروتوكول ARP بالبحث عن العنوان في ذاكرته فإذا وجدته قدم خريطة دقيقة للعنوان ، وإذا كان العنوان لحاسب في شبكة بعيدة يقوم ARP بتوجيه IP إلى عنوان الموجه Router ، ثم يقوم هذا الموجه بتسليم الطلب لـ ARP حتى يبحث عن العنوان الفيزيائي لرقم الـ IP .

#### س / كيف يعرف هذا البروتوكول العنوان الفيزيائي للحواسيب ؟

يعرفه برقم كرت الشبكة ، إذ كل كرت يصنع من المصانع المختلفة يكون له رقم فريد لا يشبه رقم آخر ، فيحتفظ ARP بهذه الأرقام في ذاكرته التي تشبه قاعدة البيانات بجميع الأرقام الخاصة في محيط الشبكة ، وهذا البروتوكول من أدوات الفحص

التي تستخدم في مراقبة الشبكة ، وتحديد بعض المشاكل .

### ضبط التكوين للبروتوكول TCP/IP .

ضبط التكوين يكون إما : ضبط تكوين ساكن ، أو تكوين عنوان تلقائي ، وبالشكل التلقائي يكون البروتوكول TCP/IP يحصل على عنوان IP تلقائي من الخدمة DHCP ، ولتغير الإعدادات

ووضع رقم IP ساكن يجب أن تفتح خصائص البروتوكول من Internet

Protocol TCP/IP Properties كما هو في الشكل التالي :

الوصف	الخيار
عنوان مكون من 32 بت : وهو رقم فريد داخل الشبكة ، وكل بطاقة شبكة تتشارك باستخدام البروتوكول TCP/IP يجب أن يكون لديها هذا العنوان ، وهو مثل 192.168.0.1 ويكون هذا الرقم مكون من جزأين : واحد للشبكة ، والجزء الثاني لجهاز مشغل البروتوكول ، وفي المثال السابق يكون عنوان الجهاز هو الرقم .	IP address
هذا الجزء مهم جداً لأنه يحدد هوية الشبكة ، ويستخدم في الشبكات الكبيرة عندما يقسم رقم IP واحد إلى عدة أقسام ، ويصبح كل رقم يمثل شبكة مستقلة ؛ ولكن تشترك كل هذه الشبكات بهوية واحدة يمثلها الـ Subnet Mask والـ Subnet تعني التقسيم ، وهو الذي يحدد رقم الشبكة ورقم الجهاز .	Sub net mask



يستخدم عندما تكون هناك عدد من الشبكات الفرعية ضمن الشبكة الكبيرة ، وهو يعني البوابة الافتراضية ، فعندما يطلب أحد المضيفين رقم IP ولا يجد هذا الرقم ضمن الشبكة الفرعية ، يقوم البروتوكول IP بطلب البروتوكول arp ، فيقوم هذا البروتوكول بالبحث عن هذا الرقم في الشبكات الفرعية الأخرى ، فإذا وجده يقدم للعنوان IP رقم ال Default gateway الذي يكون الرقم الهدف ضمن شبكتها الفرعية .

Default gateway

\* ملاحظة :

يمكن تعطيل الحصول على العنوان IP بشكل افتراضي عند وضع المفتاح IP Autoconfiguration Enabled في محرر السجل في المسار التالي :  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces  
وجعل قيمة ذلك المفتاح ( صفر ) .

### تحليل المشاكل للبروتوكول TCP/IP :

لبروتوكول TCP/IP عدد من الأدوات التي تساعد على اكتشاف المشاكل المتعلقة بالإرسال . وفي الجدول التالي كل الأدوات والوظيفة التي تقوم بها كل أداة ، وهي وظائف مهمة ولا غنى عنها لمن يستخدم هذا البروتوكول :

الأداة	الوظيفة
--------	---------

Ping	يختبر الاتصال بين رقمين IP ، وكذلك يستخدم في التحقق من تكوين البروتوكول .
Arp	يعرض كل العناوين كعناوين مادية ، وهذا البروتوكول له جدول تحويل العناوين من عنوان IP إلى عنوان كرت الشبكة MAC ، وبذلك يعرض العنوان الفيزيائي للجهاز .
Ipconfig	تعرض التكوين الحالي للبروتوكول TCP/IP وله عدد من المداخل التي تسمح تحرير وتغيير عنوان IP للبطاقة المطلوبة .
Nbtstat	تعرض حالة جلسات العمل للـ NetBIOS الحالية ، ولفحص عملية تحويل أسماء الـ NetBIOS إلى عناوين IP .
Netstat	تعرض الاتصالات الحالية والإحصائيات للبروتوكول TCP/IP .
Route	يعرض ويعدل جدول التوجيه المحلي .
Hostname	يطبع اسم المضيف الذي صدر من الأمر .
Tracert	يفحص ويعرض كامل مخطط الاتصال مع مضيف بعيد .

## ■ فحص سريع :

للتحقق من عمل البروتوكول TCP/IP ، وقد ضبط تكوينه لبطاقة الشبكة ، نستخدم

```
D:\>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time=0ms
Reply from 127.0.0.1: bytes=32 time=0ms
Reply from 127.0.0.1: bytes=32 time=0ms
Reply from 127.0.0.1: bytes=32 time=0ms

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Loss = 0%
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

عنوان الحلقة المكررة loop-back وهو الرقم 127.0.0.1 ، ولعمل هذا الفحص من محث الأوامر أكتب PING 127.0.0.1 ثم اضغط Enter ، إذا وجدت عرض مثل الذي في الشكل السابق ، فذلك يعني أن البروتوكول على هذا الجهاز يعمل بشكل سليم .

## آي بي أدرس ( IP ADDRESS )

إذا كان لدينا عنوان آي بي فذلك يعني أن لدينا بروتوكول TCP/IP ، فعند تثبيت هذا البروتوكول يجب أن نعرف رقم آي بي واحد على الأقل في الشبكة ، ثم نعين خادم DHCP يوزع الأرقام على جميع الحواسيب ... ويمكن أن نلخص مفهوم IP على النحو الآتي :  
رقم IP : هو لتعريف الجهاز في الشبكة ، وهو يشبه كثيراً رقم الهاتف ، فكل جهاز يدخل إلى الشبكة يكون له رقم متفرد لا يملكه جهاز آخر . ومثلاً : شبكة الإنترنت في وقت واحد لا يكون في العالم كله رقمين متشابهين ، وفي شبكة خاصة لو تُعين رقمين متشابهين لن يستطيعوا الاتصال في ما بينهم .  
يتألف عنوان IP من 32 بت مقسمة إلى أربع مجموعات ، وكل مجموعة تحتوي على 8 بت ، وتمثل هذه البتات بأرقام عشرية مثل : 131.107.2.200 ، وبما أن كل مجموعة مكونة من 8 بت ؛ فيمكن أن يكون أي مجموعة من الرقم 1 إلى 255 .

وينقسم رقم IP إلى قسمين : رقم للشبكة ، ورقم عنوان الحاسب . وينقسم كذلك من جهة ثانية إلى ثلاث مراتب ، وكل مرتبة لها عدد محدد من الشبكات الفرعية ، والحواسيب الممكنة في كل قسم من الأقسام ، وهي مرتبة كما يلي :

A 255.0.0.0

B 255.255.0.0

C 255.255.255.0

- ومرتبة (A) تبدأ من 1 إلى 126
- ومرتبة (B) تبدأ من 128 إلى

191

- ومرتبة (C) تبدأ من 192 إلى 255

الجدول التالي يبين مجال أرقام الشبكات في كل مرتبة :

Address Class	رقم الشبكة الأول	رقم الشبكة الأخير
<i>Class A</i>	1.0.0.0	126.0.0.0
<i>Class B</i>	128.0.0.0	191.255.0.0
Class C	192.0.0.0	223.255.255.0

والجدول التالي يبين مجال أرقام المستفيدين من الشبكة :

Address Class		الرقم الأخير
<i>Class A</i>	w.0.0.1	w.255.255.254
<i>Class B</i>	w.x.0.1	w.x.255.254
Class C	w.x.y.1	w.x.y.254

فإذا كان رقم الآي بي مثلاً 195.123.130.1 ، سيكون الرقم من المرتبة ( C ) ، وسيكون رقم الشبكة خانة رقم 1 و 2 و 3 ، وخانة رقم 4 هي للجهاز مستأجر الرقم .  
وإذا كان رقم الآي بي مثلاً 170.200.130.0 ، سيكون الرقم من المرتبة ( B ) ، وسيكون رقم الشبكة خانة رقم 1 و 2 ، وخانه رقم 3 و 4 هي للجهاز مستأجر الرقم .  
وإذا كان رقم الآي بي مثلاً 100.50.200.0 ، سيكون الرقم من المرتبة ( A ) ، وسيكون رقم الشبكة خانة رقم 1 ، وخانه رقم 2 و 3 و 4 هي للجهاز مستأجر الرقم .

وسنمثل بمثال يقرب الفكرة أكثر ،  
لنفترض أننا وجدنا عناوين IP مكتوبة كما  
يلي :

• 195.123.130.1

• 195.123.130.2

• 195.123.130.3

من النظرة الأولى ندقق في الرقم الأول كم  
يكون ؟ وهو عندنا في المثال 195 ، وذلك  
يعني أن الرقم من المرتبة ( C ) ، وهي  
المرتبة الثالثة ، وبشكل افتراضي يكون  
قناع الشبكة 255,255,255.0 ، حيث يمثل  
الرقم 195.123.130 رقم الشبكة ، والأرقام 1  
و 2 و 3 تمثل أرقام الحواسيب الموجودة في  
الشبكة ، ورقم الشبكة دائماً ثابت ،  
وأرقام الحواسيب تتغير .

وكل مرتبة لها عدد محدد من الشبكات  
الفرعية ، وعدد المضيفات الممكنة مبينة في  
الجدول التالي :

المرتبة	القناع الافتراضي	عدد الشبكات	عدد الأجهزة في كل شبكة
A	255.0.0.0	126	16777214
B	255.255.0.0	16384	65534
C	255.255.255.0	2097152	254

ويوجد بعض الخدمات المرتبطة مع  
بروتوكول TCP/IP وهي :

1 - ISS Internet Information Server :

وهي خدمة تمكن زبون TCP/IP من مشاركة  
البيانات مع أنظمة مختلفة من الحواسيب .

2 - DHCP Dynamic Host Configuration Protocol :

وهو يقدم عناوين IP بطريقة  
أوتوماتيكية لجميع مستخدمي الشبكة ، وهو  
تقديم وإعداد تلقائي لبروتوكول TCP/IP ،  
ويتمكن مخدم DHCP من العمل بعد إدخال  
عناوين IP في المجال Scope ، هذا المجال هو

حدود الأرقام تبدأ من كذا وتنتهي إلى كذا ، مثلاً نحدد هذا الـ Scope من 200.150.40.1 إلى 200.150.40.50 ذلك يعني أن لدينا 50 رقم IP متاح في الشبكة ، ولنتمكن زبون DHCP من أخذ الرقم من المخدم ، نفعل في جهاز الزبون الخيار Enable Automatic DHCP Configuration .

- ومن فوائد الـ DHCP ... لا يسمح بوجود عناوين من أرقام IP متشابهة .

- لن تكون مضطراً لإدخال القيم يدوياً .

- تقلص مشاكل البروتوكول TCP/IP بشكل كبير .

- تأجير عنوان IP لمدة محددة من قبل مدير النظام ، وهذه الميزة مفيدة عندما تكون عدد الحواسيب أكبر من عدد أرقام الـ IP المتاحة على مخدم DHCP .

- إذا تم نقل جهاز على شبكة فرعية ثانية سيأخذ إعداداته من مخدم DHCP فوراً .

### 3 - WINS Windows Internet Name Service :

وهو مسؤول عن إدارة أسماء الحواسيب وتحويلها إلى أرقام IP ، ويقوم مخدم WINS بهذه العملية بشكل أوماتيكي .

### 4 - DNS Domain Name Server :

وهو النظام الرئيسي المستخدم في تحويل أسماء المضيفات إلى أرقام IP على شبكة الإنترنت ، والـ DNS له عدد من النطاقات التي تعرف الفئة التي ينتمي إليها مثل :

Org	المنظمات غير الاقتصادية	Com	المنظمات التجارية
-----	-------------------------	-----	-------------------

Gov	المنظمات الحكومية غير العسكرية	Net	الشبكات
Sa	المملكة السعودية	Mil	المنظمات العسكرية

ولمعرفة رقم الـ IP الذي تستخدمه من محث الأوامر ، أكتب IPCONFIG ثم اضغط Enter .  
ولمعرفة رقم الـ IP ورقم السيرفر المؤجر لك الـ IP من محث الأوامر ، أكتب IPCONFIG/ALL ثم اضغط Enter .

إذا كنت تبحث عن صاحب رقم آي بي فأنصحك بهذه المواقع :

<http://www.ripe.net/cgi-bin/whois>

وهذا أيضاً :

<http://dns411.com/>

مع ملاحظة أن بعض من الأرقام التي تظهر لك مع برامج الحماية هي لمزود خدمة الإنترنت المشترك معه ، أو من أحد الأجهزة الموجودة على الشبكة ، ويكون معد إعداد غير جيد .



## إف تي بي ( FTP )

### : File Transfer Protocol

يعتبر FTP من الخدمات القوية ضمن البروتوكول TCP/IP ، وهو مخصص لنقل الملفات إلى مضيف بعيد ، وهو يسمح بالنقل والنسخ بين الأجهزة ، ولتتمكن من فعل ذلك يجب أن تتوفر الشروط التالية :

- يجب أن يكون في الحاسب المضيف خدمة مثبتة لزبون FTP.
- يجب على المرسل أن يكون له حساب مستخدم وكلمة مرور على الحاسب المضيف .
- يجب أن يكون مثبت على الجهازين خدمة TCP/IP.

وتستطيع العمل مع هذا البروتوكول بالنمط السطري ، أو نمط الأوامر .. والنمط السطري له عدد من الخيارات من أهمها ما يلي :

الخيار	الشرح
v-	يمنع العرض الذي يبين استجابة المخدم البعيد .
n-	يمنع التسجيل أثناء بداية الاتصال .
d-	تمكين عملية فحص الأخطاء .
s: Filename-	تحديد اسم أي ملف يحتوي على أوامر FTP ويتم تنفيذها بعد أن يبدأ FTP مباشرة .
host	تحديد اسم المضيف أو عنوان IP .
a-	يستخدم أي ملاءمة محلية عند الاتصال Binding .

ونمط الأوامر له خيارات من أهمها ما يلي :

Open	تحدد به المضيف البعيد الذي تتصل به
------	------------------------------------

Close	تفصل به الاتصال مع المضيف البعيد
Get	نسخ ملف من النظام البعيد إلى حاسبك
Put	نسخ ملف من حاسبك إلى النظام البعيد

### إضافة موقع FTP

تحتاج لإضافة موقع FTP لنقل الملفات في الشبكة إلى تثبيت Internet Information Services IIS عند تثبيت الويندوز 2000 تثبيت نظيف يكون الـ IIS بشكل افتراضي مثبت ، إما إذا كان التثبيت ترقية من إصدار سابق يحاول برنامج التثبيت إيجاد إصدار قديم من IIS ، إذا وجدته تتم الترقية إلى IIS 5.0 ، وإذا لم يجده لا يثبت الـ IIS 5.0 ، ويمكن إضافة أو إزالة الـ IIS من إضافة وإزالة البرامج في لوحة التحكم .

طريقة إضافة موقع FTP :  
بداية قم بإنشاء مجلد على محرك الأقراص ، وسيكون هو المجلد الافتراضي للموقع ، وضع فيه مثلاً الملف disk.exe .

من Administrative Tools ثم من Internet Services Manager تظهر لك النافذة الخاصة للأداة Internet Information Services ، وستجد اسم السيرفر ، أو الجهاز الخاص بك علم عليه ثم اختر New ثم FTP Site .

شاشة الترحيب انقر Next .  
أكتب اسم لتعريف موقع FTP ، وهو اسم لتعريف فقط ، ولن يستخدم في الطلب ؛ وليكن WIN2000 ثم Next .

في هذه الشاشة يطلب منك أن تختار عنوان ip ومنفذ للاتصال . افتح القائمة المنسدلة

، ستجد عنوان جهازك موجود فيه قم  
باختياره ، ثم أترك رقم المنفذ كما هو 21  
؛ لأنه الافتراضي ثم اضغط Next.

في هذه الشاشة اختر الخيارين أو اتركه  
كما هو ، حسب طبيعة الموقع لديك .  
انتهت العملية اختر Finish .

الآن من على اسم الموقع الجديد WIN2000  
اضغط بالزر الأيمن ، ثم اختر خصائص Properties ،  
ستجد كثير من الخيارات المتاحة أمامك  
للتحكم في الموقع حسب إمكانياتك المتوفرة ،  
مثلا علامة التبويب FTP Site فيها اسم  
التعريف الذي اخترته وعنوان ip والمنفذ ،  
وفيها خيار مهم وهو Limited To وهو من أجل  
عدد الاتصالات المتزامنة على الموقع ، حدد  
الرقم المناسب لقدرة ملقمك ، والخيار  
connection Timeout مدة الاتصال المسموح بين  
العميل والملقم .

وفي علامة التبويب Security Accounts تجد خيار  
السماح لـ Anonymous معلم عليه اتركه كما  
هو .

وفي علامة التبويب Home Directory تجد مسار  
المجلد الافتراضي للموقع تستطيع تغييره إذا  
أحببت ، وأيضاً خصائص التحكم Read , Write ،  
وملف الدخول Log visits .

من علامة التبويب Directory Security تستطيع  
عمل كنترول أمني جيد على عملية الدخول .

## تل نت ( TEL NET )

خدمة التل نت في ويندوز 2000 : تسمح لمستخدمين عميل التل نت بالاتصال بكمبيوتر يشغل خدمة التل نت ، واستعمال سطر الأوامر ، ويصبح كما لو كان يجلس أمامه ، ويمكن أن تكون خدمة التل نت عبارة لاتصال المستخدمين مع بعضهم البعض .  
وأي كمبيوتر يشغل خدمة التل نت يمكن أن يدعم إلى 63 عميل تل نت في أي وقت .  
يمكن استعمال اسمك وكلمة المرور الخاصة بك من أجل الوصول إلى ملقم التل نت ، إذا كنت تستخدم خيار التحقق من الصحة NTLM سيرسل الاسم وكلمة المرور مشفرة ، وإذا لم تكن مستخدمة سترسل كنص عادي .

### \* ملاحظة :

إذا كان هذا الخيار منشط في خصائص كلمة المرور لأحد المستخدمين ، لن يتمكن من الدخول على ملقم التلنت . عند استخدام NTLM يجب الدخول ثم تغيير كلمة المرور ثم التسجيل على خدمة التلنت .

### تشغيل وإيقاف ملقم التلنت :

في التثبيت الافتراضي لويندوز 2000 تكون خدمة التل نت غير منشطة ، وتكون على الوضع اليدوي ، ويمكن استخدام الأداة Services لتشغيل أو إيقاف خدمة التل نت .  
تشغيل التل نت و إيقافه من سطر الأوامر :

يمكن استخدام الأداة Telnet Server Admin لتشغيل أو إيقاف أو الحصول على معلومات عن الملقم ، ويمكن كذلك الحصول على عدد

المستخدمين والتحكم في الجلسة الحالية من إنهاء الاتصال وتغير الإعدادات .  
 لفتح الأداة Telnet Server Admin أضغط على Administrative Tools الموجودة في Telnet Administration Tool ، أو اضغط Start ثم Run أكتب tlntadm ثم OK ، إذا كنت لا تستطيع فتح الأداة Telnet Server Admin تحتاج إلى تثبيت أدوات الإدارة ( Adminpak.msi ) .  
 يبين الجدول التالي خيارات الأداة Telnet Server Administration :

الوصف	الاسم	الخيار
ينهي جلسة الأداة Telnet Server Admin .	Quit this application	Q
يبين المستخدمين المتصلين بخدمة التلنت ، مع توضيح اسم المستخدم والدومين وعنوان الجهاز ووقت الدخول .	List the current users	L
ينهي جلسة أحد المستخدمين الذي أنت تختاره .	Terminate a user session	T
يزود قائمة بإعدادات السجل التي يمكن تغييرها .	Display/change registry settings	D
يشغل خدمة التلنت .	Start the service	S
يوقف خدمة التلنت .	Stop the service	St

### اصطيات المشاكل :

يبين الجدول التالي بعض المشاكل التي يمكن أن تواجهك عند استخدام التل نت :

الحل	السبب	رسالة الخطاء
راجع الخيارات وأعد كتابة خيارك	القيمة المكتوبة لم تكن مقبولة	Invalid input
شغل خدمة التل نت	خدمة التل نت غير مشغلة	Failed to open the registry key
شغل الخدمة	خدمة التل نت غير مشغلة على الملقم	Failed to query the registry value

### استعمال التل نت :

لتشغيل Telnet انقر Start ، ثم Run ، ثم أكتب telnet ، وتستطيع كتابة telnet في موجه الأوامر ، لتتمكن من استخدام التل نت يجب أن يكون البروتوكول TCP/IP مثبت على جهازك ومضبوط تكوينه ، ويكون لديك حساب مسجل على الجهاز الذي ستصل به .

تمرين ضبط واتصال بخدمة التل نت :  
في هذا التمرين يجب أن يكون لديك شبكة على الأقل جهازين متصلين مع بعضهم البعض ، ولنفترض أن الجهاز الأول اسمه Hishem1 والثاني Hishem2 .

وسنفترض أن خدمة التل نت مثبتة على Hishem2 ، ثم سنقوم بالاتصال من Hishem1 إلى Hishem2 .

سنقوم الآن بتثبيت الخدمة على جهاز Hishem1 :

1 - سجل الدخول إلى Hishem1 ك Administrator .

- 2 - من Start ثم Programs ثم Administrative Tools اضغط Services . تظهر الأداة Services .
- 3 - من النافذة مرر إلى اسفل ثم اضغط مزدوج على Telnet .  
يظهر مربع حوار ( The Telnet Properties Local Computer )
- 4 - غير Startup Type من Manual إلى Automatic .
- 5 - في القسم Service status اضغط Start .
- 6 - اضغط OK لإغلاق مربع الحوار Local Computer Telnet properties .
- 7 - أغلق وحدة التحكم Services .  
سنتصل من Hishem1 إلى Hishem2 :
- 1 - من Start ثم Run .
- 2 - أكتب telnet ثم OK .  
تظهر موجه أوامر مايكروسوفت تل نت .
- 3 - أكتب help أو ؟ لمشاهدة الأوامر المتاحة .  
تظهر جميع الأوامر المدعومة في خدمة التل نت .
- 4 - أكتب open Hishem2 .  
ستشاهد شاشة الترحيب التالية :

```
D:\WINNT\System32\telnet.exe
*=====
Welcome to Microsoft Telnet Server.
*=====
C:\>
```

ملاحظة : يمكن استخدام حرف o بدل  
. open

- 5 - أي أوامر يمكنك تشغيلها من سطر الأوامر في Hishem2 .
- 6 - اترك هذا الاتصال نشط لا توقفه ، سننتقل الآن إلى جهاز Hishem2 لمشاهدة جلسة التلنت .
- من جهاز Hishem2 سنراقب خدمة التلنت ، ثم نوقف ونقطع الاتصال من العميل Hishem1 :
- 1 - من Start ثم Run .
- 2 - أكتب tlntadmn ثم OK .
- يظهر إطار أوامر الأداة Telnet Server Admin .
- 3 - أكتب 1 لمشاهدة جميع الاتصالات الحالية . كما في المثال نشاهد قد عرض اسم المستخدم واسم الدومين WIN ورقم IP

```
Select one of the following options:

0> Quit this application
1> List the current users
2> Terminate a user session ...
3> Display / change registry settings ...
4> Start the service
5> Stop the service

Type an option number [0 - 5] to select that option: 1

CURRENT USERS

  USERNAME      DOMAIN      REMOTE MACHINE      SESSION ID
-----
Administrator  NOR          131.107.2.200       3

Select one of the following options:

0> Quit this application
1> List the current users
2> Terminate a user session ...
3> Display / change registry settings ...
4> Start the service
5> Stop the service
```

- ونوع الاتصال ووقت الدخول .
- أكتب 2 لإنهاء جلسة مستخدم .
- تظهر رسالة تطلب منك تحديد هوية المستخدم الذي تريد فصله .



أكتب 1 هذا رقم المستخدم في القائمة ،  
ولا يوجد معنا في المثال غير واحد ، لذلك  
تكتب 1 .

تظهر لائحة بالأوامر المتاحة .  
ارجع إلى جهاز Hishem1 سترا أن الاتصال قد

```
D:\WINNT\System32\telnet.exe
=====
Welcome to Microsoft Telnet Server.
=====
C:\>

Connection to host lost.
Press any key to continue...
```

انفصل كما في الشكل التالي :  
7 - اضغط Enter للمتابعة .  
كيف نستفيد من خدمة التل نت في جلب  
البريد :

إذ تعذر عليك سحب البريد بالبرامج  
المخصصة لسبب ما ، يمكن أن تستخدم التل نت  
لسحب البريد وحذف الرسائل التي قد تكون  
سبب المشكلة ، والطريقة كما يلي :

- تكون على اتصال مع الشبكة .
- من Start ثم Run ثم تكتب Telnet  
pop.mail.yahoo.com 110 طبعاً إذا كان حسابك  
مع الياهو ، أو أكتب الحساب الخاص بك  
مع ملاحظة وجود فراغ بين الكلمة الأولى  
والجملة الثانية والرقم .
- ستظهر لك نافذة مثل الدوس أكتب  
user ، ثم أكتب بعدها اسم المستخدم في  
بريدك مع ملاحظة أن الذي ستكتبه لا  
تشاهده على النافذة لا تهتم مثل user xxxx  
ثم Enter .

- بعد ذلك أكتب pass ، ثم أكتب الرقم  
السري مثل pass xxxx ثم Enter .
- إذا كان إدخالك صحيح ستشاهد

```
D:\WINNT\System32\telnet.exe
+OK hello from popgate
+OK password required.
+OK maildrop ready, 4 messages
```

كلمة Ok بعد ما تضغط Enter . كما في الشكل :

سيتم إدخالك إلى الحساب .

لمشاهدة جميع الرسائل وأحجامها اكتب List ثم Enter .

ستشاهد ترتيب الرسائل تحت بعض ، وأمام كل رقم رقم ثاني يدل على حجم الرسالة . كما في الشكل :

- لحذف رسالة من القائمة أكتب delete ثم رقم رسالة الهدف .

```
D:\WINNT\System32\telnet.exe
+OK maildrop ready, 4 messages <181
+OK 4 messages <181436 octets>
1 3866
2 10508
3 72101
4 94961
.
```

تنفع هذه الطريقة مع بريد pop .

طريقة سحب البريد عن طريق التلنت من الدكتور الفنتوخ .

### بعض الأوامر المستخدمة مع التلنت :

وصل عميل التلنت مع جهاز بعيد :

بناء الجملة :

open [\\RemoteServer] [Port]

المعلومات :

\\RemoteServer

تحديد اسم الملقم الذي تريد إدارته . إن لم تحدد ملقماً ما ، سيتم افتراض الملقم المحلي .

Port

تحديد المنفذ الذي تريد استخدامه . إن لم تحدد منفذاً ما ، سيتم افتراض المنفذ الافتراضي .

ملاحظات :

• يمكنك اختصار هذا الأمر إلى 0

أمثلة :

للاتصال بملقم بعيد Redmond من خلال رقم المنفذ 44 أكتب :

o Redmond 44

لقطع اتصال عميل Telnet من كمبيوتر بعيد

:

بناء الجملة :

close [\\RemoteServer]

المعلومات :

\\RemoteServer

تحديد اسم الملقم الذي تريد إدارته . إن لم تحدد ملقماً ما ، سيتم افتراض الملقم المحلي .

ملاحظات :

• يمكنك اختصار هذا الأمر إلى c

أمثلة :

لقطع الاتصال من ملقم بعيد Redmond أكتب

:

c Redmond 44

: بناء الجملة

send [\\RemoteServer] [ao] [ayt] [esc] [ip] [synch] [?]

: المعلومات

\\RemoteServer

تحديد اسم الملقم الذي تريد إدارته .  
إن لم تحدد ملقماً ما ، سيتم افتراض الملقم المحلي .

ao

إحباط أمر الإخراج .

ayt

إرسال أمر "Are you there" ؟ .

esc

إرسال حرف الهروب الحالي .

ip

مقاطعة أمر العملية .

synch

أداء عملية تزامن Telnet .

: بناء الجملة

display

: المعلومات

. بلا

: ملاحظات

- يسرد الأمر display معلومات التشغيل الحالية لعميل Telnet ، إذا كنت في جلسة عمل Telnet ( بعبارة أخرى ، إذا كنت متصلاً بملقم Telnet ) ، يمكنك الخروج من جلسة عمل Telnet لتعديل المعلومات بضغط +CTRL . للعودة إلى جلسة عمل Telnet ، اضغط ENTER .

إدارة ملقم التلنت المحلي بالـ tlntadmn

: بناء الجملة

tlntadmn [\\RemoteServer] [start] [stop] [pause] [continue]

: المعلومات

\\RemoteServer

تحديد اسم الملقم الذي تريد إدارته .  
إن لم تحدد ملقماً ما ، سيتم افتراض الملقم المحلي .

start

بدء تشغيل ملقم Telnet .

stop

إيقاف تشغيل ملقم Telnet .

pause

مقاطعة ملقم Telnet .

continue

استئناف ملقم Telnet .

: ملاحظات

- يمكنك إدارة كمبيوتر عن بعد يشغل ملقم Telnet باستخدام الأوامر tlntadmn إذا كان كلا من جهازي الكمبيوتر يشغلان نفس نظام التشغيل فإذا المطلوب ويندوز 2000 استخدمه بي ويندوز 2000. لا يمكنك استخدام الأوامر tlntadmn لإدارة كمبيوتر عن بعد يشغل Windows 2000 وملقم Telnet من كمبيوتر يشغل Windows XP مثلاً .

: بناء الجملة

tlntadmn [\\RemoteServer] config [maxconn=PositiveInteger]

: المعلومات

\\RemoteServer

تحديد اسم الملقم الذي تريد إدارته .  
إن لم تحدد ملقماً ما ، سيتم افتراض الملقم المحلي .

maxconn=PositiveInteger

تعيين العدد الأعظمي للاتصالات . يجب عليك  
تحديد هذا العدد بواسطة عدد صحيح موجب  
أصغر من 10 ملايين .

بناء الجملة :

tlntadmn [\\RemoteServer] config [maxfail=PositiveInteger]

المعلومات :

\\RemoteServer

تحديد اسم الملقم الذي تريد إدارته .  
إن لم تحدد ملقماً ما ، سيتم افتراض الملقم  
المحلي .

maxfail=PositiveInteger

تعيين الحد الأقصى لمحاولات تسجيل الدخول  
الفاشلة المسموح بها للمستخدم . يجب عليك  
تحديد هذا العدد بواسطة عدد صحيح موجب  
أصغر من 100 .

بناء الجملة :

tlntadmn [\\RemoteServer] config [timeout=hh:mm:ss]

المعلومات :

\\RemoteServer

تحديد اسم الملقم الذي تريد إدارته .  
إن لم تحدد ملقماً ما ، سيتم افتراض الملقم  
المحلي .

timeout=hh:mm:ss

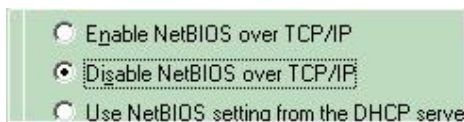
تعيين فترة المهلة بالساعات ، والدقائق  
، والثواني .  
دائماً يستخدم الـ /? لعرض التعليمات في  
موجه الأوامر .

## نت بويس ( NET BIOS )

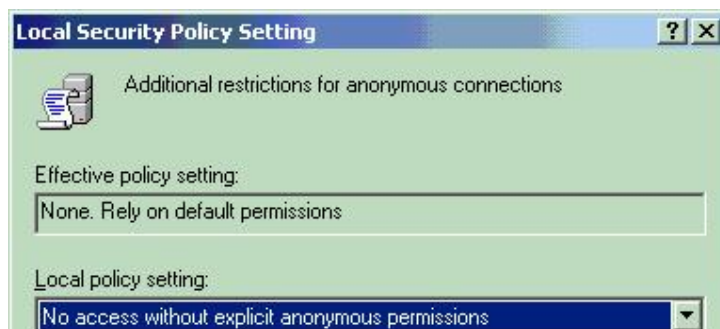
- صد الجلسات الخالية .
- منع تعداد المستخدمين .
- منع تعداد الـ SNMP .

يوجد في الإعداد الافتراضي للويندوز اعتماد على NetBIOS وهي مشكلة كبيرة لأصحاب الشبكات المهمة لأن الـ NetBIOS لها واجهات تداخل API تعيد ، وترجع معلومات حول الهدف من خلال المنفذ 139 لـ TCP ، وفي الحالة الافتراضية يكون الوصول ممكن حتى من مجهولين الهوية ، وطبعاً هذا يكون فيه خطراً قد يكون كبير عند استخدامه من محترفين الولوج على أنظمة NT.

تستطيع أن تلغي كل خدمات NetBIOS على جهاز ما عندما تجد أنها غير ضرورية لك ، ويكون ذلك من خصائص TCP/IP ، ثم من Advanced ، ثم من التبويب WINS ، ثم تعلم على الخيار الواضح في المثال التالي :



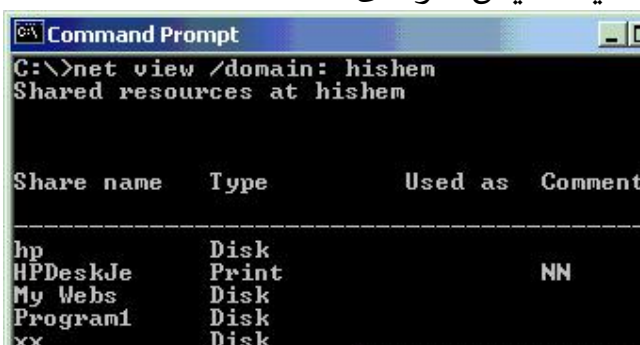
وإذا كانت هذه الخدمة مهمة لك فقد قدمت شركة مايكروسوفت حلاً مناسباً وهي تدعى Restrict Anonymous وهي تحد بشكل كبير من تسرب المعلومات عبر الوصلات المجهولة ، وتستطيع الوصول إليها من Administrative Tools ثم من Local Security policy ثم من النافذة نختار Local policies ثم من security options ثم نعلم على الخيار الأول Additional restrictions for anonymous connections ثم بالزر الأيمن نختار security ثم من النافذة نختار من الشريط المنزلق الخيار No Access Without Explicit Anonymous Permissions مثل المثال التالي :



### بعض الأمثلة لاستخدام أدوات الـ NetBIOS

#### Net View ■

هذه الأداة مضمنة ضمن نظام التشغيل نفسه وهي أداة سطر أوامر على NT/W2000 وهي تعرض الميادين المتاحة وكل الأجهزة على هذه الميادين وكل الخدمات المتاحة لتشارك على



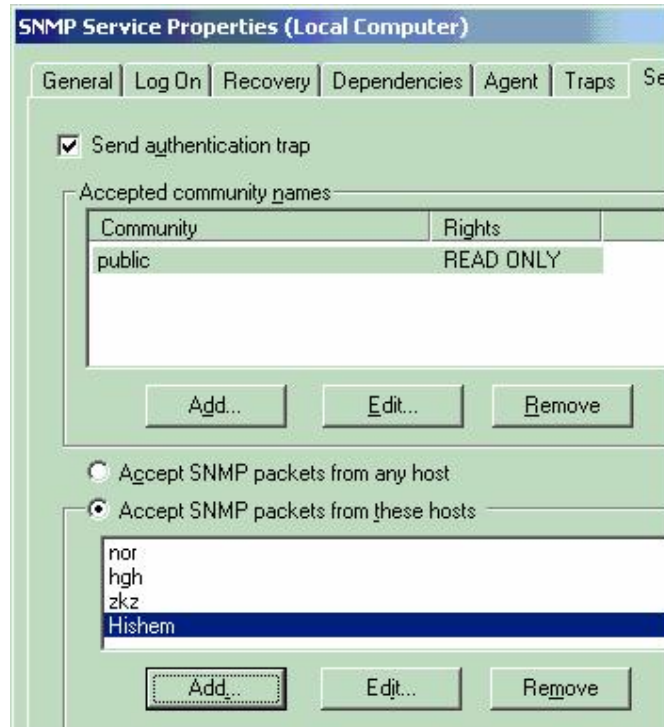
الأجهزة ، ويكفي أن تكتب عنوان IP أو اسم الدومين حتى تكون قد حصلت على ما تريد . وتوجد أدوات رسومية شعبية كثيرة على الإنترنت للقيام بنفس العمل منها على سبيل المثال البرنامج Legion .

#### ■ الحل المريح :

الحل المريح لتخلص من هذا الصداع هو حماية المنافذ المقدمة من البروتوكول TCP والبروتوكول UDP عبر المنافذ من 135 إلى المنفذ 139 + 445 ، وكل برامج الجدران النارية المتقدمة تستطيع من خلالها أن تتحكم بالمنافذ بشكل مريح ، وشاهدنا كيف نلغي الخدمة NetBIOS أو نقلل من المشاكل المحتملة منها ، ورغم كل ذلك لإزالة الخطر



موجوداً إذا كنت تستخدم البروتوكول SNMP لإدارة الشبكة على ويندوز 2000 سيرفر ، فهذا البروتوكول يمرر كل المعلومات المطلوبة إذا كان مثبتاً ، ولتأمين هذا البروتوكول بالشكل المطلوب أمامك خيارين ، الأول : حذف اسم المجموعة Public التي تكون عند التثبيت الافتراضي وتكون أسماء مخصصة من مستخدمي الشبكة كما في المثال المجموعة public موجودة علم عليها ثم من الزر Remove ثم حرر المربع Send authentication trap .



بذلك تكون قد حصرت استخدام هذا البروتوكول للأشخاص المختارين فقط .  
والحل الثاني من محرر السجل regedit  
HKEY\_LOCAL\_MACHINE\system\currentControlset\services  
\SNMP\parameters\ExtensionAgent  
ثم قم بحذف المفتاح LANManagerMIB2Agent ثم قم  
بإعادة ترقيم المدخلات مثلاً إذا كان ما

حذفته رقمه = واحد أعد الترقيم ليبدأ من  
واحد للمدخل رقم 2 .

البروتوكول TCP/IP يستطيع العمل بشكل سليم بدون خدمات الـ NetBIOS ، لذلك إذا كنت غير محتاج إليه تعطيله أفضل .	هل تعلم أن
---	------------

## دي إتش سي بي ( DHCP )

- فهم وظيفة البروتوكول DHCP .
- تثبيت البروتوكول بشكل صحيح .
- استخدامه بشكل عملي .

### DHCP Dynamic Host Configuration Protocol

وهو يقدم عناوين IP بطريقة أوتوماتيكية لجميع مستخدمي الشبكة وهو تقديم و إعداد تلقائي لبروتوكول TCP/IP ويتمكن مخدم DHCP من العمل بعد إدخال عناوين IP في المجال Scope هذا المجال هو حدود الأرقام تبدأ من كذا وتنتهي إلى كذا مثلاً نحدد هذا الـ Scope من 200.150.40.1 إلى 200.150.40.50 ذلك يعني أن لدينا 50 رقم IP متاح في الشبكة ولنتمكن زبون DHCP من أخذ الرقم من المخدم نفعل في جهاز الزبون الخيار Enable Automatic DHCP Configuration .

ومن فوائد الـ DHCP :

- 1 - لا يسمح بوجود عنوانين من أرقام IP متشابه .
- 2 - لن تكون مضطراً لإدخال القيم يدوياً .
- 3 - تقلص مشاكل البروتوكول TCP/IP بشكل كبير .
- 4 - تأجير عنوان IP لمدة محددة من قبل مدير النظام وهذه الميزة مفيدة عندما تكون عدد الحواسيب أكبر من عدد أرقام الـ IP المتاحة على مخدم DHCP .
- 5 - إذا تم نقل جهاز على شبكة فرعية ثانية سيأخذ إعداداته من مخدم DHCP فوراً .

\* تثبيت الخدمة DHCP :

The first step in implementing DHCP is to install the DHCP service. Before you install the DHCP service, you should specify a static Internet Protocol (IP) address, subnet mask, and default gateway address for the network adapter bound to Transmission Control Protocol/Internet Protocol (TCP/IP) in the computer designated as the DHCP server .

- الخطوة الأولى هي تثبيت الخدمة DHCP :  
ونحتاج قبل التثبيت أن نحدد بعض المتطلبات وهي :  
- عنوان IP ساكن .  
- قناع الشبكة الفرعية .  
\* تثبيت الخدمة والبروتوكول TCP/IP :

\*\* خطوات التثبيت :

1. Click Start, point to Settings, open Control Panel, open Add/Remove Programs, then click Add/Remove Windows Components. Click the Components button.
2. In the Windows Components Wizard dialog box, select Networking Services, then click Details.
3. In the Networking Services dialog box, in the Subcomponents Of Networking Services list, click to place a check mark in the box to the left of Dynamic Host Configuration Protocol (DHCP), then click OK وضع علامة أمام Dynamic Host Configuration Protocol DHCP .
4. Click Next to install the required components.
5. Insert the Windows 2000 Server CD-ROM when prompted. أدخل القرص المضغوط للويندوز.
6. On the Completing The Windows Components Wizard page, click Finish.
7. Close the Add/Remove Programs dialog box.
8. Close Control Panel and remove the Windows 2000 Server CD-ROM from the drive.

ملاحظة :

The DHCP service starts automatically during installation and must be running to communicate with DHCP clients.

## Configuring the DHCP Service.

The basic tasks for configuring the DHCP service are creating a DHCP scope, configuring a DHCP scope, and configuring a client reservation.

### إنشاء وتكوين المدى :

Before a DHCP server can lease an address to DHCP clients, you must create a scope. A scope is a pool of valid IP addresses available for lease to DHCP clients. After you have installed the DHCP service and it is running, the next step is to create a scope.

بعد تثبيت الخدمة DHCP عليك بوضع مدى و المدى هو المجال الذي يكون منه عناوين الـ IP التي سوف توزع على مستضافي DHCP سيرفر . وعند الإنشاء يجب الأخذ بعين الاعتبار النقاط التالية :

You must create at least one scope for every DHCP server. ■

يجب أن يكون هناك مدى واحد على الأقل لكل ملقم DHCP .

You must exclude static IP addresses from the scope. ■

أن تخرج عناوين الـ IP الساكنة من المدى .

You can create multiple scopes on a DHCP server to ■ centralize administration and to assign IP addresses specific to a subnet. You can assign only one scope to a specific subnet. إنشاء عدة أمديه متعددة على ملقم واحد ويمكن أن يكون واحد .

DHCP servers do not share scope information. As a result, ■ when you create scopes on multiple DHCP servers, ensure that the same IP addresses do not exist in more than one scope to prevent duplicate IP addressing. DHCP معلومات المدى ويجب التأكد عند إنشاء عدة أمديه على عدة ملقمات أنه لا يوجد بها أرقام IP متشابهة .

### ■ لإنشاء مدى DHCP :

1. Click Start, point to Programs, point to Administrative Tools, then click DHCP.

2. In the DHCP console, right-click the entry for the DHCP server, then click New Scope to start the New Scope Wizard.  
داخل النافذة انقر بالزر الأيمن على الطرفية DHCP واختر منها New Scope.

3. On the Welcome To The New Scope Wizard page, click Next.

4. On the Scope Name page, specify a name for the scope in the Name box. You can also specify a description for the scope in the Description box. Click Next.  
لو أحببت .

5. On the IP Address Range page, specify the range of IP addresses included in the scope. You can also specify the subnet mask by length or as an IP address. Click Next.

الصفحة حدد مدى عناوين الـ IP والنطاق التي تكون فيه مثل المثال التالي :

بداية الأرقام هي 131.107.2.200 ونهاية الأرقام هي 131.107.2.250 . ويكون عندك في هذه الحالة 50 رقم IP متاح في هذا المدى ويجب كذلك تحديد قناع الشبكة وكما في المثال السابق هو 255.255.255.0 .

6. On the Add Exclusions page, specify any addresses to be excluded from the scope, then click Next.  
حدد أي عنوان من المدى تريد أن تستبعده من العرض .  
ملاحظة :

---

Exclusion is an address or range of addresses that the server should not distribute. You can exclude multiple ranges of addresses.

---

7. On the Lease Duration page, specify how long a client can use an IP address from this scope as issued by the DHCP server, then click Next.  
يستطيع المستخدم استعمال الرقم فيها .

8. On the Configure DHCP Options page, specify if you want to configure common DHCP options now or later, then click Next. على هذه الصفحة حدد هل تريد تحديد التكوين العام لخيارات DHCP الآن أو لاحقاً .

9. If you specified that you want to configure common DHCP options later, skip to Step 12. إذا أردت تحديد التكوين العام لاحقاً تجاوز إلى الفقرة 12 .

10. If you specified that you want to configure common DHCP options now, and if you did not specify later, skip to Step 12. إذا أردت التكوين الآن قم بالخطوات التالية :

• On the Router (Default Gateway) page, specify the routers, or default gateways, to be distributed by this scope, then click Next. في هذه الصفحة حدد الموجهات والبوابات التي ستستخدم هذا المدى .

• On the Domain Name And DNS Servers page, specify the parent domain name you want client computers to use for Domain Name System (DNS) name resolution. If you want to configure scope clients to use DNS servers on your network, enter the server name and IP addresses for those servers. Click Next. الميدان الأب الذي تريد أن تستخدمه الأجهزة المستضافة من أجل اسم DNS ، وإذا أردت أن يستخدم مستضافي المدى ملقمات DNS على الشبكة أدخل اسم الملقم ورقم الـ IP لهذا الملقم .

• On the WINS Servers page, specify the server name and IP address to enable clients to query Windows Internet Name Service (WINS) before they use broadcasts to register and resolve NetBIOS names, then click Next. في هذه الصفحة حدد اسم الملقم ورقم الـ IP لتأهيل المستضافين من أجل خدمة اسم الإنترنت WINS .

11. On the Activate Scope page, specify if you want to activate the scope now or later, then click Next. إذا كنت تريد تنشيط المدى الآن أو لاحقاً .

12. On the Completing The New Scope Wizard page, click Finish.

■ حجز عنوان IP خاص لأحد المستضافين بشكل دائم :

1. In the DHCP console, open the scope entry, right-click DHCP Reservations, then click New Reservation.  
افتح المدى ثم بالزر الأيمن على Reservations ثم اختر New Reservation .

2. In the New Reservation dialog box, in the Reservation Name box, type a name to identify the client. The DHCP console uses a name associated with the hardware address of the network adapter card to identify a client.

3. In the IP Address box, type the IP address that you want to reserve for a specific client.  
الذي تريد حجزه من المدى .

4. In the MAC Address box, type the hardware address (media access control address) of the host's network adapter card. Do not use dashes in the hardware address.  
وهي كتابة رقم كرت الشبكة للجهاز الذي تريد أن تعين رقم الـ IP له .  
وعند كتابة الرقم يجب أن يكون من دون فراغات .

ملاحظة :

If you type the value for the MAC Address incorrectly, it will not match the value sent by the DHCP client, and the DHCP service will assign the client any available IP address instead of the IP address reserved for that client.  
كرت الشبكة بشكل خاطئ لن يتم إسناد الرقم المحجوز له ، ولكن سيعطى أي رقم من المدى متوفر .

5. In the Description box, type an optional description for the client.  
أكتب وصف إذا أحببت .



6. Under Supported Types, click to specify which method the client uses:  
سيستخدمها المستضاف .  
Both. Specifies that either DHCP or BOOTP clients are •  
allowed for this client reservation.  
DHCP Only. Specifies that only DHCP clients are allowed •  
for this client reservation.  
BOOTP Only. Specifies that only BOOTP clients are •  
allowed for this client reservation.  
• To add the reservation to the database, click Add. وفي  
الختام انقر Add لإضافة الحجز إلى قاعدة  
البيانات .

## دي إن إس ( DNS )

### - نظام أسماء الميادين DNS :

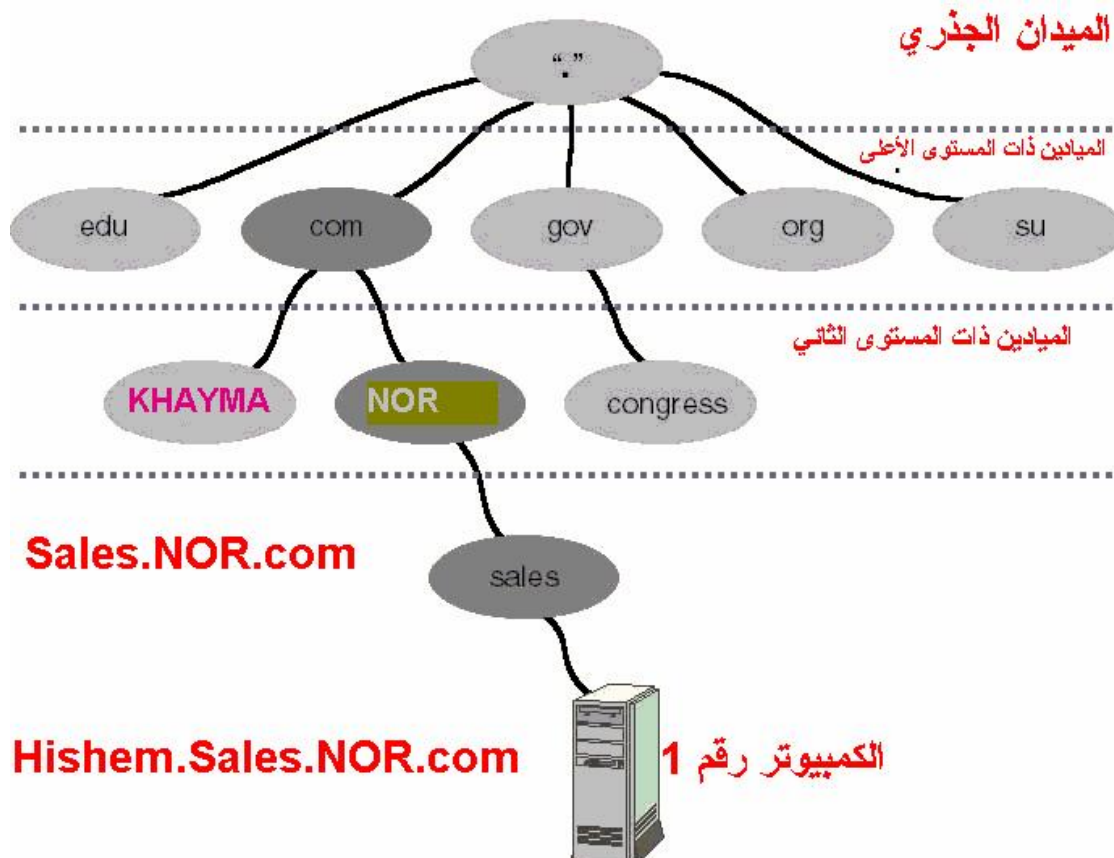
نظام أسماء الميادين DNS : هو قاعدة بيانات مستعملة في شبكات TCP/IP لترجمة أسماء المضيفين إلى عناوين IP .  
والـ DNS مقترن بالإنترنت أكثر من أي شيء ثاني . والشبكات الخصوصية تستعمل DNS بشكل كبير وذلك لترجمة أسماء مضيفي الكمبيوتر وإيجادها ضمن الشبكة المحلية .  
ومن الفوائد من استخدام DNS الأمور التالية :

- أسماء مضيفي ودودة للمستخدم وهي أسهل للتذكر من أرقام IP .
- اسم المضيف يبقى ثابت والعنوان الخاص بي IP يمكن أن يتغير .
- أسماء المضيفين تتيح للمستخدم الاتصال بالملقمات المحلية باستعمال نفس التسمية المستخدم في الإنترنت .

### - مخزن الأسماء :

مخزن أسماء الميادين : هو نظام التسمية الذي يزود البنية الهرمية لقاعدة بيانات DNS . وكل عقدة في قاعدة بيانات DNS تكون ميدان .  
وتكون قاعدة البيانات مفهرسة حسب الاسم ، لذلك يجب أن يملك كل ميدان اسماً فريداً ضمن الميدان الأب . كما في الشكل التالي :

يسمى الميدان الذي يلتحق بميدان أكبر



يسمى ميدان فرعي ويلتحق به بالاسم علاقة الأب بالطفل ، فيكون بداية الاسم بالميدان الأصغر ، ثم الأب الأكبر ، ثم الجد . مثل ما في المثال السابق يكون الميدان NOR ابن للميدان COM والميدان Sales ابن للميدان NOR ويكون كل ابن ميدان فرعي مع ميدان الأب .

### - الميدان الجذري :

الميدان الجذري : هو النقطة العليا في الهرم وتمثله النقطة " . " ، وتدير هذا الميدان عدة شركات من بينها شركة InterNIC .

### - الميادين ذات المستوى الأعلى :

الميادين ذات المستوى الأعلى : هي الشفرات التي تصنف الأسماء حسب نوع المؤسسة أو المكان الجغرافي . وفي الجدول التالي بعض الأمثلة عن الأسماء ذات المستوى الأعلى :

وصفها	الميادين ذات المستوى الأعلى
المؤسسات الحكومية	Gov
الشبكات	Net
المؤسسات التجارية	Com
المؤسسات التربوية	Edu
المنظمات العسكرية	Mil
المؤسسات غير التجارية	Org
رمز لأستراليا	Au
رمز للمملكة العربية السعودية	Sa

الميادين ذات المستوى الأعلى يمكن أن تحتوي على ميادين ذات مستوى ثاني وأسماء مضيفين .

### - الميادين ذات المستوى الثاني :

الميادين ذات المستوى الثاني : يمكن أن تحتوي على مضيفين وميادين فرعية مثلاً . كما شاهدنا في المثال يمكن أن يحتوي الميدان NOR.com على مضيف كـ Sales ، ويمكن للميدان Sales أن يحتوي على مضيف كـ Hishem .

### أسماء المضيفين :

تكون أسماء المضيفين إشارة إلى كمبيوترات موجودة على الإنترنت ، أو في شبكة خصوصية وتكون أسماء المضيفين دائماً في أقصى اليسار ضمن الاسم . وكما في المثال السابق يكون عنوان المضيف Hishem.Ktaly Hishem.Sales.NOR.com ، ويكون بذلك اسم مؤهل بالكامل FQDN .

### حول التسمية :

قبل أن تنشئ قاعدة لأسماء الـ DNS تنبه للأمور التالية :

- قلل من عدد المستويات وتكون مجرد ثلاث أو أربع مستويات .
- استعمل أسماء فريدة لكل ميدان .
- اختر أسماء سهلة التذكر وبسيطة وذلك لسهولة البحث عنها في الإنترنت ، أو الشبكة الخصوصية .
- تجنب الأسماء الطويلة ؛ لأن كامل الاسم FQDN لا يمكن أن يتجاوز الـ 255 حرفاً .

### تثبيت وتكوين الـ ( DNS ) :

تثبيت الـ DNS :

عند تثبيت الويندوز 2000 لا يتم تثبيت الـ DNS معه ، وتحتاج إلى الخطوات التالية حتى تثبته على شبكتك ، ولكن من المهم قبل التثبيت التأكد من تكوين بروتوكول TCP/IP صحيح للقم DNS ويجب كذلك أن يتوفر له عنوان ساكن ولا يكون يأخذه من مخدم DHCP ... \* خطوات التثبيت :

- ☐ في لوحة التحكم انقر على Add/Remove Programs .
- ☐ ثم انقر على Add/Remove Windows Components .
- ☐ حدد Networking Services ثم انقر Details .

□ تشاهد في النافذة خيارات Networking

. Services

بجانب DNS علم على خانة الاختيار ثم انقر

OK انقر Next .

يتم تثبيت الخدمة وعند الانتهاء انقر

على Finish .

ملاحظة : عند تثبيت الدليل النشط Active Directory يتم تثبيت الـ DNS إجباري ، ولن تكون في هذه الحالة محتاج للخطوات السابقة .

وعند الانتهاء من التثبيت تجد اختصار

للـ DNS في قائمة Administrative Tools ، ويتم

كذلك إنشاء مجلد في المسار التالي :

. System32\DNS%\%systemroot

\* ضبط وتأهيل الخدمة DNS :

في التثبيت الافتراضي للخدمة لا يتم

إنشاء مناطق تفتيش عن الأسماء لذلك تحتاج

لضبط التكوين للخدمة حتى يكون بمقدورك

استخدامها على شبكتك .

والمنطقة المطلوبة هي منطقة التفتيش إلى

الأمام forward lookup zone ، وتحتاج إلى واحدة

على الأقل حتى تعمل الخدمة ( التفتيش إلى

الأمام هي تفتيش العميل عن اسم إنترنت مثل

[www.nor2000.com](http://www.nor2000.com) ملقم DNS يبحث عن مقابل لهذا

الاسم بعنوان IP في قاعدة بياناته ) ، ،

وتوجد منطقة أخرى وتسمى منطقة تفتيش

عكسي Reverse Lookup Zones . وهي عبارة عن

تفتيش بعنوان IP عن اسم إنترنت وهي ليست

مطلوبة لعمل الـ DNS ، ولكنها مطلوبة

عندما تريد تسجيل اسم بدلا عن عنوان IP في

سجلات IIS Microsoft Internet Information Services .

### \* إنشاء منطقة تفتيش إلى الأمام :

إذا كنت قد ثبت الدليل النشط على الويندوز 2000 ستجد أن الويندوز قد قام بتثبيت الدنس ، وقام كذلك بإنشاء منطقة تفتيش إلى الأمام باستخدام اسم الميدان الذي اخترته عند تثبيت الدليل النشط .

\* \* انقر Start .

\* \* ثم Programs .

\* \* ثم Administrative Tools .

\* \* اختر DNS .

\* \* علم على ملقمك ثم من القائمة Action .

\* \* ثم اختر Configure The Server ( هذا الخيار يظهر في التثبيت الأول للخدمة بعد ذلك يمكنك استخدام الخيار New Zone ) .

\* \* يظهر معالج المنطقة انقر على NEXT .

\* \* أترك الخيار كما هو Standard Primary ثم

NEXT .

أيضاً أترك الخيار الافتراضي Forward Lookup كما هو .

الآن شاشة الاسم أكتب اسم الميدان الذي تريد مثل NOR2000.COM ثم انقر Next .

أترك الخيار Create A New File With This File Name

كما هو وتأكد أن اسم الملف هو nor2000.com.dns

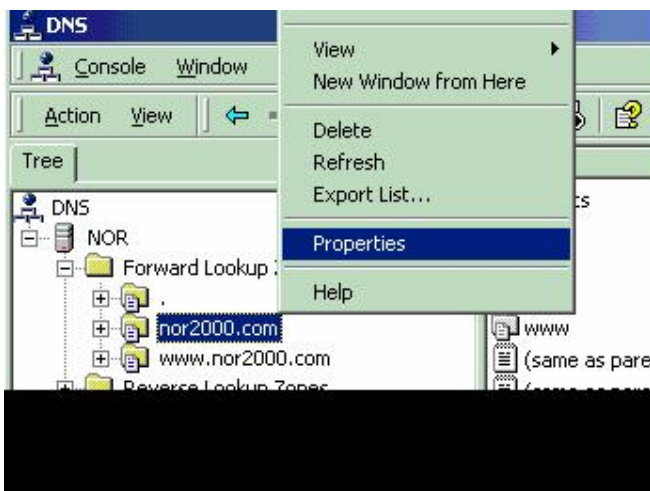
انقر Next .

راجع معلوماتك في هذه الشاشة تستطيع الرجوع إذا أردت ، أو انقر على Finish .

### \* مزيد من التكوين :

- حدد الحاوية Reverse Lookup Zones .
  - ثم من القائمة Action .
  - اختر New Zone .
  - أنقر Next .
  - أترك الخيار كما هو ثم Next .
- من هذه الشاشة أمام Network ID أكتب عنوان شبكتك مثلا عندي عنوان خادم DNS هو 192.168.0.1 مع قناع شبكة 255.255.255.0 ، سأكتب في هذه الخانة الرقم 192.168.0 ، ستجد في اسفل النافذة خيار Reverse Lookup Zone Name ، عندما تكتب عنوان الشبكة يصبح يحتوي على العنوان التالي : 0.168.192.in-addr.arpa .
- تأكد من اسم الملف وأن الخيار Create A New File With This File Name معلم عليه
- راجع المعلومات ثم انقر Finish .
- ### كيف تضبط التحديث ؟
- التحديث يسمى DNS Dynamic وضبطه بسيط من على اسم الميدان الذي أنشأت ، وكذلك من على الحاوية x.Subnet تضغط بالزر الأيمن .
- ثم من أمام الخيار Dynamic Updates drop-down في القائمة المنسدلة اختر yes .
- ثم OK .
- بذلك تكون قد ضبطت التحديث الديناميكي لمنطقة التفتيش إلى الأمام ، ومنطقة التفتيش العكسي وهذا مثال حي عن ذلك :





### \*تشخيص المشاكل :

تستخدم في تشخيص الخدمة DNS الأداة nslookup ، وهي أداة سطر أوامر بسيطة وهي تثبت مع تثبيت البروتوكول TCP/IP .

### \*لاستخدام الأداة :

في موجة الأوامر أكتب nslookup ثم إنتر Enter

إذا كان تكوين الـ DNS سليم ستظهر لك اسم خادم الأسماء وعنوانه ، ثم بعد ذلك أكتب set all ثم إنتر سيظهر لك كل القيم الحالية للخدمة DNS .

```
D:\>nslookup
Default Server:  nor.nor2000.com
Address:  192.168.0.1

> set all
Default Server:  nor.nor2000.com
Address:  192.168.0.1

Set options:
nodebug
defname
search
recurse
nod2
novc
noignoretc
port=53
type=A
class=IN
timeout=2
retry=1
root=A.ROOT-SERVERS.NET.
domain=nor2000.com
MSxfr
IXFRversion=1
srchlist=nor2000.com
```

### عمل الـ DNS :

المحطات الموجودة على الشبكة التي تم ضبط البروتوكول TCP/IP عليها سيكون بمقدورها استعمال خدمة DNS .

افتح خصائص البروتوكول TCP/IP وفي اسفل الشاشة علم على الخيار Use the following DNS server addresses ، ثم أكتب عنوان ip الخاص بخادم الـ DNS ومن زر Advanced يمكنك التحكم بشكل أوسع .

### \* بروتوكولات الويندوز :

#### عمل الـ DNS :

المحطات الموجودة على الشبكة التي تم ضبط البروتوكول TCP/IP عليها سيكون بمقدورها استعمال خدمة DNS .

افتح خصائص البروتوكول TCP/IP ، وفي اسفل الشاشة علم على الخيار Use the following DNS server addresses ، ثم أكتب عنوان ip الخاص بخادم الـ DNS ، ومن زر Advanced يمكنك التحكم بشكل أوسع .

### \* البروتوكول ATM :

البروتوكول ATM هو اختصار Asynchronous Transfer Mode ، وهو للإرسال غير المتزامن يكون مثالي لنقل الصوت والفيديو ، وينتقل هذا البروتوكول في خلايا بطول ثابت وبسرعة عالية ، ويدعم الويندوز 2000 الـ ATM بطريقتين وهي :

LAN Emulation  
Winsock

ويستخدم هذا البروتوكول اتصال المنحى ويقوم بإنشاء مسار وهمي بين المرسل والمستقبل ويمرر البيانات عبر هذا المسار بسرعة متساوية وترتيب ملائم .

NWLink

هو النسخة المكررة من مايكروسوفت للبروتوكول IPX/SPX التابع لـ NetWare ، وهو مطلب مهم للشبكات المخططة بين الويندوز والنتوير ، وفي الويندوز سيرفر يجب استخدام الـ Gateway Service for NetWare حتى يتمكن عملاء النتوير من المشاركة في الملفات والطباعة ، وفي الويندوز Professional يجب استخدام الـ Client Service for NetWare ، وعند المشاركة مع النتوير يجب تحديد ما يسمى نوع اللوح ، وهو التنسيق الذي يكون عليه كرت الشبكة ، ويجب أن يكون النوع واحد في ملقم الويندوز وعملاء النتوير ، أو العكس ومن الأنواع التي يدعمها البروتوكول NWLink ما يلي : -

الإيثرنت	Ethernet II و 802.2 و 802.3
توكن رينغ	802.5 و SNAP

وعند تحميل البروتوكول يتم التعرف على نوع اللوح بشكل تلقائي ، ويمكن تعديله يدوي ، والويندوز 2000 يدعم عدد من الأنواع في الوقت نفسه .

البروتوكول NetBEUI :

هو البروتوكول المناسب للشبكات الصغيرة التي تكون إلى حد 200 جهاز ، وهو بروتوكول غير قابل للتوجيه ، ولا يمكن استخدام الموجهات معه ويستطيع التعامل مع الجسور ، وله عدد من المواصفات الجيدة التي تجعله مرغوبا ومستعملا وهي :

- خالي من الاتصالات واتصالي المنحى سريع .
- حماية من الأخطاء .
- عبء على الذاكرة بسيط .
- تكوين ذاتي .

في الشبكات التي تشغل الخدمات Active Directory لا يمكنها أن تستخدم هذا البروتوكول كبروتوكول رئيسي

: AppleTalk

هو مجموعة من البروتوكولات المستخدمة في أجهزة الماكنتوش ، وحتى يتمكن ملقم الويندوز من تقديم خدمات الطباعة ، والمشاركة في الملفات مع عملاء ماكنتوش يجب ضبط الملقم بـ Windows 2000 Services for Macintosh .

: DLC

هو من تطوير شركة IBM للمشاركة بين الأجهزة الإيوانية ، ويستخدم في الويندوز من أجل طابعات هيولت باكارد القديمة ، والتي لا تدعم البروتوكول TCP/IP ، وعند الرغبة في استخدام هذه الطابعات يثبت هذا البروتوكول على ملقم الطباعة فقط .

: IrDA

هي مجموعة من البروتوكولات التي تعمل بالأشعة تحت الحمراء ، وهو من البروتوكولات اللاسلكية مرتفعة السرعة ثنائية الاتجاه وتستخدم في الاتصال بين الأجهزة ، مثل الكاميرات والأجهزة النقالة والطابعات .

## المراجع

- 1 ( <http://www.nor2000.com> .
- 2 ( <http://www.shabakah.net> .
- 3 ( دراسة معدة عن شبكة الحاسب الآلي بالجمعية الخيرية لتحفيظ القرآن الكريم بالمدينة المنورة - إعداد : علي برناوي - نذير أحمد حافظ - منير أحمد حافظ .
- 4 ( شبكات نوفيل ، طبعة 1414 هـ .
- 5 ( <http://www.bahoori.net/vb> .
- 6 ( دراسة معدة عن شبكة الحاسب الآلي في بلدية العقيق - إعداد : علي برناوي .
- 7 ( <http://www.net4top.net/vb> .