الفصل الخامس

إعداد البروتوكول TCP/IP

Setup of TCP/IP Protocol

بينَّا في الفصلين السابقين كيفية إعداد نظام تشغيل الشبكة، وسنتناول في هذا الفصل كيفية إعداد البروتوكول TCP/IP لأنه أهم جزء في نظام التشغيل

التعريف بالبروتوكول TCP/IP :

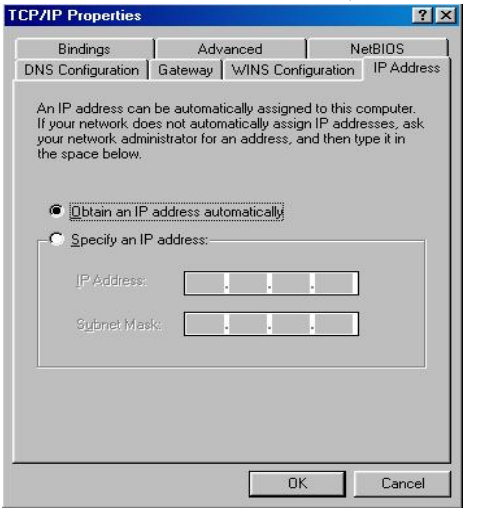
هذا البروتوكول (كما ذكرنا من قبل) ليس بروتوكولاً واحدًا، ولكنه مزيج من (2 بروتوكول). أحدهما هو الـ TCP (Transmission Control Protocol) ويمثل طبقة الـ Transport Layer، والثاني هو بروتوكول IP (Internet Protocol) ويمثل طبقة Internet Layer، ولذا فهو أسرع في الاتصال من البروتوكولات التي تستخدم النموذج OSI-7 Layers مثل البروتوكول Netbui وذكرنا أن هذا البروتوكول تم استحداثه مع ظهور الإنترنت للحاجة الملحة إلى السرعة مع تطور عالم الشبكات وكثرة عدد الأجهزة.

عرض خصائص البروتوكول TCP/IP في Windows98 :

☜ قم بعرض مكونات نظام تشغيل الشبكة، من خلال النقر بالزر الأيمن للماوس على أيقونة Network Neighborhood، واختر Properties من القائمة المنسدلة، أو من خلال النقر المزدوج على أيقونة Network داخل لوحة التحكم، فيتم عرض مكونات نظام تشغيل الشبكة (انظر شكل 6 في الفصل الثالث)

☜ قم بالنقر على البروتوكول TCP/IP، ثم اضغط على زر Properties.

☜ تظهر خصائص البروتوكول (كما في شكل 1).

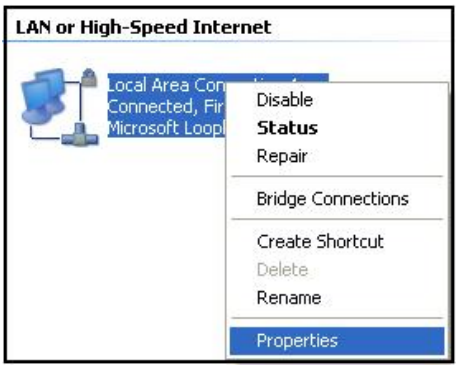


شكل رقم (1)

عرض خصائص البروتوكول TCP/IP في WindowsXP :

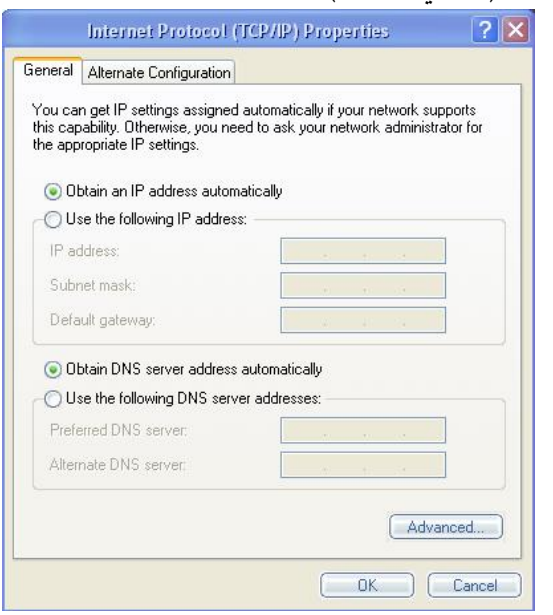
☜ قم بالنقر بالزر الأيمن للماوس على أيقونة My Network Places، ثم اختر Properties من القائمة المنسدلة.

☜ انقر بالزر الأيمن للماوس على أيقونة الشبكة الداخلية، واختر Properties من القائمة المنسدلة (كما في شكل 2)، يتم عرض مكونات نظام تشغيل الشبكة (انظر شكل 17 في الفصل الرابع).



شكل رقم (2)

☜ قم بالنقر على البروتوكول TCP/IP، ثم اضغط على زر Properties تظهر خصائص البروتوكول (كما في شكل 3)



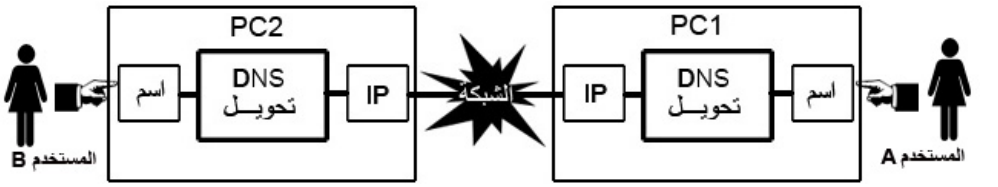
شكل رقم (3)

إعداد الـ IP :

يلاحظ أنه عند عرض خصائص البروتوكول TCP/IP في كلا نظامي التشغيل Windows98 و WindowsXP ظهرت صفحة واحدة هي الخاصة بإعداد الـ IP، لأنه أهم جزء في البروتوكول TCP/IP، وسنتناول في هذا الجزء الشرح التفصيلي لـ IP وكيفية إعداده.

ما هو الـ IP :

لابد لأي جهاز متصل بالشبكة من هويتين: الهوية الأولي هي الاسم (Host Name) وهو الاسم الذي يظهر به الجهاز في الشبكة، ويستطيع باقي مستخدمي الشبكة الوصول إليه من خلاله، ولا يمكن تكراره، والهوية الثانية هي العنوان الرقمي له والذي يستطيع من خلاله الاتصال بباقي أجهزة الشبكة وهو كذلك لا يمكن تكراره ويطلق عليه الـ IP (العنوان الداخلي Internal Pointer)، وعليه فلابد من أن يحدث تحويل من الاسم إلى الـ IP والعكس أثناء عملية الاتصال. والنظام الذي يقوم بعملية التحويل يطلق عليه الـ DNS (Domain Name System)، وهو أيضا جزء من البروتوكول TCP/IP وخطوات الاتصال موضحة (كما في شكل 4)



شكل رقم (4)

خصائص الـ IP :

العنوان IP يتكون من 32-bit، وهذا معناه أن أقصي عدد من الأجهزة (أو العناوين) في أي شبكة لن يتعدى 429,496,7296 (2^{32}) والجهاز هنا يعني عنوان، لأنه غير مسموح بتكرار أي عنوان. ويقسم الـ IP إلى 4 خانات كل منها 4-bit، وهذا يعني أن أقصى عدد في كل خانة هو 255 (2^8-1)، ويتم الفصل بين الخانات بـ (.) وتتم قراءة الـ IP بدءًا من الخانة التي في اليسار وهنا سنبين بعض الملاحظات الهامة :

- أقصى رقم = $2^{\text{عدد الـ Bits}}$ – 1(لأن العد يبدأ من 0).
- المجموع الكلي للأعداد = $2^{\text{عدد الـ Bits}}$ (لأن الصفر يتم عده)
- الأرقام في أي خانة من خانات الـ IP تتراوح من الـ 0 الى 255.

العمليات هنا منسوبة إلى العدد 2، لأن النظام المستخدم في الكمبيوتر هو النظام الثنائي والذي أساسه الرقم 2

مثال : افترض 3 خانات في النظام العشري (نظام الأعداد العادي والذي أساسه الرقم 10)، يكون أقصي رقم هو 999 (10^3-1) والمجموع الكلي للأعداد هو 1000 (من 0 إلى 999).

وسنقوم هنا بعرض أمثلة على بعض أشكال الـ IP الصحيحة :

IP=192.163.36.1 IP=53.63.68.4 IP=10.3.36.69

وهنا أمثلة لبعض أشكال الـ IP الخاطئة، وسنبين الخطأ:

IP	سبب الخطأ
10..3.6	الخانة الثانية خالية.
360.336.2	الخانة الأولي أكبر من 255.
10.5.1.-1	الخانة الرابعة 1- والأرقام في أي خانة دائمًا موجبة

كيف يتم الوصول إلى أجهزة الشبكة من خلال الـ IP الخاص بها :

لكي يتم الاتصال بجهاز في الشبكة لابد من معرفة عنوان الشبكة الفرعية التابع لها أولاً ثم معرفة عنوانه داخل هذه الشبكة الفرعية ولذا تم تقسيم الـ IP إلى قسمين :

القسم الأول : عنوان الشبكة الفرعية Subnet Address.

القسم الثاني : عنوان الجهاز داخل الشبكة الفرعية.

ملاحظة : هذا النظام متبع في كثير من الأنظمة وكمثال أرقام الهواتف تجد أن أي رقم هاتف مقسم إلى قسمين: الأول كود المدينة والثاني رقم الهاتف.

والسؤال الآن كيف يمكن معرفة عدد الخانات الخاصة بعنوان الشبكة الفرعية وعدد الخانات الخاصة بعنوان الجهاز داخل الشبكة الفرعية ؟

والجواب: باستخدام الـ Subnet Mask (قناع الشبكة الفرعية). وكلمة قناع تعني أنه يظهر شيئًا ويخفي شيئًا آخر وهذا صحيح لأنه يظهر عنوان الشبكة الفرعية (ولهذا يطلق عليه قناع الشبكة الفرعية)، ويخفي عنوان الجهاز. ومن خصائص القناع أنه يماثل الكائن الأصلي من حيث الحجم، وهذا أيضا صحيح، لأن تمثيل الـ Subnet Mask يماثل تمامًا الـ IP.

وبعد شرح كل هذا يأتي السؤال الهام وهو: كيف سيحدد الـ Subnet Mask عدد الخانات الخاصة بعنوان الشبكة وعدد الخانات الخاصة بعنوان الجهاز ؟

والجواب : الـ Subnet Mask يتكون من عدد من الـ 1's يتم عمل AND (عملية منطقية معروفة ولكننا سنوضحها لاحقًا) بينها وبين الـ IP فيظهر خانات عنوان الشبكة ويخفي خانات عنوان الجهاز. وقبل أن نوضح ذلك بمثال سنقوم بشرح عملية الـ AND لمن لا يعرفها .

عملية AND يتم إجراؤها بين 2-bit، وتكون نتيجة العملية معتمدة علي قيمة كل bit والجدول التالي يوضح نتيجة عملية الـ AND حسب جميع احتمالات قيمة كل Bit

Bit1	Bit2	نتيجة عملية الـ AND
0	0	0
0	1	0
1	0	0
1	1	1

والجدول السابق يوضح التالي :

- نتيجة عملية الـ AND تكون 0، إذا كانت قيمة أي Bit تساوي 0
- نتيجة عملية الـ AND تكون 1، إذا كانت قيمة كل Bit تساوي 1
- أن عملية الـ AND تشبه تقريبًا عملية الضرب، فعند ضرب عددين، إذا كانت قيمة أي منهما 0 تكون نتيجة الضرب 0، ولا تكون هناك قيمة لعملية الضرب إلا إذا كانت قيمة العددين لا تساوي الـ 0

بعد شرح عملية AND سنوضح الآن كيفية استخدام الـ Subnet Mask في تحديد عنوان الشبكة الفرعية وعنوان الجهاز داخل الشبكة الفرعية من خلال بعض الأمثلة :

مثال1 :

افترض أن جهازًا له IP=192.168.1.20 و Sub Mask=255.255.0.0 ، فما هو عنوان الشبكة الفرعية، وما هو عنوان الجهاز داخل الشبكة الفرعية ؟

الحل : قم بعمل التالي :

☜ قم بوضع الـ IP فوق الـ Subnet Mask (كل خانة فوق المناظرة لها).

IP	192	168	1	20
Subnet Mask	255	255	0	0

☜ قم بعمل AND بين كل خانة في الـ IP ونظيرتها في الـ Subnet Mask ويجب مراعاة الآتي عند إجراء العملية :

- الـ 255 عند تمثيلها بالنظام الثنائي تكون 11111111 (8 من الواحد) ولتسهيل العملية سنعتبرها بمثابة 1.
- يمكن اعتبار عملية الـ AND بمثابة عملية الضرب

☜ تكون نتيجة العملية كما يلي :

النتيجة	192	168	0	0

وهذه النتيجة تم الحصول عليها من خلال إجراء عملية AND بين 192 و 255 (أي ضرب 192 في 1) فتكون النتيجة 192 وكذلك بالنسبة لعملية الـ AND بين 168 و 255 تكون النتيجة 168 وعند إجراء عملية الـ AND بين الـ 1 و الـ 0، (أي ضرب 1 في 0) تكون النتيجة 0، وكذلك بالنسبة لعملية الـ AND بين 20 والـ 0 تكون النتيجة 0.

بعد الحصول على النتيجة السابقة يكون الرقم الذي ظهر هو عنوان الشبكة الفرعية والرقم الذي اختفي هو عنوان الجهاز داخل الشبكة الفرعية ، وعليه، ففي المثال السابق يكون عنوان الشبكة 192.168.0.0 (لأنه الرقم الذي ظهر) وعنوان الجهاز داخل الشبكة الفرعية هو 1.20

مثال2 :

افترض أن جهازًا لـه IP=192.168.1.20 و Sub Mask=255.255.255.0 ، فما هو عنوان الشبكة الفرعية، وما هو عنوان الجهاز داخل الشبكة الفرعية ؟

الحل :

IP	192	168	1	20
Subnet Mask	255	255	255	0
عملية AND	192	168	1	0

عنوان الشبكة = 192.168.1.0 (تم أخذ 3 خانات من الـ IP من اليسار والتي يناظرهم 255 في الـ Subnet Mask)

عنوان الجهاز داخل الشبكة الفرعية = 20

مثال3 :

افترض أن جهازًا لـه IP=192.168.1.20 و Sub Mask=255.0.0.0 ، فما هو عنوان الشبكة الفرعية، وما هو عنوان الجهاز داخل الشبكة الفرعية ؟

الحل :

IP	192	168	1	20
Subnet Mask	255	0	0	0
عملية AND	192	0	0	0

عنوان الشبكة = 192.0.0.0(تم أخذ خانة واحدة من الـ IP من اليسار والتي يناظرها 255 في الـ Subnet Mask)

عنوان الجهاز داخل الشبكة الفرعية = 168.1.20

وفيما يلي فوائد استخدام الـ Subnet Mask :

1. الـ IP لأي جهاز في الشبكة لا يأتي منفردًا أبدًا، ولكن لابد من أن يرفق معه الـ Subnet Mask لكي يتم تحديد عنوان الشبكة.
2. أي مجموعة من الأجهزة لابد من أن يكون عنوان الشبكة واحدًا لها جميعًا لكي تقع في شبكة واحدة، وإذا اختلف عنوان الشبكة لأي منها فهذا معناه أنه سيقع في شبكة فرعية أخرى.

مثال 1: مجموعة من الأجهزة تم تعيين IP و Subnet Mask لها كما يلي :

الجهاز A : IP= 192.168.1.20 Subnet Mask=255.255.0.0

الجهاز B : IP=192.168.2.30 Subnet Mask=255.255.0.0

الجهاز C : IP=192.168.5.40 Subnet Mask=255.255.0.0

هل هذه الأجهزة تقع في شبكة واحدة ؟ والجواب: نعم لأن عنوان الشبكة واحد لها جميعا وهو 192.168.0.0.

مثال 2: مجموعة من الأجهزة تم تعيين IP و Subnet Mask لها كما يلي :

الجهاز A : IP= 192.160.1.10 Subnet Mask=255.255.0.0

الجهاز B : IP=192.168.4.50 Subnet Mask=255.255.0.0

الجهاز C : IP=192.168.8.60 Subnet Mask=255.255.0.0

هل هذه الأجهزة تقع في شبكة واحدة ؟ والجواب: لا، الجهازين B و C يقعان في شبكة واحدة لأن عنوان الشبكة لهما هو 192.168.0.0 أما الجهاز A فإنه يقع في شبكة أخرى لأن عنوان الشبكة له هو 192.160.0.0.

1. قيمة الـ Subnet Mask تكون واحدة لجميع الأجهزة في أي شبكة فرعية.
2. يمكن معرفة عدد الأجهزة داخل كل شبكة فرعية من خلال معرفة قيمة الـ Subnet Mask.

مثال 1: شبكة فرعية قيمة الـ Subnet Mask لها هي 255.0.0.0، فما هو أقصى عدد من الأجهزة داخل هذه الشبكة ؟

الجواب: سيتم حجز الخانة اليسرى من الـ IP (والتي يناظرها الـ 255) لعنوان الشبكة والخانات الثلاث الأخرى لعناوين الأجهزة كما يلي:

عناوين الأجهزة			**عنوان الشبكة**

وعليه تكون سعة القسم الخاص بعناوين الأجهزة هي 24-bit (8-bit لعنوان الشبكة و 24-bit لعناوين الأجهزة) ، وعليه يكون أقصى عدد للأجهزة في هذه الشبكة هو 2^{24}، أي 167,772,16.

مثال 2: شبكة فرعية قيمة الـ Subnet Mask لها هي 255.255.0.0، فما هو أقصى عدد من الأجهزة داخل هذه الشبكة ؟

الجواب: سيتم حجز (2 خانة) من اليسار من الـ IP (والتي يناظرها الـ 255) لعنوان الشبكة والـ (2 خانة) الأخريين لعناوين الأجهزة كما يلي :

عناوين الأجهزة		**عنوان الشبكة**	

وعليه تكون سعة القسم الخاص بعناوين الأجهزة هي 16-bit (16-bit لعنوان الشبكة و 16-bit لعناوين الأجهزة) ، وعليه يكون أقصى عدد للأجهزة في هذه الشبكة هو 2^{16} أي 655,36 (عدد الأجهزة أقل من المثال السابق).

مثال 3: شبكة فرعية قيمة الـ Subnet Mask لها هي 255.255.255.0 فما هو أقصى عدد من الأجهزة داخل هذه الشبكة ؟

الجواب: سيتم حجز 3 خانة من اليسار من الـ IP (والتي يناظرها الـ 255) لعنوان الشبكة والخانة الأخرى لعناوين الأجهزة كما يلي :

عناوين الأجهزة	عنوان الشبكة		

وعليه تكون سعة القسم الخاص بعناوين الأجهزة هي 8-bit (24-bit لعنوان الشبكة و 8-bit لعناوين الأجهزة) ، وعليه يكون أقصى عدد للأجهزة في هذه الشبكة هو 2^8، أي 256 (عدد الأجهزة أقل من المثالين السابقين).

تم تقسيم الشبكات من حيث عدد الأجهزة في كل منها إلى ثلاث مجموعات Classes بناءً على قيمة الـ Subnet Mask لكل شبكة كما يلي :

المجموعة Class	الـ Subnet Mask	عدد الأجهزة	ملاحظات
A	255.0.0.0	2^{24} = 167,772,16	شبكة كبيرة
B	255.255.0.0	2^{16} = 655,36	شبكة متوسطة
C	255.255.255.0	2^8 = 256	شبكة صغيرة

إعداد الـ IP والـ Subnet Mask :

والآن تبين لنا أن أي جهاز في الشبكة لابد له من IP و Subnet Mask ولابد أن يكون عنوان الشبكة له مطابق لعنوان الشبكة لباقي الأجهزة، لكي يتم الاتصال بينه وبين باقي الأجهزة ولكننا قمنا بإعداد نظام تشغيل الشبكة، وقمنا باستعراض الأجهزة دون إعداد لـ IP والـ Subnet Mask. والسؤال كيف تم ذلك دون أن نقوم باعداهما؟ والجواب: أن نظام التشغيل قام تلقائيًا بإعداد الـ IP والـ Subnet Mask بصورة معينه تضمن اتصال الأجهزة، لكنه ترك للمستخدم إمكانية تعديل هذا الإعداد، والخطوات التالية توضح كيفية إعداد الـ IP والـ Subnet Mask في Windows98 و WindowsXP :

خطوات الإعداد :

☜ قم بعرض خصائص البروتوكول TCP/IP ، فتظهر صفحة إعداد الـ IP و الـ Subnet Mask (كما في شكل 1 و 3) وهناك خياران للإعداد :

الخيار الأول : Obtain IP Automatically :هو الخيار الافتراضي، ويعني أن يقوم نظام تشغيل الشبكة بإعداد الـ IP والـ Subnet Mask تلقائيًا، ولذا تجد أنه في حالة تحديد هذا الخيار أن حقلي الـ IP والـ Subnet Mask غير نشيطين. وهذا الخيار مناسب للمستخدمين قليلي الخبرة

بالشبكات، الذين يريدون تكوين الشبكة دون الخوض في تفاصيل قد لا يعرفونها، والسؤال الآن: ما هي قيمة الـ IP والـ Subnet Mask في حالة إذا ما قام نظام التشغيل بإعدادهما تلقائيًا ؟ والجواب يكمن في كيفية قراءة الـ IP والـ Subnet Mask.

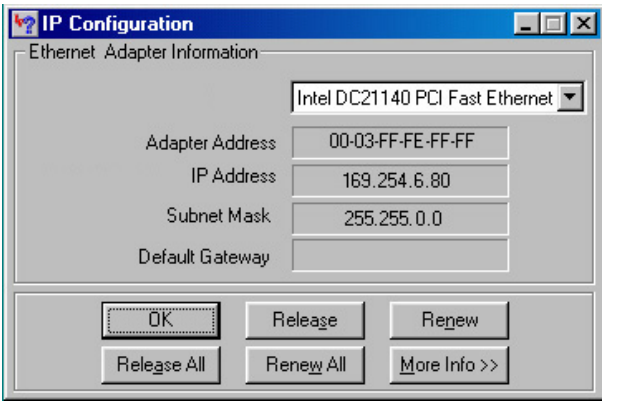
قراءة الـ IP والـ Subnet Mask :

الجدول التالي يوضح الأوامر التي يمكن من خلالها قراءة الـ IP والـ Subnet Mask وتوافقها مع أنظمة التشغيل:

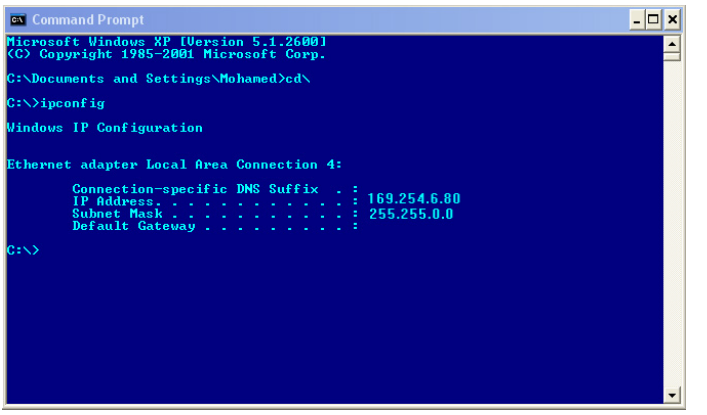
الأمر	الواجهة	أنظمة التشغيل المتوافق معها
Winipcfg	ويندوز	Windows98 و Windows ME
Ipconfig	دوس	جميع أنظمة التشغيل

وعند تشغيل الأمر Winipcfg (Windows IP Configuration) في نظام التشغيل Windows98 (كما في شكل 5) (أو Ipconfig في WindowsXP) (كما في شكل 6) لجميع أجهزة الشبكة تجد أن قيمة الـ IP الذي قام نظام التشغيل بوضعه هو 169.254.x.x (x تعني متغير) والـ Subnet Mask هو 255.255.0.0، وعليه فإن نظام التشغيل قد حدد الخصائص التالية للشبكة تلقائيًا :

- عنوان الشبكة هو 169.254.0.0.
- الشبكة من النوع Class B، وهي الشبكة المتوسطة (حيث أنها شبكة متوسطة بين الشبكات الكبيرة Class A والشبكات الصغيرة Class C).



شكل رقم (5)



شكل رقم (6)

وسنتناول الآن فوائد وعيوب هذه الخيار

الفوائد :

1. يتم تحديده تلقائيًا دون تدخل من المستخدم.
2. يضمن عدم وجود تعارض (تكرار) بين الـ IP الذي قام بوضعه وأي IP أخر في الشبكة.
3. يقوم بتغيير الـ IP تلقائيًا في حالة وجود تعارض بينه وبين أي IP آخر في الشبكة

العيوب :

1. الإعدادات التي يقوم بها ليست هي الأمثل بالنسبة للمستخدم.
2. يبطئ تحميل الجهاز، لأنه في حالة تحديده يترك لنظام التشغيل مسئولية تحديد الـ IP وضمان عدم تكراره، ولذا ففي كل مرة يقوم الجهاز بالتحميل والدخول إلى الشبكة فإن نظام التشغيل يقوم بفحص الـ IP's لجميع أجهزة الشبكة ليتأكد أن الـ IP الذي قام بوضعه ليس متعارضًا مع أي IP آخر في الشبكة، وفي حالة تكراره فإنه يقوم بتغيير الـ IP تلقائيًا. وهذه العملية تأخذ وقتًا مما يبطئ عملية التحميل، وهذا متعارف عليه فإن كثير من المستخدمين يلاحظون هذا البطء، ولا يعرفون أن سبب ذالك هو تحديد هذا الخيار.

الخيار الثاني : Specify an IP address : يترك للمستخدم تحديد الـ IP والـ Subnet mask بنفسه، ولذا فإنه عند تحديده يتم تنشيط كلاً من حقلي الـ IP والـ Subnet، ويتم إعداد كل منهما كما يلي :

☜ قم بتحديد الـ Subnet Mask بناءً على عدد أجهزة الشبكة كما يلي :

عدد الأجهزة	Subnet Mask	الـ Class

اقل من أو يساوي 256 جهازًا	255.255.255.0	Class C
أكبر من 256 جهازًا واقل من أو يساوي 65536 جهازًا	255.255.0.0	Class B
أكبر من 65536 جهازًا	255.0.0.0	Class A

☜ قم بإدخال الـ Subnet Mask ويكون عامًا لجميع أجهزة الشبكة.

☜ قم بإدخال الـ IP بصورة صحيحة في حقل IP address، بحيث تضمن وقوع الأجهزة في شبكة واحدة، وضمان عدم تكراره،

مثال : شبكة مكونة من 5 أجهزة، كيف يمكن إعداد الـ IP والـ Subnet Mask بصورة مثالية ؟

الخطوة الأولي : تحديد الـ Subnet Mask المثالي، وفي هذه الحالة يكون 255.255.255.0، لأن عدد الأجهزة أقل من 256 جهازًا

الخطوة الثانية : إدخال الـ Subnet Mask لجميع أجهزة الشبكة بنفس القيمة السابقة.

الخطوة الثالثة : قم بتحديد IP لأجهزة الشبكة، على أن يكون أول 3 خانات من اليسار ثابتة لجميع أجهزة الشبكة (التي يناظرها 255 في الـ Subnet Mask)، وهي التي تمثل عنوان الشبكة والخانة الرابعة متروكة لعناوين الأجهزة، وعليه فيمكن أن تكون عناوين الأجهزة في الشبكة كما يلي :

الجهاز الأول : 169.254.20.1.

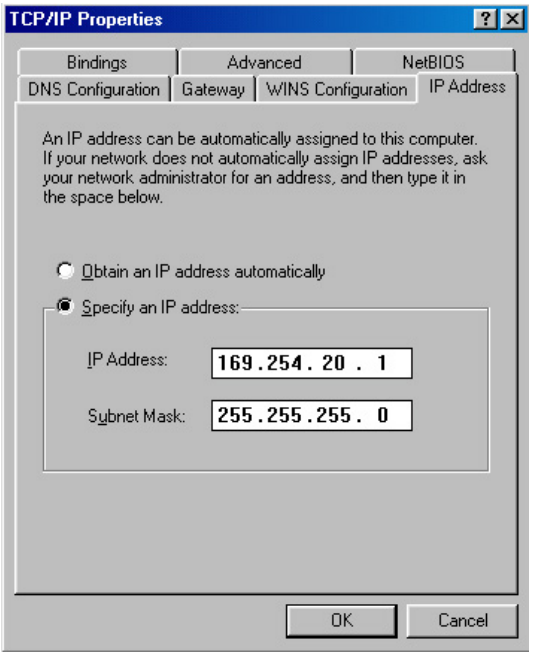
الجهاز الثاني : 169.254.20.2.

الجهاز الثالث : 169.254.20.3.

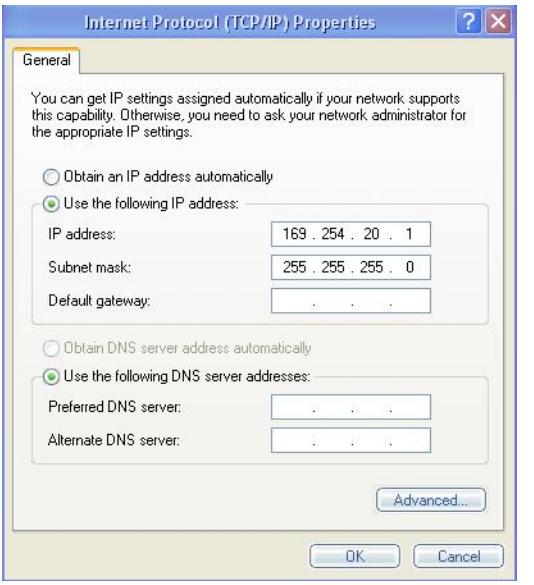
الجهاز الرابع : 169.254.20.4.

الجهاز الخامس : 169.254.20.5.

ولاحظ أننا استخدمنا الـ IP الشائع وهو 169.254 ولكننا كان يمكن أن نستخدم أي أرقام بحيث تكون صحيحة (بين 0 والـ 255) وغير متعارضة (شكل 7 يبين عملية الإعداد في Windows98 وشكل 8 يبين عملية الإعداد في WindowsXP)



شكل رقم (7)



شكل رقم (8)

وسنتناول الآن فوائد وعيوب هذه الخيار

الفوائد :

1. يمكن إعداد الـ IP والـ Subnet Mask بالطريقة الأمثل.

2. يسرع في عملية تحميل الجهاز، لأن المستخدم الآن أصبح هو المسئول عن الـ IP، وبالتالي لن يقوم نظام التشغيل أثناء عملية التحميل بالبحث عن وجود تعارض بين الـ IP الذي قام المستخدم بوضعه وأي IP آخر في الشبكة.

العيوب :

1. قد يحدث تعارض بين الـ IP الذي قام المستخدم بوضعه و IP آخر في الشبكة.
2. لا يقوم نظام التشغيل بتغييره تلقائيًا في حالة وجود تعارض بينه وبين IP آخر في الشبكة، ولكن على المستخدم أن يقوم بتغيير الـ IP بنفسه، بعد أن يقوم نظام التشغيل بإخبار المستخدم بوجود التعارض

وسنوضح الآن بعض المفاهيم الهامة من خلال الأسئلة التالية :

♦ السؤال الأول: كيف يمكن للمستخدم العادي (الذي ليس لديه دراية بإعداد الـ IP والـ Subnet Mask) إعداد الـ IP والـ Subnet Mask بحيث يستفيد من مميزات كلا الخيارين؟

والجواب: في الخطوات التالية :

- يقوم المستخدم أولاً بتحديد الخيار الأول Obtain IP automatically، ويترك لنظام التشغيل إعداد الـ IP والـ Subnet Mask بنفسه، وبذلك نكون قد استفدنا من ميزة عدم التعارض.
- قم بقراءة الـ IP والـ Subnet Mask الذي قام نظام التشغيل بوضعهما لجميع أجهزة الشبكة (وقد وضحنا سابقًا كيف يمكن قراءة كل منهما).
- قم بتحديد الخيار الثاني Specify an IP Address ثم قم بإدخال القيم التي تمت قراءتها حسب كل جهاز. وبذلك نكون قد استفدنا من ميزة سرعة التحميل.

♦ السؤال الثاني: ما تأثير نوع الـ Class (A أو B أو C) على أداء الشبكة ؟

والجواب: عندما يتصل جهاز بجهاز آخر داخل شبكة واحدة فلا داعي لاستخدام عنوان الشبكة، بل يكفي فقط استخدام عنوان الجهاز داخل الشبكة (وكمثال الاتصال بالهاتف، عندما يتصل شخص بآخر داخل نفس المدينة فإنه لا يستخدم كود المدينة، ولكن يستخدم فقط رقم الهاتف الداخلي)، وعليه فكلما كان عدد خانات عنوان الجهاز أقل كلما كان أسرع في الاتصال، أي أن Class C أسرع من Class B، والأخير أسرع من Class A (وقد بينَّا كيف يمكن تحديد نوع الـ Class الأمثل حسب عدد الأجهزة في الشبكة).

♦ السؤال الثالث: هل يمكن استخدام الـ IP بدلاً من اسم الجهاز في تنفيذ عمليات الشبكة ؟ وأيهما أسرع ؟

والجواب: نعم يمكن استخدام الـ IP بدلاً من الاسم في عمليات الشبكة. فمثلاً إذا أراد الجهاز PC1 تعيين محرك أقراص شبكة للمجلد Test في الجهاز PC2 الذي لـه IP=192.168.0.20 يمكن استخدام المسار التالي :

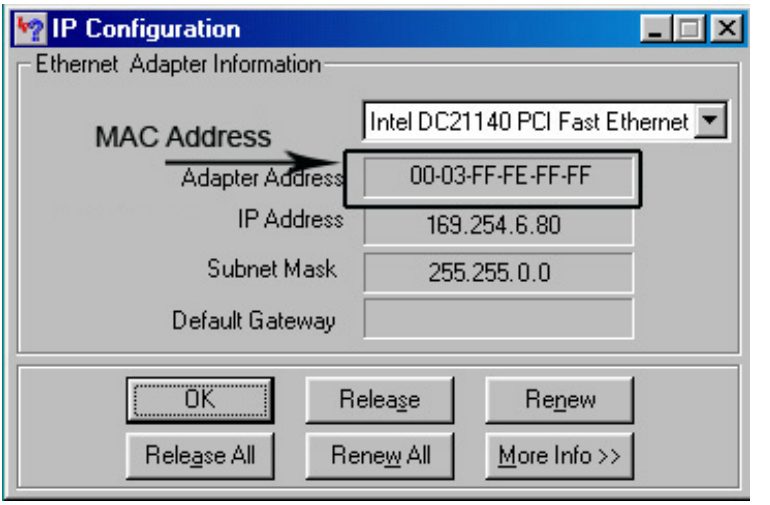
\\192.168.0.20\Test بدلاً من \\PC2\Test

والأسرع في الاتصال هو استخدام الـ IP بدلاً من الاسم، لأن الاتصال في النهاية سيتم من خلال الـ IP، ولذا عند استخدام الاسم سيحدث بطء نتيجة عملية التحويل من الاسم إلى الـ IP باستخدام الـ DNS.

♦ السؤال الرابع- هل الـ IP هو العنوان الفعلي للجهاز ؟

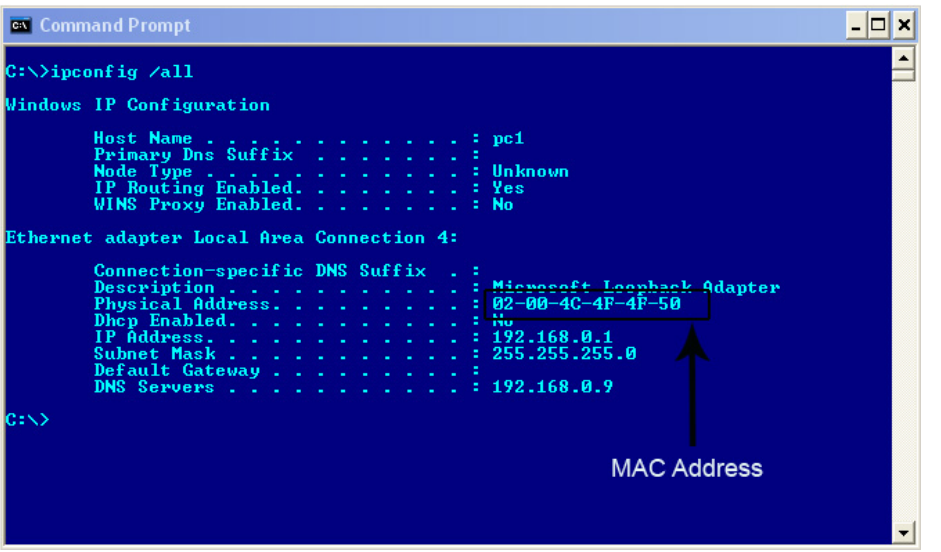
الجواب: الـ IP ليس العنوان الفعلي للجهاز ولكنه عنوان منطقي يمكن التحكم في إعداداته من قبل المستخدمين. ولكن العنوان الفعلي للجهاز يسمى الـ MAC Address (Media Access Control). وأحيانًا يطلق عليه الـ Adapter Address و ويمثل عنوان كارت الشبكة، ويتم تخزينه داخل شريحة الـ ROM الخاصة بكارت الشبكة وسعته 48-bit، ومقسم إلى 6 خانات، كل خانة سعتها 8-bit ويتم الفصل بينها بـ (-) وتمثل الـ 3 خانات من اليسار كود الشركة المصنعة والـ 3 خانات من اليمين رقم التسلسل الخاص بالكارت داخل الشركة، وبالتالي فإن هذا العنوان لا يمكن تكراره. ويمكن قراءة الـ MAC address من خلال نفس الأوامر الخاصة بقراءة الـ IP :

1. الأمر Winipcfg يقوم بقراءة الـ MAC Address في Windows98 (كما في شكل 9)



شكل رقم (9)

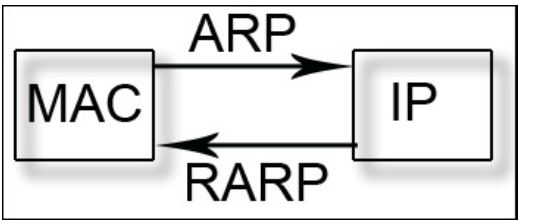
2. الأمر Ipconfig /all يقوم بقراءة الـ MAC Address في WindowsXP (كما في شكل 10) ولاحظ أننا استخدمنا all/ مع الأمر Ipconfig، لأن الأمر بدونه يعرض الـ IP فقط.



شكل رقم (10)

وبناءًا عليه لابد من أن يحدث تحويل بين الـ IP والـ MAC والعكس. ويقوم برنامج Arp (Address Resolution Protocol) بعملية التحويل من الـ IP إلى الـ MAC، ويقوم البرنامج Rarp (Reverse Address Resolution Protocol) بالعملية العكسية، وهي التحويل من الـ

MAC إلى الـ IP وهذان البرنامجان ضمن نظام تشغيل الشبكة. والرسم التوضيحي للتحويل (كما في شكل 11)



شكل رقم (11)

تقسيم الشبكات Subnetting:

سنتناول في هذا الجزء كيفية تقسيم شبكة واحدة إلى عدة شبكات فرعية. والمثال التالي يوضح فائدة عملية التقسيم.

مثال: افترض أن شركة بها 5 أقسام تريد عمل شبكة داخلية بحيث تكون شبكة كل قسم منفصلة تمامًا ولا يستطيع مستخدمو الشبكة في أي قسم من الأقسام الاتصال بأجهزة قسم آخر. كيف يمكن تنفيذ ذلك ؟

الجواب: هناك حلان:

الحل الأول: باستخدام الـ Hardware، حيث يتم عمل شبكة منفصلة لكل قسم وهذا لاشك سيكلف الشركة الكثير.

الحل الثاني: عمل شبكة واحدة ثم تقسيم الشبكة إلى 5 شبكات فرعية. وفي هذه الحالة لن يستطيع أحد مستخدمي الشبكة في أي قسم من الأقسام الاتصال بأجهزة قسم آخر (كأننا قمنا تمامًا بالحل الأول ولكننا وفرنا الكثير من الجهد والمال).

فكرة عملية التقسيم: عملية التقسيم تعتمد على تغيير عناوين الشبكة، وكل شبكة فرعية سيكون لها عنوان مختلف (حيث أننا ذكرنا من قبل أنه لكي تقع مجموعة من الأجهزة في شبكة واحدة لابد أن يكون عنوان الشبكة واحدًا لها جميعًا، وإذا اختلف عنوان الشبكة لأي منها يكون قد وقع في شبكة أخرى).

وهناك طريقتان لعملية التقسيم كما يلي:

الطريقة الأولى: ليست لها خطوات محددة ولكنها تعتمد فقط على فكرة التقسيم السابقة ولكن بأي وسيلة.

مثـــال: شـبكة واحـدة بهـا 20 جهـازًا وعنـاوين الـ IP لهـذه الأجهـزة مـن 192.168.0.1 إلـى 192.168.0.20 والـ Subnet Mask=255.255.255.0 يراد تقسيمها إلى 5 شبكات فرعية، كل شبكة بها 4 أجهزة، فما هي خطوات التنفيذ ؟

☜ قم بتحديد الـ Subnet Mask المناسب لهذه الشبكات الفرعية. وفي هذا المثال سيكون الـ Subnet Mask هو 255.255.255.0

☜ قم بافتراض أرقام لعناوين الشبكات الفرعية المطلوبة، في هذا المثال (مثلاً)

الشبكة الأولي: 192.168.0

الشبكة الثانية: 192.168.1

الشبكة الثالثة: 192.168.2

الشبكة الرابعة : 192.168.3

الشبكة الخامسة : 192.168.4

☜ قم بافتراض أرقام لعناوين الأجهزة داخل كل شبكة حسب عدد كل شبكة في هذا المثال (مثلاً) سنفترض عناوين للأجهزة من 1 إلى 5

الشبكة الأولي: عناوين الـ IP لأجهزة الشبكة هي 192.168.0.1 حتى 192.168.0.5.

الشبكة الثانية: عناوين الـ IP لأجهزة الشبكة هي 192.168.1.1 حتى 192.168.1.5.

الشبكة الثالثة: عناوين الـ IP لأجهزة الشبكة هي 192.168.2.1 حتى 192.168.2.5.

الشبكة الرابعة : عناوين الـ IP لأجهزة الشبكة هي 192.168.3.1 حتى 192.168.3.5.

الشبكة الخامسة : عناوين الـ IP لأجهزة الشبكة هي 192.168.4.1 حتى 192.168.4.5.

ويمكن أي يكون هناك حل آخر كما يلي :

الشبكة الأولي : 192.168.0.

الشبكة الثانية : 192.169.0.

الشبكة الثالثة : 192.170.0.

الشبكة الرابعة : 192.171.0.

الشبكة الخامسة : 192.172.0.

الشبكة الأولي: عناوين الـ IP لأجهزة الشبكة هي 192.168.0.10 حتى 192.168.0.14.

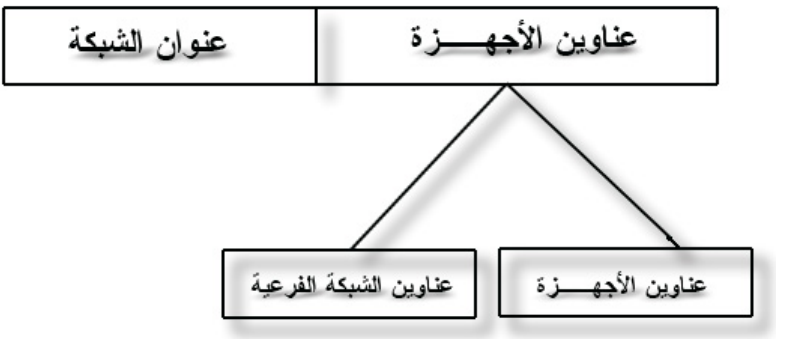
الشبكة الثانية: عناوين الـ IP لأجهزة الشبكة هي 192.169.0.25 حتى 192.169.0.29.

الشبكة الثالثة: عناوين الـ IP لأجهزة الشبكة هي 192.170.0.30 حتى 192.170.0.34.

الشبكة الرابعة : عناوين الـ IP لأجهزة الشبكة هي 192.171.0.1 حتى 192.171.0.5.

الشبكة الخامسة : عناوين الـ IP لأجهزة الشبكة هي 192.172.0.45 حتى 192.172.0.49.
وإذا استمررنا حسب هذه الطريقة سيكون عندنا حلول متعددة. وعيب هذه الطريقة أنها ليس لها نظام محدد، ولكنها مناسبة للمستخدمين غير متخصصين والطريقة التالية هي التي ينصح بها، لأنها محددة، ويمكن من خلالها عمل إحصاءات دقيقة عن الشبكة، وهي من أساسيات دورة الـ CCNA لمن سيرغب في الالتحاق بها.

الطريقة الثانية: وتعتمد على فكرة تقسيم عنوان الجهاز في الـ IP إلى قسمين: الأول يمثل عنوان الشبكة الفرعية والآخر يمثل عناوين الأجهزة داخل الشبكة الفرعية (لأن عنوان الشبكة سيكون عامًا لجميع الشبكات الفرعية) والرسم التوضيحي (كما في شكل 12)



شكل رقم (12)

والمثال التالي يوضح هذه الطريقة

مثال 1 : شبكة لها عنوان 169.254.x.x والـ Subnet Mask هو 255.255.0.0 يراد تجزئتها إلى 16 شبكة فرعية، فما هي عناوين الشبكات الفرعية ونطاق كل شبكة والـ Subnet Mask لهذه الشبكات الفرعية ؟ وما هي خطوات التقسيم ؟

الحل :

الخطوة الأولي: تحديد عدد الـ Bits الخاصة بعناوين الأجهزة، في هذا المثال 16-bit.

الخطوة الثانية: تحديد عدد الـ Bits التي سنحجزها إلى عنوان الشبكة الفرعية ويتم تحديدها بناءً على عدد الشبكات الفرعية حسب القاعدة التالية:

$$\text{عدد الشبكات الفرعية} = 2^{\text{عدد الـ Bits}}$$

وحيث أن عدد الشبكات الفرعية المطلوبة = 16 فإن عدد الـ Bits التي سيتم حجزها لعنوان الشبكة هي 4-bits (لأن $16=2^4$) ويتبقى 12-bit لعناوين الأجهزة داخل كل شبكة

الخطوة الثالثة: التمثيل الثنائي (Binary) للشبكات الفرعية الـ 16(من 0 إلى 15) من خلال الـ 4-bit كما يلي:

رقم الشبكة	عنوان الشبكة				عناوين الأجهزة											
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
4	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
6	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
8	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
10	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
11	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
12	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
14	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
15	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0

الخطوة الرابعة: تحديد عناوين الشبكات، من خلال دمج كل 8-bit من الجدول السابق لتمثيل الخانة الثالثة والرابعة في الـ IP (تذكر وجود (2 خانة) ثابتة من الـ IP وهما عنوان الشبكة الرئيسية 169.254) كما يلي:

رقم الشبكة	الخانة الثالثة في الـ IP								الخانة الرابعة في الـ IP								عنوان الشبكة
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.0.0
1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	169.254.16.0
2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.32.0
3	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	169.254.48.0
4	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.64.0
5	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	169.254.80.0
6	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.96.0
7	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	169.254.112.0
8	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.128.0

9	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.144.0
10	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.160.0
11	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.176.0
12	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.192.0
13	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.208.0
14	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.224.0
15	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.240.0

الخطوة الخامسة: تحديد نطاق كل شبكة، ويعني عدد الأجهزة، أو الـ IP's داخل كل منها بناءً على الجدول السابق كما يلي:

تحديد بداية نطاق الشبكة: بداية نطاق الشبكة هو ثاني IP في الشبكة (وليس أول IP). (مثلاً) الشبكة رقم 0 عنوانها هو 169.254.0.0 ، أول IP فيها هو 169.254.0.0 وهو نفسه عنوان الشبكة، لذا يتم تفادي استخدام أول IP لأنه يؤدي إلى عدم اتصال الجهاز بالشبكة واستخدام الـ IP الذي يليه وهو 169.254.0.1

تحديد نهاية نطاق الشبكة: نهاية نطاق أي شبكة هو الـ IP الذي يسبق بداية الشبكة التي تليها مطروحًا منه 1، (مثلاً) نهاية نطاق الشبكة رقم 0 هو الـ IP الذي يسبق بداية الشبكة رقم 1 وهو 169.254.15.255 (وهنا خطأ يقع فيه كثير من المستخدمين حيث يعتقدون أن الـ IP الذي يسبقه هو 169.254.15.0 وهذا خطأ، والدليل على ذلك أن الرقم الذي يسبق الـ 20 (كمثال) هو 19 وليس 10) مطروحًا منه 1، أي 169.254.15.245. وقد يتساءل البعض لماذا يتم طرح 1؟ والسبب أنه لو كانت نهاية النطاق في المثال السابق 169.254.15.255 دون طرح الـ 1 فلن يحدث Mask له من خلال الـ Subnet Mask، لأن الخانة الرابعة 255 وهي تماثل نفس أرقام الـ Subnet Mask، ولذا يتم تفادي استخدامه، لأنه يؤدي إلى عدم اتصال الجهاز بالشبكة ونستخدم الذي يسبقه. والرسم التوضيحي لبداية ونهاية الشبكات الفرعية (كما في شكل 13)

←	**الشبكة رقم 2**	**الشبكة رقم 1**	**الشبكة رقم 0**
←	**نطاق الشبكة**	**نطاق الشبكة**	**نطاق الشبكة**

شكل رقم (13)

تحديد نهاية نطاق الشبكة الأخيرة: نظرًا لأن الشبكة الأخيرة ليس بعدها شبكة أخرى، يكون نهاية نطاق الشبكة الأخيرة آخر أرقام في الخانة الثالثة والرابعة في الـ IP وهما 254.254، لأننا كما قلنا لا يمكن استخدام الأرقام 255.255

والجدول التالي يوضح نطاق الشبكات الفرعية:

رقم الشبكة	عنوان الشبكة	نطاق الشبكة	
		من	إلى
0	169.254.0.0	169.254.0.1	169.254.15.254
1	169.254.16.0	169.254.16.1	169.254.31.254
2	169.254.32.0	169.254.32.1	169.254.47.254
3	169.254.48.0	169.254.48.1	169.254.63.254
4	169.254.64.0	169.254.64.1	169.254.79.254
5	169.254.80.0	169.254.80.1	169.254.95.254
6	169.254.96.0	169.254.96.1	169.254.111.254
7	169.254.112.0	169.254.112.1	169.254.127.254
8	169.254.128.0	169.254.128.1	169.254.143.254
9	169.254.144.0	169.254.144.1	169.254.159.254
10	169.254.160.0	169.254.160.1	196.254.175.254
11	169.254.176.0	169.254.176.1	169.254.191.254
12	169.254.192.0	169.254.192.1	169.254.207.254
13	169.254.208.0	169.254.208.1	169.254.223.254
14	169.254.224.0	169.254.224.1	169.254.239.254
15	169.254.240.0	169.254.240.1	169.254.254.254

الخطوة السادسة : تحديد سعة كل شبكة فرعية (والمقصود بها عدد الأجهزة داخل كل شبكة فرعية)، وسعة جميع الشبكات الفرعية متساوية، ويتم تحديد سعتها من خلال عدد الـ Bits الخاصة بعناوين الأجهزة حسب القاعدة التالية:

سعة الشبكة = 2 عدد الـ **Bits** الخاصة بعناوين الأجهزة **−2**

وتم طرح 2، لأننا كما ذكرنا نطاق الشبكة يكون بعد بداية الشبكة بـ 1 وقبل نهايتها بـ 1

وعليه فسعة أي شبكة فرعية في المثال السابق هي 4094 جهازًا (2^{12}-2=4094)

الخطوة السابعة : تحديد قيمة الـ Subnet Mask ، وحيث أن قيمة الـ Subnet Mask الأصلية هي 255.255.0.0، ونظرًا لأننا خصصنا 4-bit من الخانة الثالثة لعنوان الشبكة يتم وضع 1's فيها لعمل الـ Mask (كما في شكل 14)

الخانة الرابعة	الخانة الثالثة	الخانة الأولى

255.255	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
والثانية																

شكل رقم (14)

يكون قيمة الـ Subnet Mask هي 255.255.240.0 ويكون عامًا لـ 16 شبكة الفرعية.

مثال 2 : شبكة لها عنوان 169.254.x.x والـ Subnet Mask هو 255.255.0.0. يراد تجزئتها إلى عدد من الشبكات الفرعية، بحيث تكون سعة كل شبكة 1022 جهازًا فما هو عدد الشبكات الفرعية وعناوينها وقيمة الـ Subnet Mask لهذه الشبكات الفرعية ؟

الحل :

هذا المثال عكس المثال السابق حيث أننا هنا لدينا نطاق الشبكة، ونريد عدد الشبكات الفرعية ولكن الفكرة واحدة في المثالين، والحل في الخطوات التالية:

الخطوة الأولي: تحديد عدد الـ Bits الخاصة بعناوين الأجهزة من خلال عدد الأجهزة كما يلي:

عدد الأجهزة = 2 عدد الـ **Bits** الخاصة بعناوين الأجهزة **–2**

إذن عدد الـ Bits المطلوبة لعناوين الأجهزة = 10 لأن $(2^{10}-2=1022)$

الخطوة الثانية : تحديد عدد الـ Bits الخاصة بعناوين الشبكات الفرعية من خلال القاعدة :

عدد الـ Bits الخاصة بعناوين الشبكات الفرعية= عدد الـ Bits الكلية – عدد الـ Bits الخاصة بعناوين الأجهزة

حيث أن عدد الـ Bits الكلية هي عدد الـ Bits التي كانت مخصصة لعناوين الأجهزة وسيتم تقسيمها إلى عناوين الشبكات الفرعية وعناوين الأجهزة داخل كل شبكة فرعية وفي هذا المثال 16-bit وبناءً عليه يكون:

عدد الـ Bits الخاصة بعناوين الشبكات الفرعية = 6 (16-10)

الخطوة الثالثة: تحديد عدد الشبكات الفرعية بناءً على الخطوة السابقة كما يلي:

عدد الشبكات الفرعية = 2 عدد الـ **Bits** الخاصة بعناوين الشبكات الفرعية

عدد الشبكات الفرعية = 2^6 = 64 شبكة فرعية.

الخطوة الرابعة : التمثيل الثنائي (Binary) للشبكات الفرعية الـ 64(من 0 إلى 63) من خلال الـ 6-bit كما يلي:

رقم الشبكة	عنوان الشبكة						عناوين الأجهزة									
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0
4	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0
6	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0
8	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0
10	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0
11	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0
12	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0
14	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0
15	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0
16	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
↓ ↓ ↓ ↓							↓ ↓ ↓ ↓									
63	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0

الخطوة الخامسة: تحديد عناوين الشبكات من خلال دمج كل 8-bit من الجدول السابق لتمثيل الخانة الثالثة والرابعة في الـ IP (تذكر وجود (2 خانة) ثابتة من الـ IP وهما عنوان الشبكة الرئيسية 169.254) كما يلي:

رقم الشبكة	الخانة الثالثة في الـ IP								الخانة الرابعة في الـ IP								عنوان الشبكة
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.0.0

1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	169.254.4.0
2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	169.254.8.0
3	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	169.254.12.0
4	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	169.254.16.0
5	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	169.254.20.0
6	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	169.254.24.0
7	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	169.254.28.0
8	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.32.0
9	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	169.254.36.0
10	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	169.254.40.0
11	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	169.254.44.0
12	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	169.254.48.0
13	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	169.254.52.0
14	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	169.254.56.0
15	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	169.254.60.0
16	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	169.254.64.0
17	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	169.254.68.0
⬇⬇⬇⬇																	⬇⬇⬇⬇
63	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	169.254.252.0

الخطوة السادسة– تحديد نطاق كل شبكة فرعية بناءً على الجدول السابق كما يلي:

رقم الشبكة	عنوان الشبكة	نطاق الشبكة	
		من	إلى
0	169.254.0.0	169.254.0.1	169.254.3.254
1	169.254.4.0	169.254.4.1	169.254.7.254
2	169.254.8.0	169.254.8.1	169.254.11.254
3	169.254.12.0	169.254.12.1	169.254.15.254
4	169.254.16.0	169.254.16.1	169.254.19.254
5	169.254.20.0	169.254.20.1	169.254.23.254
6	169.254.24.0	169.254.24.1	169.254.27.254
7	169.254.28.0	169.254.28.1	169.254.31.254
8	169.254.32.0	169.254.32.1	169.254.35.254
9	169.254.36.0	169.254.36.1	169.254.39.254
10	169.254.40.0	169.254.40.1	169.254.43.254
11	169.254.44.0	169.254.44.1	169.254.47.254
12	169.254.48.0	169.254.48.1	169.254.51.254
13	169.254.52.0	169.254.52.1	169.254.55.254
14	169.254.56.0	169.254.56.1	169.254.59.254
15	169.254.60.0	169.254.60.1	169.254.63.254
16	169.254.64.0	169.254.64.1	169.254.67.254
17	169.254.68.0	169.254.68.1	169.254.71.254
⬇ ⬇ ⬇ ⬇	⬇ ⬇ ⬇ ⬇	⬇ ⬇ ⬇ ⬇	⬇ ⬇ ⬇ ⬇
63	169.254.252.0	169.254.252.1	169.254.254.254

الخطوة السابعة– تحديد قيمة الـ Subnet Mask ، وحيث أن قيمة الـ Subnet Mask الأصلية هي 255.255.0.0 ونظرًا لأننا خصصنا 6-bit من الخانة الثالثة لعنوان الشبكة يتم وضع 1's فيها لعمل الـ Mask (كما في شكل 15)

الخانة الأولى والثانية	الخانة الثالثة								الخانة الرابعة							
255.255	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0

شكل رقم (15)

تكون قيمة الـ Subnet Mask هي 255.255.252.0 ويكون عامًا لـ 64 شبكة الفرعية.

وفيما يلي ملاحظات حول عملية التقسيم :

الملاحظـة الأولـي : افترض أنـه يـراد تقسـيم شـبكة إلـى 20 شـبكة فرعيـة، فمـا هـو عـدد الـ Bits المطلوبة لتمثيل عنوان الشبكة ؟

الجواب : حسب القاعدة المذكورة

عدد الشبكات الفرعية = 2 عدد الـ Bits

2 عدد الـ Bits = 20 وعنـد حـل المعادلـة يكـون عـدد الـ bits المطلوبـة يسـاوي 4.32، لـذا يـتم استخدام 5-bits لتمثيل عناوين الشبكات الفرعية.

الملاحظة الثانية: أحيانًا يتم دمج كل من الـ IP والـ Subnet Mask لجهاز في الشبكة في سطر واحد بدلاً من ذكرهما منفصلين كما يلي:

مثال: افترض جهازًا له IP=192.168.0.1 والـ Subnet Mask=255.255.255.0

يمكن دمجهما في سطر واحد كما يلي:

192.168.0.1/24

حيث أن الـ 24 هي عدد الـ 1's من اليسار، وحيث أن كل 255 يتم تمثيلها في 8 من الـ 1's يكون العدد الكلي لـ 1's يساوي 24.

مثال : افترض جهاز له IP=192.168.0.1 والـ Subnet Mask=255.255.255.192

يمكن دمجهما في سطر واحد كما يلي:

192.168.0.1/26

لأن 255.255.255 بها 24 من الـ 1's و 192 بها 2 من الـ 1'sمن اليسار عند تمثيلها في النظام الثنائي (11000000) فيكون العدد الكلي لـ 1's يساوي 26.

الملاحظة الثالثة: لابد من إلمام القارئ جيدًا بعملية التحويل من النظام الثنائي إلى النظام العشري، والعكس، لكي يتمكن من القيام بعملية التقسيم، لأنه لا يتسع المجال هنا لشرح هذه العملية.

اختبار الشبكة:

المقصود باختبار الشبكة اختبار حالة الاتصال بين الأجهزة، فمثلاً لو أراد الجهاز PC1 اختبار الاتصال بالجهاز PC2 ليتأكد هل يوجد اتصال شبكي بينهما أم لا ؟ فهناك طريقتان لهذا الاختبار كما يلي :

الطريقة الأولي: عن طريق استعراض الأجهزة داخل أيقونة الـ Network Neighborhood (في Windows98)، أو أيقونة My Network Places (في WindowsXP) فإذا كان موجودًا دل ذلك على وجود اتصال شبكي بينهما، والعكس صحيح. ولكن هذه الطريقة غير دقيقة، والسبب هو أن الأجهزة داخل الشبكة يتم التعامل بينها باستخدام الـ IP، وعند استعراضها داخل أي من أيقونة الـ Network Neighborhood أو My Network Places يحدث تحويل من الـ IP إلى اسم الجهاز باستخدام الـ DNS (كما ذكرنا). وعملية التحويل هذه العملية تأخذ وقتًا، مما قد يحدث تأخيرًا في ظهور بعض الأجهزة داخل أي من الأيقونتين، أضف إلى ذلك تأخيرًا آخر وهو بحث نظام التشغيل عن الأجهزة التي قامت بإدراج الـ Service (File and Printer Sharing) ضمن نظام تشغيل الشبكة الخاص بها، هذا التأخير قد يؤدي إلى اعتقاد المستخدم بعدم وجود اتصال بتلك الأجهزة

الطريقة الثانية: وهي أدق من الطريقة الأولي، بل هي دليل قطعي على اتصال أو عدم اتصال جهازين في الشبكة. ويتم تنفيذ هذه الطريقة باستخدام أمر Ping(Packet InterNet Groper) (وهو أمر من أوامر الـ DOS)، ومعناه تلمس طريق الـ Packet وهي الرسالة. وفكرة هذا البرنامج قائمة على إرسال 4 رسائل (4 Packets) من الجهاز الذي يقوم بالاختبار إلى الجهاز الذي يقوم باختباره، فإذا قام بالرد (Reply) على الرسائل المرسلة دل ذلك على اتصاله والعكس صحيح (انظر شكل 14 في الفصل الثاني). ومن المصادفة أن أمر Ping هو الشق الأول من لعبة Ping Pong وهي تعني إرسال الكرة من لاعب (Ping) إلى لاعب آخر على الطرف المقابل ثم يعيدها اللاعب الثاني (Pong) إليه. ولما كانت كلمة Ping هي الشق الأول من الكلمة فهي تعني إرسال الكرة من الطرف الأول إلى الثاني، ثم انتظار رد منه، فقط لتعرف إذا كان هو موجودًا أم لا.

استخدام أمر Ping :

يمكن استخدام أمر Ping في جميع أنظمة التشغيل، ويمكن اختبار الاتصال بجهاز من خلال اسمه (Host Name)، أو من خلال الـ IP الخاص به. والصيغة العامة للأمر كما يلي :

Ping *Host_Name* أو Ping *IP*

مثال : الجهاز PC1 يريد التأكد من وجود اتصال شبكي بينه وبين الجهاز PC2 الذي له IP=10.0.2.2. ماذا يفعل ؟ يمكن استخدام أمر Ping كما يلي :

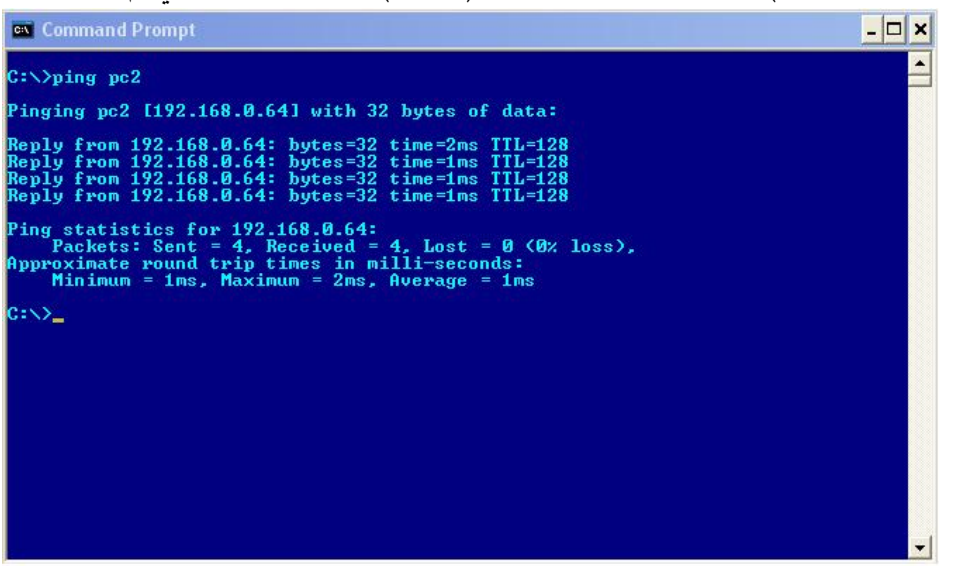
Ping PC1

أو

Ping 10.0.2.2

بعد تنفيذ الأمر تظهر نتيجته، وهناك ثلاثة احتمالات لنتيجة الاختبار :

الاحتمال الأول: أن يكون هناك اتصال وفي هذه الحالة تكون نتيجة الاختبار (كما في شكل 16) حيث تظهر بالشكل 4 ردود (Reply) على الـ 4 رسائل التي تم إرسالها

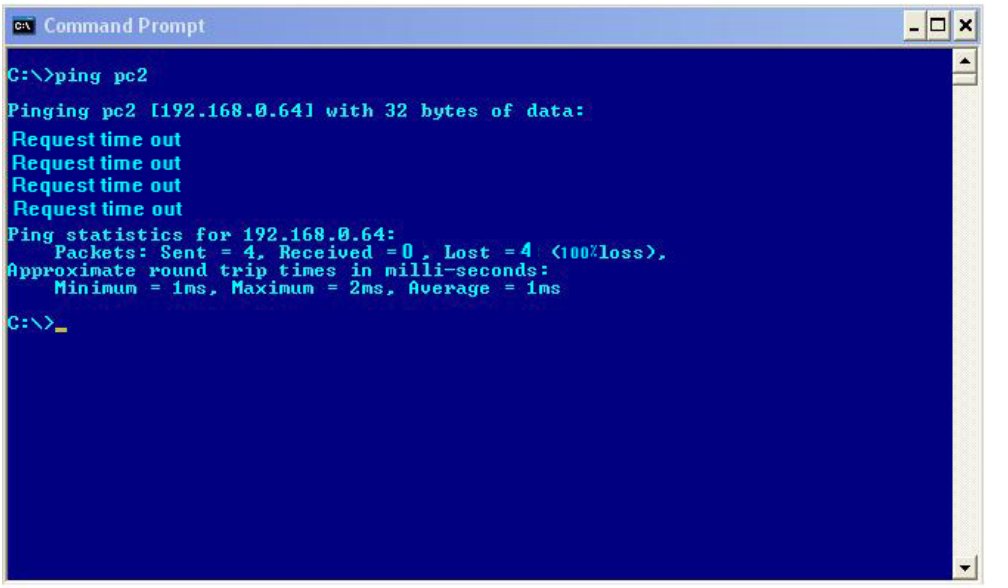


شكل رقم (16)

الاحتمال الثاني: عدم وجود اتصال لأي سبب (مثلاً قام المستخدم بكتابة اسم جهاز خطأ غير موجود بالشبكة، أو الجهاز مغلق أو عاطل ... الخ) تكون نتيجة الاختبار (كما في شكل 17)، حيث تظهر رسالة Unknown Host: أي أن هذا الجهاز غير معروف (غير متصل)

شكل رقم (17)

الاحتمال الثالث : وجود اتصال بين الجهازين، ولكن يوجد بطء بالشبكة يحول دون أن يكون هناك اتصال فعلي بينهما. وفي هذه الحالة يظهر بدلاً من الرد رسالة Request time out (كما في شكل 18) أي أن الوقت الذي من المفترض أن يرسل فيه الرد انقضى ولم يصل الرد بعد



شكل رقم (18)

ملاحظات هامة حول أمر Ping :

- عندما نقوم بتحليل السطر الأول في الاحتمال الأول، وهو Pinging pc2 [192.168.0.64] with 32 bytes of data نلاحظ أمرين :

الأمر الأول : أن البرنامج قام بتحويل اسم الجهاز PC2 إلى الـ IP الخاص به لكي يستخدمه في عملية.

الأمر الثاني : أن حجم الـ Packet المرسلة هي 32 byte وهنا لابد من توضيح أمرين: الأول أن الرسالة ليست الـ Packet ولكن الـ MTU (التي يتم تقسيم الـ Packet إليها) وقد قمنا بتوضيح ذلك (انظر شرح الـ Layers 7 في الفصل الثاني) ولكن يطلق عليها Packet، لأن الـ Packet هي الشائعة بين المستخدمين ، الأمر الثاني أن الحجم الافتراضي للـ MTU هو 32 byte، وهذا معناه أن أي Packet سيزيد حجمها على 32 byte سيتم تجزئتها إلى عدة MTU، سعة كل منها 32 byte، والأفضل للمستخدم أنه كلما زادت سعة الـ MTU كلما زادت سرعة الشبكة (أقصى سعة لـ MTU لأي شبكة هي 1500 byte)، لأنه في هذه الحالة سيقلل من عدد مرات الإرسال. والمثال التالي يوضح ذلك :

مثال : Packet سعتها 1000 byte وكانت الـ MTU=200 byte ، يكون عدد الـ MTU يساوي 5 أي أنه سيتم إرسال الـ Packet على 5 مرات ، لو كانت الـ MTU=500 كان عدد الـ MTU يساوي 2، أي أنه سيتم إرسال الـ Packet علي مرتين ، ولو كانت الـ MTU تساوي 1200 كان عدد الـ MTU يساوي 1، أي أنه سيتم إرسال الـ Packet مرة واحدة.

- عندما نقوم بتحليل أي سطر من سطور الرد في الاحتمال الأول Reply from 192.168.0.64: bytes=32 time=2ms TTL=128 ، نجد أن المقصود بـ Time الوقت الفاصل بين إرسال الـ Packet ووصول الرد، وهذا لاشك يمكن أن يعبر عن أداء وسرعة الشبكة فكلما كان هذا الوقت أصغر كلما كان أداء الشبكة أفضل ، أما TTL(Time To Live) فمعناه عدد الأجهزة التي يمكن تمر عليها الـ Packet قبل أن تفقد (أي تظل حية) وهذا الرقم تقريبًا ثابت ويساوي 128.

- سيتم الاختبار أسرع في حالة استخدام الـ IP بدلاً من اسم الجهاز، لأنه سيوفر الوقت الذي تأخذه عملية التحويل باستخدام الـ DNS من الاسم إلى الـ IP.

- قد يتساءل أحد: لماذا يقوم برنامج Ping بإرسال 4 Packets وليس Packet واحدة للاختبار؟ والجواب: لزيادة التأكيد في نتيجة الاختبار. فلو اكتفي بإرسال Packet واحدة واستلم الرد ربما لا تصل الثانية، ولكن إذا أرسل 4 واستلم الرد عليها فهذا دليل كبير على نتيجة الاختبار.

- يمكن مراقبة حالة الاتصال بجهاز في الشبكة، من خلال الاستمرار في إرسال الـ Packets واستلام الردود عليها من خلال الأمر :

*Ping –t **IP*** أو *Ping –t **Host_Name***

ويمكن إيقاف الإرسال من خلال الضغط على Ctrl+Break

فوائد فرعية لأمر Ping :

بعد أن قمنا بشرح الغرض الأساسي لأمر Ping سنوضح هنا بعض الفوائد الفرعية والتي لا تقل أهمية عن الغرض الأساسي. وهذه الفوائد كما يلي :

1. معرفة الـ IP لجهاز في الشبكة من خلال اسمه من خلال الأمر :

*Ping **Host_Name***

مثال : Ping PC2

2. معرفة اسم جهاز في الشبكة من خلال الـ IP الخاص به من خلال الأمر:

*Ping –a **IP***

مثال : Ping –a 192.168.0.64

3. تحديد أقصي قيمة لـ MTU عند الاتصال بجهاز في الشبكة من خلال الأمر:

Ping **HOST_IP_ADDRESS** *-f -l* **MTU_SIZE**

حيث أن :

HOST_IP_ADDRESS : الـ IP الخاص بالجهاز الذي نريد تحديد أقصى قيمة لـ MTU عند الاتصال به.

f- : وهو مفتاح مع برنامج Ping يعني عدم السماح للجهاز بتجزئة الـ MTU إذا كانت أكبر من إمكانياته.

l- : قيمة الـ MTU التي نريد اختبار تحديد ما إذا كانت أقصى قيمة أم لا.

والفكرة في هذا الأمر أن أحد الأجهزة يقوم بإرسال MTU بقيم مختلفة إلى جهاز آخر، مع عدم السماح له بتجزئتها إذا كانت أكبر من طاقته، ويقوم بتحليل الرد، إذا قبل الـ MTU وعمل رد

Reply نقوم بزيادة قيمة الـ MTU حتى تصل رسالة <Packet needs to be fragmented> وعندها نتوقف عن الزيادة وتكون هذه هي أقصى قيمة لـ MTU (مع العلم أن أقصى قيمة هي 1500byte)، ونقوم بإعادة إعداد البروتوكول TCP/IP ليستخدم القيمة التي وصلنا إليها بدلاً من القيمة الافتراضية وهي 32byte.

مثال : Ping 216.109.118.76 –f –l 1400

إعداد البروتوكول TCP/IP بالقيمة القصوى لـ MTU :

تتم عمل الإعداد من خلال الـ Registry ويختلف مكان الإعداد حسب نظام التشغيل

نظام التشغيل Windows98 :

- قم بفتح الـ Registry من خلال الأمر Regedit في نافذة Run
- اختر

HKEY_LOCAL_MACHINE\System\CurrentControlset\Services\Class\netTrans\000n

حيث n هي الـ Adapter المستخدم في الاتصال.

- انقر بالزر الأيمن للماوس على الجهة اليمنى.
- اختر New ->String Value.
- قم بكتابة MaxMTU، ثم ضع لها القيمة التي حددتها من الخطوة السابقة.

نظام التشغيل WindowsXP :

- قم بفتح الـ Registry من خلال الأمر Regedit في نافذة Run
- قم بالذهاب إلى

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Ndiswan\Paraeters\Proto\0

- انقر بالزر الأيمن للماوس على الجهة اليمنى واختر New->DWORD value
- قم بكتابة ProtocolMTU، ثم ضع لها القيمة التي حددتها من الخطوة السابقة.

مراقبة الشبكة :

عملية المراقبة تتم من خلال الأمر Netstat (وهو أمر من أوامر الـ DOS)، وهو عام لجميع أنظمة التشغيل. المقصود بمراقبة الشبكة، مراقبة الاتصالات التي تتم بين جهاز ما وباقي

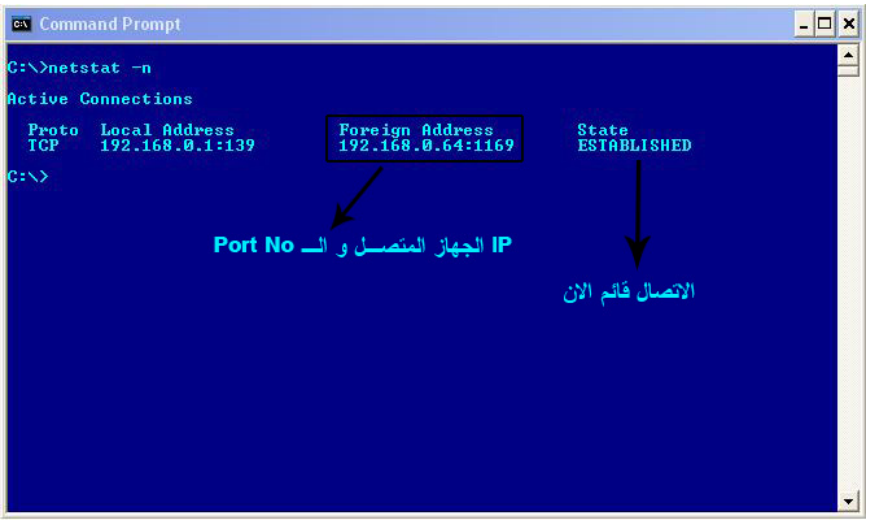
أجهزة الشبكة. والسؤال الآن: كيف تتحقق المراقبة؟ والجواب: المراقبة تحقق من خلال معرفة عنوان المتصل. وهناك سؤال آخر وهو: ما هو عنوان المتصل؟ والجواب: الذي سيجيبه البعض هو: الـ IP وهذا الجواب ناقص، لأن الـ IP جزء من العنوان وليس العنوان كله ، فالـ IP يكفي فقط لوصول الرسالة إلى الطرف الآخر، ولكن في أي تطبيق سيتم فتح الرسالة (Application Layer) ؟ إذن لابد أن يشمل العنوان اسم التطبيق الذي سيتم فتح الرسالة به. وهنا سنواجه مشكلة وهي: كيف يتم دمج اسم التطبيق وهو نص مع الـ IP وهو رقم ؟ والحل: في تعيين أرقام لجميع التطبيقات وتمت تسمية هذا الرقم الخاص بالتطبيق الـ Port No أو رقم البوابة ويتم تمثيل الـ Port No في 16-bit (أي أنه يمكن للشبكة إدارة 65536 تطبيقًا) والسبب في تسميته تلك أن كل تطبيق يجلس خلف باب Port له رقم معين (رقم التطبيق) يتنصت Listening على وصول رسالة تحمل نفس رقمه، فإذا وصلت قام بفتح الباب Port وفتح الرسالة، وعليه فإن عنوان أي جهاز في الشبكة هو IP+Port No. ويكتب على الصورة IP:PortNo وتكون سعة العنوان الآن هي 48-bit (32bit لـ IP + 16 لـ Port No) (انظر شكل 15 في الفصل الثاني تجد أن عنوان الأجهزة Source Address و Destination Address يتم تمثيلها بـ 48bit).
والآن سنوضح عملية المراقبة من خلال المثال التالي :

مثال : افترض أن الجهاز PC2 الذي له IP=192.168.0.64 قام بالدخول على الجهاز PC1 الذي له IP=192.168.0.1، وأراد الجهاز PC1 معرفة بيانات الأجهزة المتصلة به من خلال الأمر Netstat كيف ؟

الجواب :

1. الخروج إلى DOS من خلال اختيار Start->All Programs->Accessories->Command Prompt أو كتابة الأمر Command في نافذة Run (في Windows98 اختر Start->Program->MS-Dos Prompt)
2. كتابة الأمر Netstat -n ، فتظهر بيانات المتصلين (كما في شكل 19) في صف واحد به 4 أعمدة: **العمود الأول** خاص بالبروتوكول المستخدم في الاتصال وهو الـ TCP (البروتوكول الخاص بطبقة الـ Transport Layer في البروتوكول TCP/IP)، **والعمود الثاني** Local Address هي بيانات الجهاز PC1 الذي يريد مراقبة الاتصال، **والعمود الثالث** Foreign Address هو ما يهمنا حيث يوجد به الـ IP للجهاز المتصل (PC2) وكذلك الـ Port No وهو رقم التطبيق الذي يقوم بفتحه في الجهاز PC1 (192.168.0.64:1169)، **والعمود الرابع** State وهو يوضح حالة الاتصال، وقد يكون

احتمالاً من اثنين: الأول إما Listening أي في حالة تنصت، ولم يتم الاتصال بعد، أو Established ويعني أن الاتصال قائم الآن (وهو الذي يظهر بالشكل)

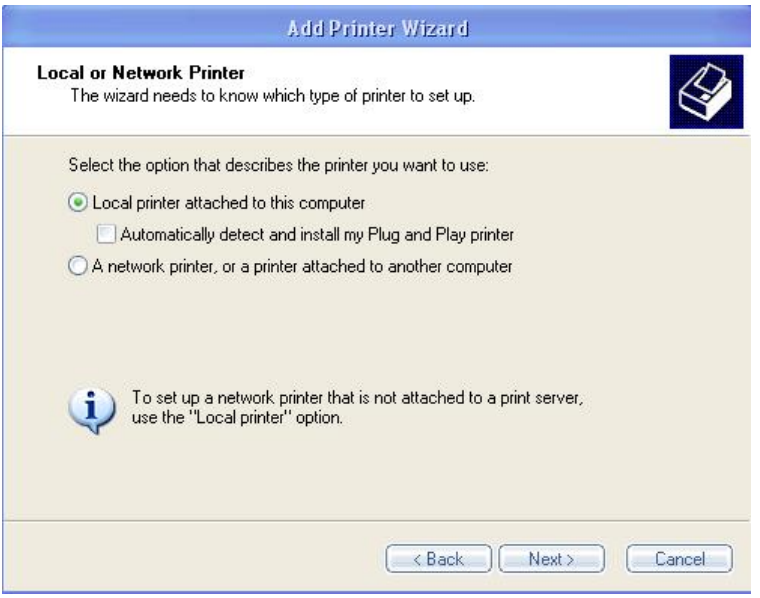


شكل رقم (19)

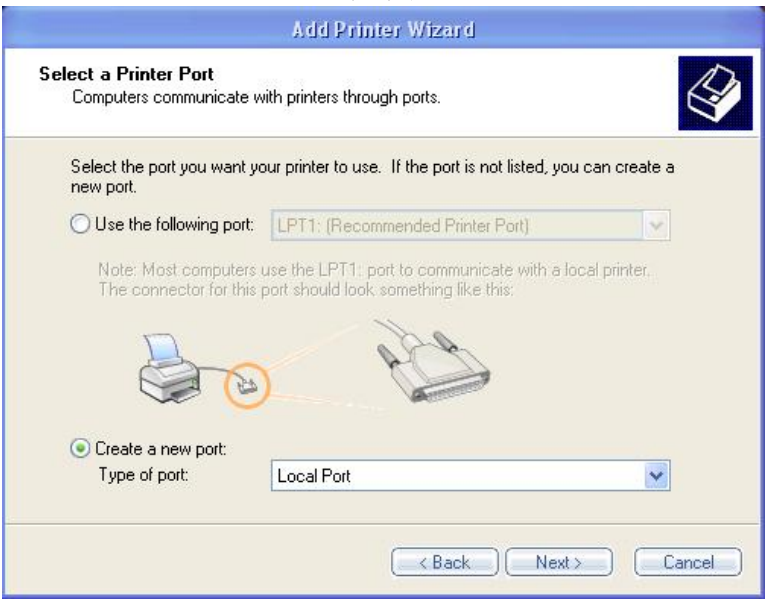
تثبيت طابعات الـ TCP/IP :

نوهنا على تثبيت طابعات الـ TCP/IP في الفصل الرابع عند إعداد WindowsXP ولم نقم بعملية التثبيت لأنها كانت مرتبطة بالبروتوكول TCP/IP والذي لم نكن قد قمنا بشرحه. وحيث أننا الآن قد تعرفنا عليه فسنقوم بشرح عملية التثبيت لهذه الطابعات.

- قم بالذهاب إلى مجلد الطابعات من خلال اختيار Start->Printers and Faxes.
- قم بالنقر على الارتباط Add New Printer.
- حدد الخيار Local Printer، وقم بإلغاء تحديد الخيار Automatically detect and Install my plug and play printer (كما في شكل 20)، ثم اضغط Next
- قم بتحديد الخيار Create New Port، ثم قم باختيار Standard TCP/IP Port من القائمة (كما في شكل 21) ثم اضغط زر Next.
- يظهر معالج إضافة الطابعة ، اضغط زر Next.

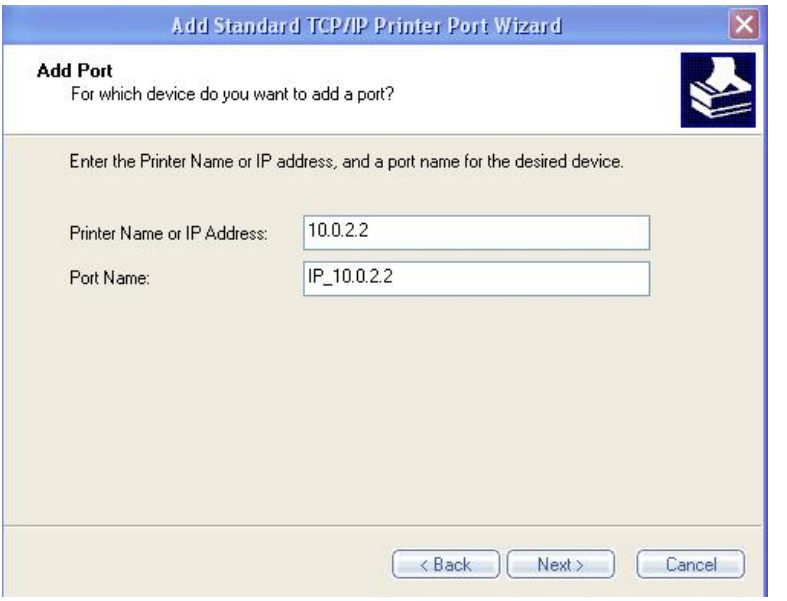


شكل رقم (20)



شكل رقم (21)

☜ يظهر نموذج بيانات الطابعة. قم بإدخال الـ IP الخاص بالطابعة في حقل Printer Name or IP Address، واترك حقل الـ Port Name حيث سيتم تحديثه تلقائيًا (كما في شكل 22)



شكل رقم (22)

☜ أكمل المعالج حتى النهاية