



# Certified Network Engineer

منهج شهادة مهندس الشبكات المعتمد

تعلم بناء الشبكات وإدارتها في هذا المنهج المعتمد

تغطية شاملة لأسئلة الإختبار

احصل على شهادتك دون عناء

**Your Key To Pass ACNE Exam**

By  
M. El-Guindy  
Founder & CIO  
ASK PC, LLC  
Alpharetta, GA  
USA.  
[www.askpc.org](http://www.askpc.org)

## ACNE Study Guide

### Author

Mohamed N. El-Guindy  
BSc. CS. Trinity University, USA  
MCSE, MCT  
IEEE Computer Society Member  
British Computer Society Member  
IWA & HWG Member  
Member of Experts Exchange  
Member of E-Learning Guild  
Member of WAOE  
Listed in "Marquise Who's Who in the World 2007 Publication" by invitation.  
Chief Information Officer  
ASK PC, LLC  
Alpharetta, GA  
USA

### ASK-PC

The Largest Arabic Technical Support Community in association with  
Microsoft  
Symantec  
Winternals  
Sysinternals

ASK PC, LLC is a registered legal name in United States of America.

### Dedication:

This work is dedicated to my great wife for her continues support.

Contact the Author

[admin@ask-pc.com](mailto:admin@ask-pc.com)

[naguib@computer.org](mailto:naguib@computer.org)

This book is protected by international copyright law  
Copyright © 2006 [www.askpc.org](http://www.askpc.org)



بسم الله الرحمن الرحيم

## تقويم

كتاب المنهج الدراسي الخاصة بشهادة "مهندس الشبكات المعتمد" أو ACNE

هذا الكتاب يضم المادة الاساسية التي تساعدك على اجتياز اختبار شهادة مهندس الشبكات المعتمد من ASK PC والتي تتخذ من الولايات المتحدة الأمريكية مقرا لها وهي تقدم هذا المنهج لينتج للدارسين العرب او المتحدثين باللغة العربية الحصول على شهادة معتمدة من الولايات المتحدة ومعترف بها دوليا في مجال الشبكات وما يتعلق بها.

الكتاب يغطي جميع جوانب التخصص من البداية حتى الاحتراف كما يعد مرجعا لا غنى عنه لمن يريد ان يستفيد او ينمي مهاراته في مجال شبكات الكمبيوتر وقد قررنا ان نقدم جميع مناهجنا باللغة العربية نظرا للمصاعب التي تواجه الكثيرين في فهم المناهج الخاصة بعلوم الكمبيوتر باللغة الانجليزية مع المحافظة ايضا على مصطلحات المنهج باللغة الانجليزية لكي تستفيد الاستفادة القصوى وايضا لكي لا نضعف القيمة العلمية للمنهج المتخصص.

يفترض بك كدارس لمنهج مهندس الشبكات ان تكون على دراية باساسيات الكمبيوتر التي لن نتطرق لها تفصيلا في هذا المنهج حيث سيركز المنهج على الاشياء العلمية التي يحتاجها الدارس وايضا يتعرض لاهم المشكلات الخاصة بالشبكات وحلولها بالطرق المتعارف عليها من قبل الخبراء. ويفضل ان تكون ملما بمنهج ACTSP او ACTSE في الاكاديمية او حاصل على اي من الشهادات السابقة لكي تتمكن من فهم المنهج بسهولة.

فلهذا تتشرف اكااديمية الكمبيوتر في الولايات المتحدة بطرح هذا المؤلف بين ايدي دارسيها لاجتياز اختبار شهادة مهندس الشبكات المعتمد بنجاح.



## ما معنى ACNE؟

هذه هي الشهادة المقدمة من اكااديمية الكمبيوتر في ASK PC بالولايات المتحدة الامريكية كدليل على اجتيازك لاختبار مهندس الشبكات او Certified Network Engineer المعتمد من مؤسستنا المسجلة في امريكا والتي تصدر شهادات معترف بها دوليا و العضو في اكبر المنظمات العالمية المتخصصة وايضا تتمتع بشراكة مع العديد من بيوت الخبرة العالمية مثل Microsoft. وهذه الشهادة تختص بالشبكات السلكية فقط والتقنيات المتعلقة بها.

## حقوق الملكية الفكرية:

طبقا لحقوق الملكية الفكرية التي تحمي هذا المؤلف والتي تم تسجيلها في مكتبة الكونجرس في الولايات المتحدة الامريكية وفي الدول التي تخضع لاتفاقية برن فان هذا الكتاب جزء لا يتجزأ من موقعنا المسجل تحت قوانين حماية الملكية الفكرية ولهذا فان هذا المنهج للاستخدام داخل الموقع والاكاديمية فقط ولا يجوز نسخه او توزيعه او تحميله او تبادله مع الاخرين او نقل جزء منه باي وسيلة كانت مقروءة او اليكترونية حالية او ستطرا بعد الا باذن مسبق الشركة والمؤلف ومن يخالف ذلك يعرض نفسه للمسائلة القانونية امام المحاكم الدولية فيما يخص حقوق الملكية الفكرية في الولايات المتحدة الامريكية وحول العالم. وايضا العلامات التجارية و البرمجيات الواردة في هذا الكتب ملكية خاصة لاصحابها ومحمية بموجب القوانين الدولية.

## Network Fundamentals

### مبادئ الشبكات

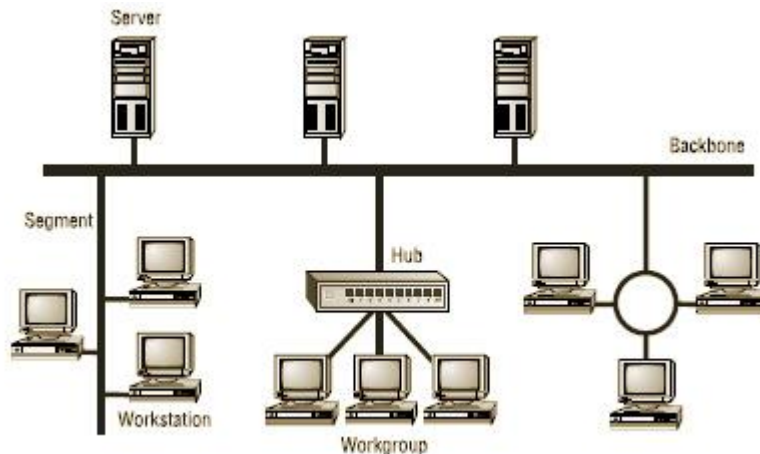
سوف نتعرف في هذا الجزء من المنهج كما هي البداية دائما بالتعرف على الاساسيات وبما ان موضوع الشبكات من اكثر الموضوعات تشويقا وايضا تعقيدا في تكنولوجيا المعلومات فلا بد ان نتعرف على اساسيات هذا الموضوع فسوف نتعرف على انواع الشبكات والكوابل المستخدمة واساسيات التشبيك والربط بين الأجهزة على الشبكات المختلفة.

### Network Elements

كما هو معلوم لدى الجميع بأن جهاز الكمبيوتر في حد ذاته اداة قوية جدا لمعالجة البيانات باشكال لا تحصى ولا تعد وكأمر طبيعي إذا تم توصيل هذه الأجهزة فائقة القدرة ببعضها البعض سوف تصبح اكثر قوة على وقدرة على اداء المهام المختلفة وتعد هذه هي الفكرة الاساسية في توصيل الأجهزة عبر الشبكات المختلفة Networking والشبكة تتكون من عدة مكونات او عناصر تسمى Elements والتي سوف نتعرف عليها في الفقرات التالية.

### Local Area Network (LAN)

من اكثر انواع الشبكات انتشارا تسمى الشبكات المحلية LAN والشبكات المحلية محصورة بمكان محدد لا تتعداه مثل مبنى معين او مصنع او مكتب وهناك شروط معينة في الشبكات المحلية منها ان المسافة ما بين الكمبيوتر او ما يسمى Node في الشبكة وبين جهاز التوصيل مثل Hub او Switch لايجب ان تتعدى الـ 185m وليس اكثر من 30 كمبيوتر إلا ان التقنيات الآن قد اختلفت ويمكن زيادة هذه المسافة وايضا عدد الأجهزة.



## Wide Area Network (WAN)

هذا النوع من الشبكات هي الشبكات الواسعة الإنتشار وهي التي تعبر المسافات الكبيرة ما بين المدن والبلدان مستخدما طرق أخرى في الإتصال والكثير من المستخدمين هم جزء من شبكة كبيرة WAN إذا ما استخدموا الإنترنت حيث يعتبر الإنترنت اكبر شبكة WAN على الأرض! وتختلف الـ WAN عن شبكات الـ LAN بما يلي:

- الـ WAN تغطي مساحات شاسعة اكبر من LAN
- سرعة نقل البيانات عبر شبكات LAN اسرع من شبكات WAN
- تتكون الـ WAN من العديد من شبكات الـ LAN المتصلة ببعضها البعض

## Workstation

لكي تكون ملما بالشبكات الماما جيدا فلا بد ان تعي جيدا معنى هذه الكلمة، وتعنى Workstation جهاز كمبيوتر متصل بالشبكة مباشرة قد يكون جهازا ذا مواصفات عالية او مواصفات اعتيادية إلا ان الكلمة تطلق على اي جهاز كمبيوتر متصل بالشبكة وهناك مصطلح آخر يطلق على جهاز متصل بالشبكة وهو Client ويعرف بانه اي جهاز على الشبكة يستخدم Resources ولكن ضع في اعتبارك بأن اي Workstation قد يكون Client إلا انه ليس كل Client هو Workstation بمعنى ان الطابعة Printer على سبيل المثال تعتبر Client إلا انها لا تعتبر Workstation.

## Servers

هو جهاز معناه كما هي الترجمة "الخادم" بالفعل هو يقوم بخدمة باقي الأجهزة او Workstations على الشبكة إلا ان الـ Server هو جهاز بالكاد ذو امكانيات عالية مثل Multiprocessors او RAID Technology والكثير من الإمكانيات التي يجب توافرها في هذا الجهاز وهو ايضا يستخدم نظام تشغيل مخصص مثل Windows 2003 Server ولكن من المحبذ تخصيص Server او خادم لكل وظيفة على الشبكة للحصول على اداء ومن هنا نشأت مسميات أخرى او انواع أخرى للـ Servers كما يلي:

- File Server:** يستخدم لتخزين الملفات على الشبكة
- Print Server:** يستخدم لأداء امور الطباعة وما يتعلق بها على الشبكة
- Proxy Server:** يقوم بأداء وظيفة متعلقة بأجهزة أخرى على الشبكة
- Application Server:** يستخدم لتخزين البرمجيات المستخدمة على الشبكة

**Web Server**: يستخدم لإستضافة المواقع وصفحات الإنترنت على الشبكة  
**Mail Server**: يستخدم للتعامل مع البريد على الشبكة بين الأجهزة المختلفة  
وهناك العديد من الـ Servers التي يمكن اضافتها للشبكة كلما دعت الحاجة

### Hosts

الـ Host هو مصطلح او مسمى يطلق على اي جهاز على الشبكة يتعامل مع TCP/IP ولهذا فإن جميع الأجهزة على الشبكة طالما انها تتعامل بـ TCP/IP فهي جميعها Hosts

### Peer To Peer Network

يستخدم هذا المصطلح للتعبير عن الشبكات التي يشارك فيها كل كمبيوتر موارده مع مجموعة اخرى من الأجهزة على الشبكة ويمكن لكل جهاز على منفردا اي Peer التحكم في الـ Resources الخاصة به من حيث دخول الأجهزة الأخرى والمستخدمين عليها ام لا. وكل جهاز من الأجهزة على الشبكة قد يكون Client على الشبكة يطلب ملفات او خدمات من جهاز الخادم او الـ Server وكل جهاز على هذه الشبكة هو جهاز خاص بمفرده او مسؤولية من يعمل عليه. وانظمة التشغيل على الأجهزة ايضا يمكن ان تختلف من جهاز للأخر.

### Client/Server Network

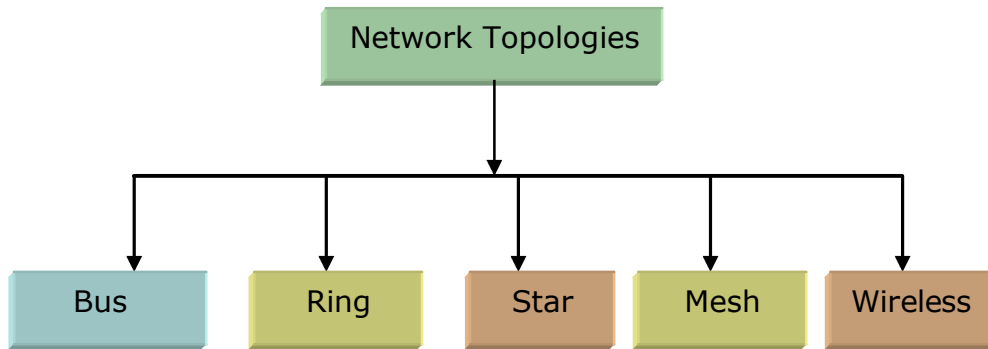
هذا المصطلح يطلق على الشبكات التي تعتمد على خادم Server وهي اكثر تنظيما من شبكات الـ Peer لوجود خادم مركزي يقوم بعملية التنظيم المركزية للشبكة Centralized Administration إلا ان إدارة هذا النوع من الشبكات اكثر تعقيدا من النوع السابق. وايضا امن المعلومات على هذا النوع اعلى بكثير من شبكات الـ Peer لوجود معلومات الأمن او Security على قاعدة بيانات ويتحكم فيها جهاز واحد. ولها من الخواص الكثير سوف نتعرف عليه لاحقا.



## Physical Network Topologies

### تخطيط الشبكات

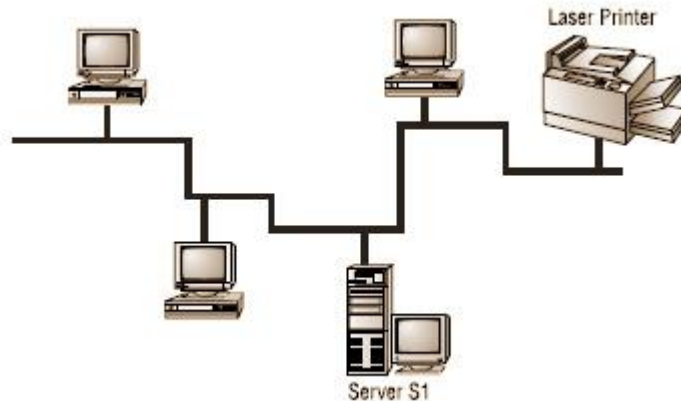
في هذا الجزء من المنهج سوف نتعرف تخطيط الشبكات على ارض الواقع والتي تعتبر من اهم النقاط التي يجب ان تكون ملما بها كخبير للشبكات وسوف نتعرف على طرق تشبيك الشبكات والأجهزة والكوابل والأدوات المستخدمة في هذا الأمر. تخطيط الشبكات ينقسم إلى عدة انواع هامة جدا سنتعرف عليها تفصيلا كما يلي:



### Bus Topology

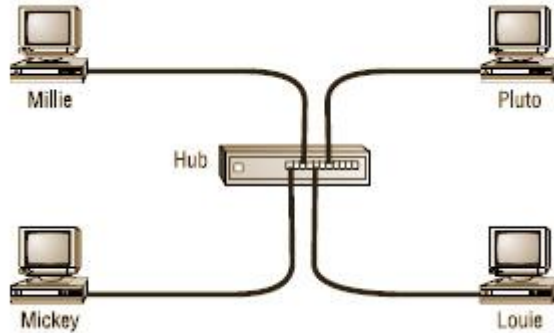
هذا النوع من التخطيط او التشبيك يعتمد على كون الأجهزة على الشبكة متصلة بكابل واحد ممتد على طول الشبكة وهذا الكابل يتم وضع ما يسمى Terminator في نهاياته الطرفية وهذا النوع من الشبكات تركيبه سهل إلا ان مشاكله كثيرة نظرا لوجود كابل واحد للشبكة ككل.

راجع منهج شهادة CTSE



## Start Topology

التخطيط من نوع Star هو من اكثر التخطيطات انتشارا وشيوعا في الـ LAN نظرا لسهولة

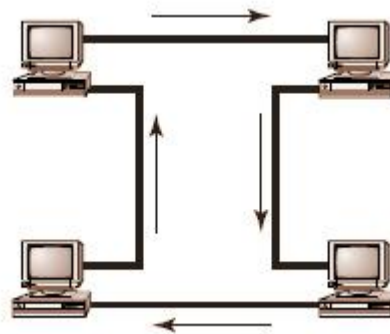


تركيبه وسهولة عمل Troubleshoot او صيانة له وايضا الكثير من الميزات العملية مثل عدم حدوث مشكلة في الشبكة ككل عندما تحدث مشكلة في جهاز منفصل وايضا تتمتع بما

يعرف بـ Centralized Switching وهو وجود جهاز مركزي مسؤول عن توصيل الأجهزة داخل هذا التخطيط ببعضها البعض وايضا سهولة اضافة جهاز لهذا التخطيط.

## Ring Topology

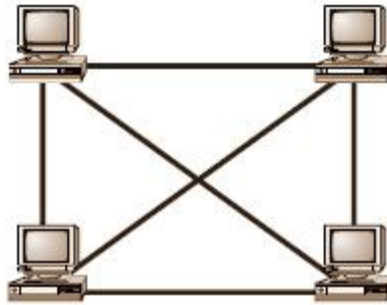
هذا النوع من التخطيط يعتمد على توصيل كل جهاز على شبكة بجهازين آخرين على الشبكة مباشرة وتتحرك المعلومات او Data في اتجاه واحد فقط عبر الكوابل ومن اهم عيوبها هو ان اي جهاز تحدث به مشكلة سوف يتسبب في احدثات مشكلة في الشبكة ككل ووقوعها!



وتعد مسألة صيانة هذا النوع من الشبكات وادارته من اعقد ما يمكن ولهذا فهو غير شائع في استخدامات التشبيك على ارض الواقع او مايعرف باسم Physical Topologies

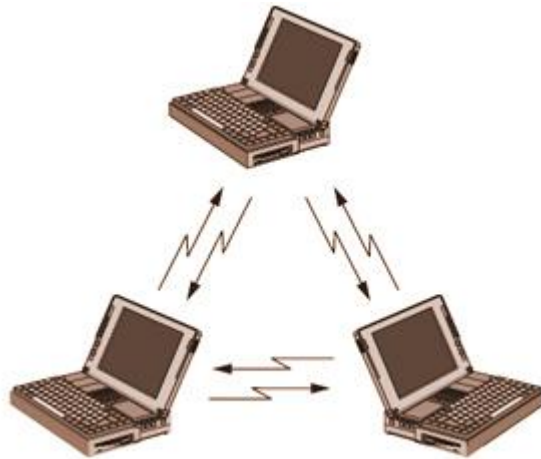
## Mesh Topology

هذا النوع من التشبيك او التخطيط يعتمد على ان كل جهاز على الشبكة متصل مباشرة بجميع الأجهزة الاخرى على الشبكة بكوابل خاصة وهذا النوع من التخطيط غير شائع مطلقا في الشبكات المحلية LANs إلا انك قد تجد بعض تطبيقاته في الـ WANs ولكن ليس بالتفصيل فلن تجد جهاز متصل بجميع الأجهزة على الشبكة او بجميع النقاط على الشبكة. وهي من اعقد انواع التشبيك ايضا ومسألة ادارة وصيانة هذه الشبكات مزعجة جدا نظرا لتشعب الاسلاك والكوابل كما سترى في الشكل التالي



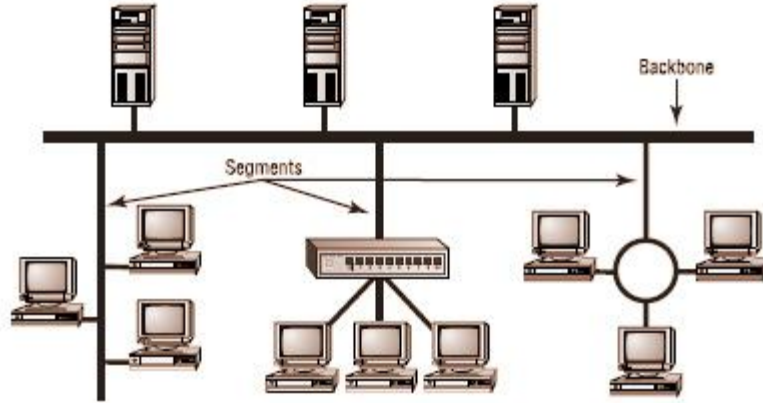
## Wireless Topology

هذا النوع من التشبيك من احدث انواع التشبيك هذه الايام وهو يعتمد على التقنيات اللاسلكية مثل تقنية RF او Radio Frequencies وهذه الشبكات من الممكن ان تجدها منفصلة كشبكة مستقلة او جزء من شبكة اخرى سلكية.



## Segments & Backbone

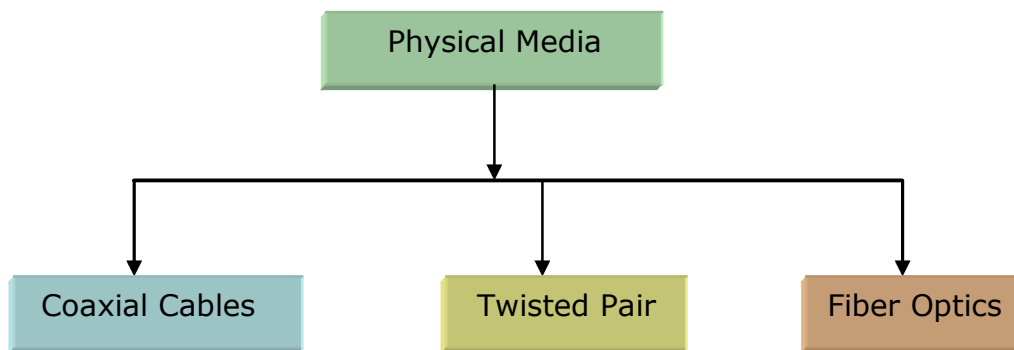
من اهم الاشياء في الشبكات هي كيفية ربط اجزاء الشبكة ببعضها بالأخص عندما تكون الشبكة كبيرة ومتشعبة فكل جزء منفصل من الشبكة يسمى Segment او شريحة وكل هذه الـ Segments يتم ربطها بما يسمى Backbone وهو وصلة عالية السرعة مثل Fiber Optics او Fast Ethernet



ويجب ان تضع في الاعتبار ان الـ Servers هي التي يتم توصيلها مباشرة على الـ Backbone للحصول على اقصى قدر من الأداء اما الـ Workstation فيتم توصيلها بالـ Segments كما هو امامك في الشكل السابق.

## Physical Media

يشار إلى هذا المصطلح بالكوابل المستخدمة في توصيل الشبكات او بتوثيل الأجهزة على الشبكة، وعلى الرغم من انتشار الشبكات اللاسلكية واستخدامها لتقنيات مختلفة في الإتصال بلا اسلاك او كوابل إلا ان الشبكات السلكية تستخدم عدة انواع من الكوابل سوف نتعرف عليها في الجزء التالي من المنهج.



## Coaxial Cables

هذا النوع من الكوابل يشبه إلى حد كبير الكوابل المستخدمة في وصلات التلفزيون أو الـ Satellites ويطلق عليها اختصاراً Coax وهي تعتمد على جزء نحاسي في المنتصف داخل جزء بلاستيكي ومن فوقه جزء معدني آخر مكسو بالبلاستيك أو PVC

وهذه الكوابل لها نهايات طرفية خاصة لتوصيلها بكرات الشبكة وإيضاً كرات الشبكة لابد أن يكون مجهز لتوصيل هذا النوع من الكوابل والتي ترتفع تكلفتها عن الكوابل الأخرى المستخدمة.



والـ Connectors المستخدمة في توصيل هذه الكوابل تسمى BNC connectors وهي Male و Female. إلا أن هذه الأنواع من الكوابل يحدث بها ما يسمى Signal Bounce أو ارتداد الإشارة مرة أخرى من نهاية الـ Cable إلى داخله مرة أخرى ولهذا فهي تحتاج إلى Terminators في النهاية لإمتصاص هذه الإشارات حتى لا تنعكس مرة أخرى في الكابل وتؤدي إلى مشاكل كبيرة في الشبكة وفقد للمعلومات والتوصيل.

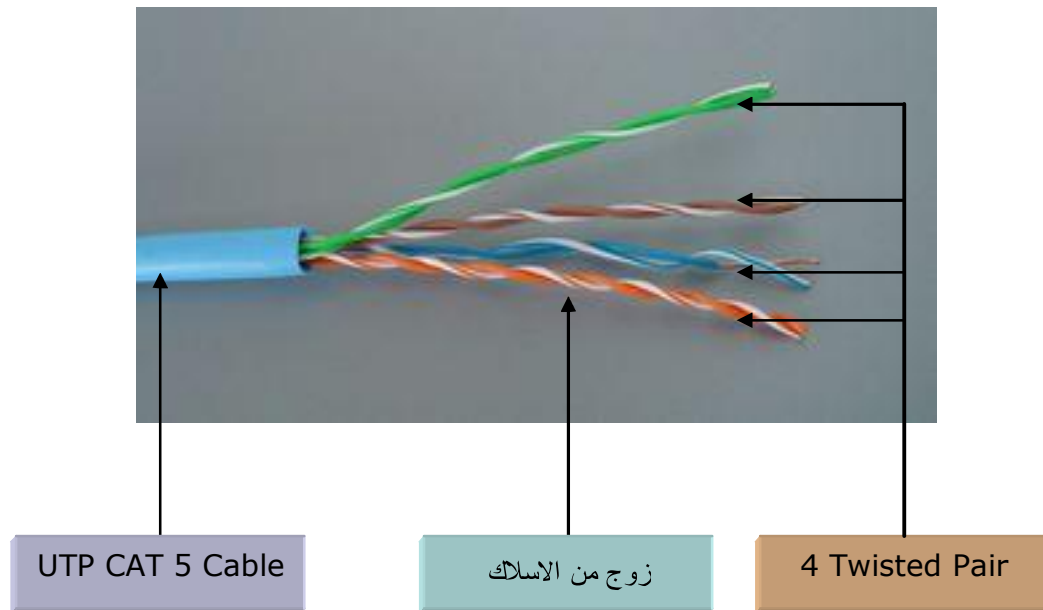




## Twisted Pair Cables

هذا النوع من الكوابل هو الأكثر شيوعا هذه الايام وهو عبارة عن مجموعة من الأزواج من الأسلاك Pairs يتكون منها الكابل الاساسي منها ما يتكون من زوجين او زوج او اكثر حسب النوع وهذه الكوابل تنقسم إلى قسمين UTP او Unshielded Twisted Pair وهي الكوابل الغير معزولة وهي مستخدمة اكثر في شبكات Star وهناك النوع الثاني وهو STP او Shielded Twisted Pair ويستخدم اكثر في شبكات Token Ring والكوابل لها فئات وانواع مختلفة تعرف باسم CAT اختصارا لـ Category وسوف نتعرف عليها فيما يلي:

- CAT 1:** يتكون من 4 اسلاك او زوجين Two Twisted Pair وهو غير مناسب لنقل المعلومات او Data Communication وهو غالبا يستخدم في الـ Voice مثل التليفونات.
- CAT 2:** 8 اسلاك او اربع أزواج من الاسلاك 4 Twisted Pair وهو صالح لنقل 4Mbps
- CAT 3:** 8 اسلاك او اربعة أزواج من الاسلاك 4 Twisted Pair صالح لنقل 10Mbps
- CAT 4:** 8 اسلاك او اربعة أزواج من الاسلاك 4 Twisted Pair صالح لنقل 16Mbps
- CAT 5:** 8 اسلاك او اربعة أزواج من الاسلاك 4 Twisted Pair صالح لنقل 100Mbps
- CAT 6:** 8 اسلاك او اربعة أزواج من الاسلاك 4 Twisted Pair صالح لنقل 1000Mbps



وسوف نتعرف على كيفية تركيب هذه الكوابل لاحقا في المنهج.

وتستخدم مقابس من نوع RJ-45 حيث يتم تركيبها في نهايات الكابل وكلمة RJ هي اختصار  
Registered Jack وتستخدم التليفونات وشبكات نقل الصوت من نوع CAT 1 مقابس من  
نوع RJ-11 .



### Ethernet Cable Description

وصف انواع الكوابل المستخدمة في تشبيك شبكات Ethernet سوف نتطرق إلى هذا الأمر  
لانه يقابلك في اي تعامل لك مع الشبكات هل رأيت هذا الكود على احد الكوابل او في اي  
كتيب يهتم بالشبكات 100BaseT ؟  
بالتأكيد رأيته ولكن ماذا يعني؟

هذا هو ما يسمى الوصف الكودي للكوابل المستخدمة ويعبر عنها بمعادلة بسيطة تدعى

**N<signal>X**

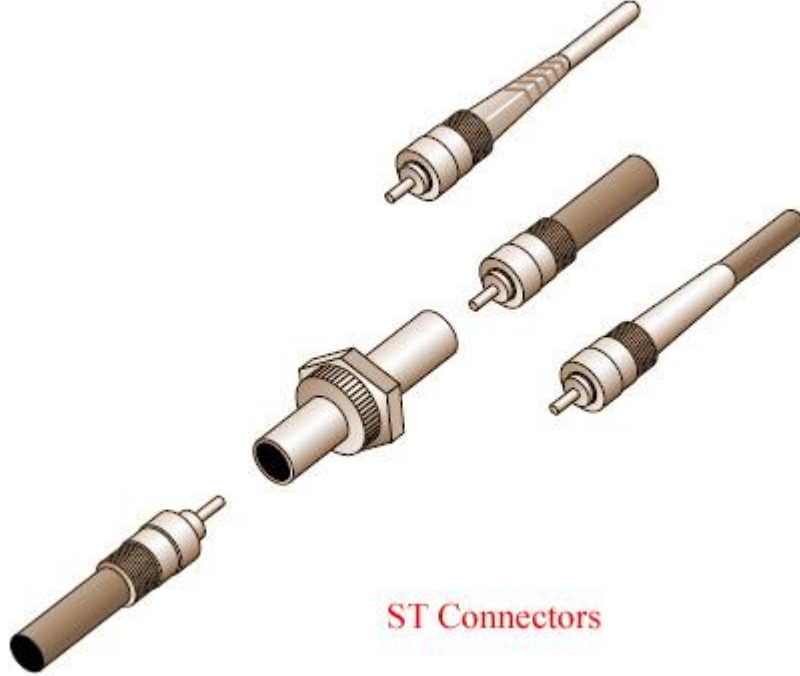
وتعنى عموما ما يلي N هو سرعة الكابل اي 100 Mega bit/ second على سبيل المثال  
اما Signal فهو يعبر عن نوع الإشارة المستخدمة داخل الكابل هل هي Base والتي تعني  
Baseband او Broad والتي تعني Broadband اما الـ X فهي غالبا تعني مواصفة معينة  
للكابل تختلف ما بين الكوابل وهي خاضعة لتقنين المعهد الأمريكي للهندسة IEEE.

### 100BaseT

هي تقنية الكوابل التي تدعم سرعة نقل بمعدل ١٠٠ ميجا بت في الثانية الواحدة وحرف الـ  
T طبقا لتعرف الـ IEEE فهي Twisted Pair

## Fiber-Optic Cables

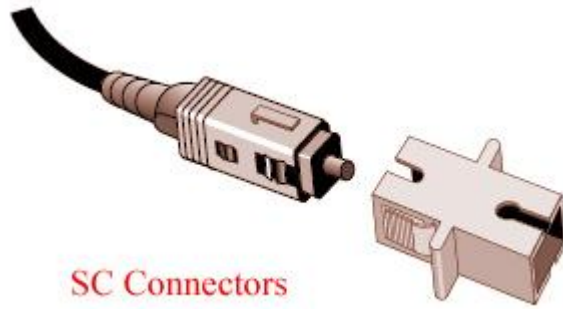
هذا النوع من الكوابل باهظ الثمن وتستخدم هذه الكوابل تقنية نقل البيانات باستخدام الضوء ولهذا جاء المسمى بالاليف الضوئية او Fiber Optics.



ST Connectors

وتستخدم هذه الكوابل مقابس توصيل اشهرها ST Connectors او Straight Tip Connectors و SC Connectors او Subscriber Connector

ويجب ان تضع في الحسبان ان هذا النوع من الكوابل يستخدم لنقل البيانات عبر عدة كيلومترات وليس مترات كما في كوابل CAT5 ومثيلاتها فهو يعتمد على سريان الضوء في الكابل وانعكاسه لمسافات طويلة تعتمد على



SC Connectors

نوع الكابل قد تصل إلى ٤ كيلومترات إلا انه كما ذكرنا صعوبة التركيب وباهظة التكاليف وتستخدم عادة في عمل الـ Backbone وايضا التوصيل ما بين المباني والأماكن البعيدة عن بعضها البعض والتي لن تستطيع توصيلها بـ UTP Cables او حتى بالـ Coaxial.

## Network Connectivity Devices

### أجهزة التوصيل في الشبكات

في هذا الجزء من المنهج سوف نحاول ان نتعرض لأهم الأجهزة التي تستخدم في الشبكات وطريقة عملها مثل الـ Routers, Switches والكثير من الاجهزة الاخرى التي تراها في الشبكات.

### NIC

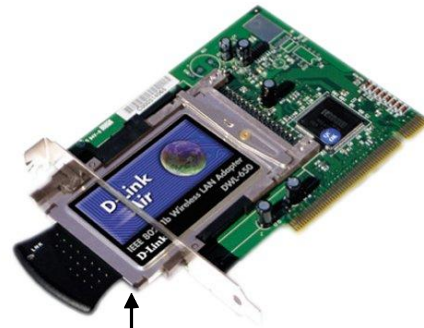
هذا هو اهم جزء واول جزء لابد ان نتعرف عليه الا وهو Network Interface Card اختصارا NIC وهو كارت الشبكة الذي يتم تركيبه في جهاز الكمبيوتر لتوصيل كابل الشبكة به ومن ثم توصيه بالنقطة المركزية Switch او Hub إذا كنت تستخدم Start Topology



وهذه الايام اغلب اللوحات الرئيسية Motherboards في الأجهزة الحديثة تأتي مدعومة بـ Built-in Ethernet Card او كروت شبكة عليها مباشرة فتغنيك عن شراء كارت شبكة منفصل وغالبا تأتي هذه الكروت بسرعات تتراوح ما بين 10/100 Mbps و 1000Mbps



Wireless NIC



PCMCIA NIC

## Hub

هذا الجهاز من اشهر الأجهزة التي تستخدم في شبكات الـ Ethernet وبالتحديد Star Topology وهو النقطة المركزية التي يتم تجميع فيها الكوابل التي يتم توصيل الاجهزة بها عبر الشبكة إلا ان الـ Hub يقوم بارسال المعلومات التي تخرج من الجهاز الـ Sender إلى جميع الـ Ports للأجهزة الـ Receivers دفعة واحدة.



## Switch

هذا الجهاز يقوم بنفس عمل الـ Hub ويقوم ايضا بربط الشبكات الصغيرة ببعضها بالشبكة الأكبر إلا انه يختلف عن الـ Hub بأنه يقوم بعمل ما يسمى Direct Link ما بين الجهاز الـ Sender والجهاز الـ Receiver على عكس الـ Hub الذي يقوم بإرسال الإشارة إلى جميع الأجهزة على الشبكة مما يؤدي إلى بطء الشبكة ولهذا الـ Switches اسرع بكثير.

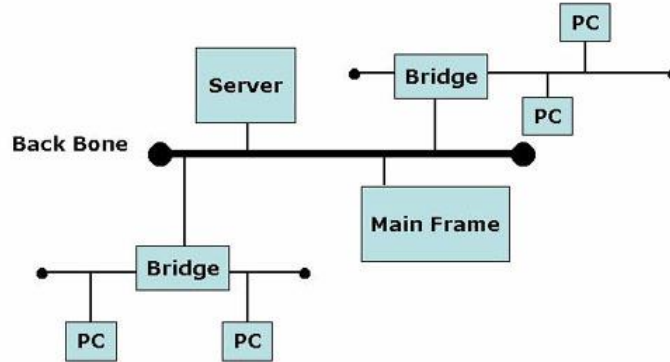




## Bridges

تستخدم هذه الأجهزة أما لتوصيل شريحتين من الشبكة ببعضهما البعض أو 2 Segments أو تستخدم لتقسيم الشبكات الكبيرة إلى شبكات أخرى أصغر لتقليل الـ Traffic.

### Back Bone



## Router

يستخدم هذا الجهاز في توصيل الشبكات الغير متشابهة ببعضها البعض أو ما يطلق عليها dissimilar networks على سبيل المثال يمكنك استخدام الـ Router لتوصيل شبكتك المحلية LAN بشبكة أخرى أكبر WAN أو بالإنترنت.



## Gateways

تستخدم هذه الأجهزة أيضا في الربط ما بين الشبكات غير المتوافقة إلا أنه أكثر أجهزة الشبكات تعقيدا لأنها عبارة عن Hardware و Software معا وقد يمكنك استخدامها للإتصال من LAN مثلا بـ Mainframe وهما مختلفان تماما حتى في أسلوب الإتصال. وهناك امثلة مختلفة للـ Gateway مثل Email Gateway والذي يتيح الإتصال مع .Email Servers

## Modems

بالتأكيد سمعت عن هذه الأجهزة وهي المسؤلة عن اتصالك بالإنترنت ومن امثلة هذه الأجهزة ADSL Modems و ISDN Modems

## CSU/DSU

اختصارا ترمز إلى Channel Service Unit و Data Service Unit وهي اجهزة توجد في الأماكن المتصلة بـ T Series data Connections مثل T1 Line وهي في الغالب جهازين في جهاز واحد وحاليا توجد هذه الأجهزة ضمن اجهزة الـ Router الحديثة المخصصة للإتصال بـ T1 Lines

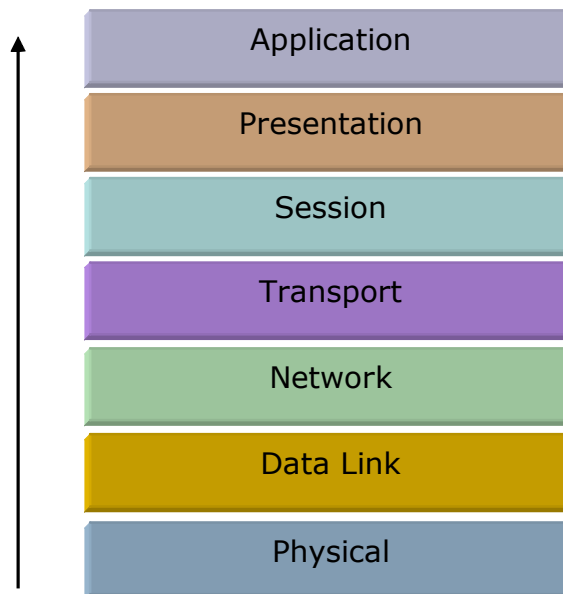
## The OSI Model

في هذا الجزء من المنهج سوف نتعمق اكثر في الشبكات وسوف يصبح الأمر أكثر تعقيدا حيث نتناول طرق الإتصال و Data layers وما يتعلق بها والكثير من الأشياء العلمية الهامة والتي سوف نتعرف عليها في الأجزاء التالية من المنهج.

### OSI Model Introduction

هي اختصار لـ Open System Interconnect هي الطريقة التي بها تستطيع ان تفهم كيفية نقل البيانات عبر الشبكات، وكما هو معلوم لك بأن الشبكات ربما تحوي اجهزة — Hardware مختلف وايضا برامج وانظمة تشغيل مختلفة OS إذا كيف نوجد علاقة للتعامل مع هذه الاجهزة على الشبكة في اطار واحد إذ ليس من المنطق ان نتعامل مع بعضها البعض بدون طريقة وسطية وايضا نقل الملفات مثلا عبر الشبكة قد تكون مسألة بسيطة بالنسبة لك لا تتعدي نقرة زر إلا ان الأمر وراء الكواليس يحتاج غلى عمليات أكثر تعقيدا لنقل هذه البيانات عبر الشبكة من جهاز إلى آخر وهنا يأتي دور الـ OSI Model لنفهم مالذي يحدث بالضبط.

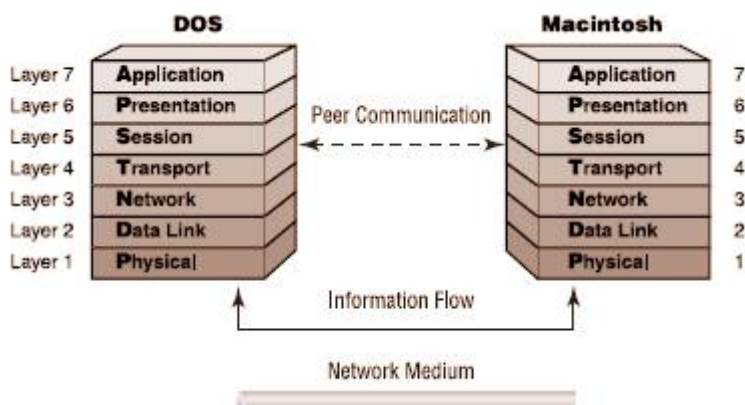
عموما الـ OSI Model تم ابتكارها من قبل منظمة ISO عام ١٩٧٧ لوصف اي بروتوكول على الشبكة وعرفت بعد ذلك بالـ OSI Model ويتكون الـ OSI Model من التالي:



كما هو واضح امامك في الصورة ولكن بالطبع تذكر هذه الـ layers ليس سهلا فقط تذكر هذه المقولة الشهيرة التي يرددوها الكل **All People Seem To Need Data Processing** وخذ الحرف الأول من كل كلمة لتعبر لك عن كل Layer إلا انه ضع بإعتبارك ان الإتجاه الخاص بتنفيذ او نقل البيانات يكون في اتجاه السهم اي من اسفل إلى اعلى بمعنى ان الخطوة تبدأ اولاً بـ Physical ثم تنتهي بالـ Application. هذا فيما اذا كان الجهاز

هو من يستقبل المعلومة اما إذا كان الجهاز يرسل البيانات فالعكس صحيح!

لاحظ في الصورة التالية كيف تنتقل البيانات عبر هذه الـ Layers من جهاز يعمل بالـ Dos مثلا وجهاز يعمل بنظام Mac العمليات تبدأ بالعكس في كلا الجهازين!



ضع في اعتبارك ان الـ OSI هو مجرد Model او نموذج يشرح فقط كيفية الإتصال وليس Protocol مستخدم في الإتصال من قبل الأجهزة والبرمجيات!

ولنتعرف في الجزء التالي على كل Layer على حدى.

### Application Layer

هي اعلى Layer او جزء في الـ Model وهي لا تعني الـ Applications كبرنامج الـ Word او الـ Access وخلافه بقدر ما تعني الـ Application المسؤول عن تنفيذ الأمر المتعلق بالشبكة الذي يطلبه برنامج مثل الـ Word مثلا عندما تقوم بفتح برنامج عبر الشبكة فإنه يستخدم بعض الأدوات التى لا تراها تسمى Tools هذه هي الـ Applications المقصودة في المعنى، وتتضمن ايضا الطباعة والرسائل ولا تقتصر على ذلك بل تتعداه.

### Presentation Layer

في خلال هذه الـ Layer يتم كما هو واضح من المعنى تقديم الـ Data وتجهيتها للتبادل او Exchange فيتم تعديل الـ Character Set و يتم ايضا عمل Encryption او تشفير للمعلومات او حتى ضغط او Compression للمعلومات.

### Session Layer

في هذه الـ Layer يتم الإتصال المباشر ما بين الجهازين حيث يتم التأكد من رقم الجهاز وعنوانه وهل تم ارسال المعلومات ام لا؟ وايضا كلمات السر وتأمين البيانات يتم هنا في هذه الـ Layer واي عملية يتم فيها التأكد من المعلومات تتم هنا ايضا.

### Transport layer

هذه الـ Layer مسؤولة عن التأكد من نقل البيانات دون حدوث اخطاء او Error-Free وايضا يتم في هذه الـ Layer تقسم الرسائل الكبيرة إلى عدة رسائل صغيرة وايضا العكس تحول الأجزاء الصغيرة من الرسالة إلى رسالة طويلة مرة أخرى. وهي ايضا مسؤولة عن التحقق من وصول البيانات بشكل صحيح عن طريق ما يسمى ACK او Acknowledgement اي التحقق من الوصول او اشعار الإستلام! ايضا يتم هنا تعريف اسماء الأجهزة Logical Address/ names إلا انها تستخدم على الأكثر في ACK.

### Network Layer

في هذه الـ Layer او الطبقة يتم تحويل الـ Logical Names اي اسماء الأجهزة مثلا إلى Physical Addresses ايضا هناك خدمة تسمى QoS او Quality Of Service تعمل ايضا في هذه الطبقة وهي مسؤولة عن عدم حدوث تأخير في بعض الخدمات على الشبكة مثل الفيديو والصوت، ايضا مهام الـ Routing تتم في هذه الطبقة. حيث تعمل الأجهزة التالية (Routers, Layer 3 Switches)

### Data Link Layer

هذه الطبقة من الـ OSI Model تقوم بتحويل البيانات واستلامها من Physical Layer وتحويلها إلى Logical Structure وهي ايضا تدعم الـ Logical Network وتكون ايضا تحوي اسم الكمبيوتر والبيانات المرسله وايضا تنتظر كود ACK. وتتكون هذه الطبقة من قسمين هامين هما MAC او Media Access Control و LLC او Logical Link Control وتنتقل خلال هذه الطبقة ما يسمى الـ Packet او اجزاء صغيرة من المعلومات وهي وحدة نقل المعلومات. والـ MAC Address كما هو معلوم لك هو الـ Physical Address الخاص بكرت الشبكة وهو يتألف من ١٢ رقما Hexadecimal وهذا النظام يستخدم الارقام من ٠ إلى ٩ والحروف من A إلى F

حيث يصبح الرقم كالتالي: 07:57:AC:B2:76

والأجهزة التالية تعمل في هذه الطبقة وهي:

**Bridges**  
**Switches**  
**NIC**



### Physical Layer

هي الطبقة أو الجزء الذي يهتم بتسجيل بيانات الإتصال الخاص بالـ Hardware مثل نوع الكارت عدد الـ Pins وما شابه ذلك.

لاحظ ان الـ Physical Layer تحوي أيضا معلومات التشبيك المختلفة والتي هي Physical Topologies وتتمثل في (Star, Ring, Mesh, and Bus) Topologies وايضا من الأجهزة التي تعمل في الـ Physical Layer (NIC – Transceivers- Repeaters – Hubs)

وقد تعرفت فيما سبق على بعض هذه الأجهزة لكن سوف نوضح لك بإختصار البعض الآخر وهو *Repeater* والذي يقوم بعمل *Amplify* او تقوية للإشارة عبر الشبكة هذا إذا كنت تريد نقل البيانات عبر مسافات قد تضعف فيها الإشارة.

### ماهي الـ Logical Topology؟

كما تعلمت مسبقا ان الـ Physical Topology هي الطريقة التي يتم ربط الشبكة بها او هي طرق التشبيك المختلفة للكوابل والأجهزة اما الـ Logical Topology فهي تعبر عن الطريقة التي تسري بها المعلومات وتنتقل داخل هذه الكوابل وهي نفس الـ Physical Topology في المسميات إلا ان سريان المعلومات في الكابل هو الذي يحدد نوع الـ Physical Topology المستخدمة.

ولكن ماهي التقنيات المستخدمة في نقل المعلومات عبر الشبكة الواحدة خلال الكوابل؟

نظريا توجد ثلاث تقنيات مستخدمة كالتالي:

CSMA/CD  
Token Passing  
CSMA/CA

## CSMA/CS

هي اختصار Carrier Sense/ Multiple Access with Collision Detection وهي التقنية السائدة والأكثر استخداما وهي في البداية تعتمد على تحسس الإشارة في الكابل الذي هو الـ Carrier فإذا لم يكن هناك أي إشارة مرسله فسوف تحاول إرسال الإشارة ثم يتم تحسس هل هناك أي إشارة أخرى ترسل في نفس الوقت أم لا؟ إذا كان هناك فعلا إرسال في نفس اللحظة فسوف يحدث ما يسمى Collision أو تعارض وسوف يتم إيقاف الإرسال في كلا النقطتين اللتان ترسلان ثم سيتم إعادة المحاولة مرة أخرى بعد وقت عشوائي حتى يتم الإرسال.

وتستخدم هذه التقنية في شبكات Ethernet و Wireless Ethernet

## Token Passing

تعتمد هذه التقنية على ما يسمى الـ Packet في الشبكة وهي اصغر جزء من المعلومات يتم نقله عبر الشبكة حيث أن كل جهاز موجود على الشبكة إذا تم تشغيله سوف يقوم بعمل Token أو "رمز مميز له" وسوف يتم إرسال هذا الرمز إلى الكمبيوتر المجاور وهكذا حتى تصل هذه الـ Token إلى الجهاز الذي يكون لديه معلومات ليرسلها إلى كمبيوتر آخر فيقوم بالحصول على الرمز Token وتعديله وإضافة البيانات له ومن ثم إرساله إلى الأجهزة الأخرى حتى تصادف الجهاز الذي يريد المعلومات فيستقبلها ويتم أخذ الـ Token وتعديلها وإرسالها مرة أخرى إلى بقية الأجهزة في شكل تكرار حتى يستقبلها كمبيوتر آخر وهكذا.

## CSMA/CA

هي اختصار لـ Carrier Sense/ Multiple Access with Collision Avoidance وهي تشبه كثيرا التقنية الأولى CSMA/CD إلا أنه بدلا من إرسال المعلومات والإنتظار للتحقق هل تم نقلها أم لا فإن الراسل أو Sender يرسل كود RTS ثم ينتظر لإستقبال كود CTS قبل أن يتم إرسال البيانات كاملة. وتستخدم هذه التقنية من قبل شبكات AppleTalk ولكي تفهم الفارق بشكل عملي، لنضرب مثال مثلا أنك تريد أن تعبر طريقا مزدحما بالسيارات فإذا اتبعت الطريقة الأولى CSMA/CD فسوف تعبر وإذا خبطتك سيارة فسوف ترجع إلى نقطة البداية وتعاود مرة أخرى العبور حتى تعبر بسلام! أما إذا استخدمت الطريقة الثانية CSMA/CA فسوف ترسل أي شخص آخر أو أخيك الصغير إذا خبطه سيارة هذا يعني أن الطريق غير مؤمن للعبور فسوف تقوم بإرساله أكثر من مرة حتى يتم إعطاؤك تصريح بالمرور بأمان! لا تطبق هذا المثال في الحقيقة!!!

## Networking Protocols

في هذا الجزء من المنهج سوف نتعرف على اهم البروتوكولات المستخدمة في الشبكات ويكفي ان تعرف ان البروتوكولات هي اساليب التخاطب او تقنيات التخاطب ما بين الأجهزة على الشبكة او بين الشبكات المختلفة وسوف نتعرف على التالي:

TCP/IP  
IPX/SPX  
NetBEUI  
AppleTalk

### TCP/IP

هو اختصارا Transfer Control Protocol / Internet Protocol حقيقة هو ليس بروتوكول في حد ذاته اكثر منه مجموعة من الأدوات وهو الأكثر استخداما في الإنترنت ويستخدم للربط والتخاطب ما بين الأجهزة عبر الشبكة المحلية وايضا عبر الإنترنت وهو الـ Protocol الأكثر استخداما وشيوعا ولهذا سوف نفرّد له جزء خاص من هذا المنهج لاحقا لكي نتعرف عليه عن قرب.

### IPX/SPX

هذا البروتوكول تم ابتكاره من قبل Novel NetWare والتي كان متوقعا لها ان تصبح LAN Server و WAN server ولهذا ابتكرت هذا الـ Protocol والذي هو اختصار Internetwork Packet eXchange/ Sequences Packet eXchange

### NetBEUI

هو بروتوكول تم ابتكاره اساسا لدعم شبكات NetBIOS والتي تم ابتكارها من قبل شركة IBM وتم تطويرها فيما بعد من قبل Microsoft و Novell واستخدم فيما بعد في أنظمة تشغيل ويندوز للـ Servers مثل Windows NT و Windows 2000 ودائما تجد هذه البروتوكولات مجتمعة وهي NetBEUI/NetBIOS

### AppleTalk

عندما قدمت شركة Apple كمبيوتر Macintosh عام ١٩٨٤ قدمت معه اداة للشبكات تستخدم بروتوكول AppleTalk ونظاما للربط سمي LocalTalk ثم بعد ذلك طور ليصبح EtherTalk حيث اصبح اسرع مع امكانية التعامل مع Ethernet.

## TCP/IP Fundamentals

سوف نتعمق في هذا الجزء الهام من المنهج في فهم بروتوكولات TCP/IP حيث سنتعرض لاساسياته وتاريخه ويكيفية عمله لأنه من الأجزاء الهامة جدا في علم الشبكات وقد يخصص له كتب متخصصة يمكنك العثور عليها ايضا لتنمية مهاراتك وخبراتك في الشبكات.

### لمحة تاريخية عن TCP/IP

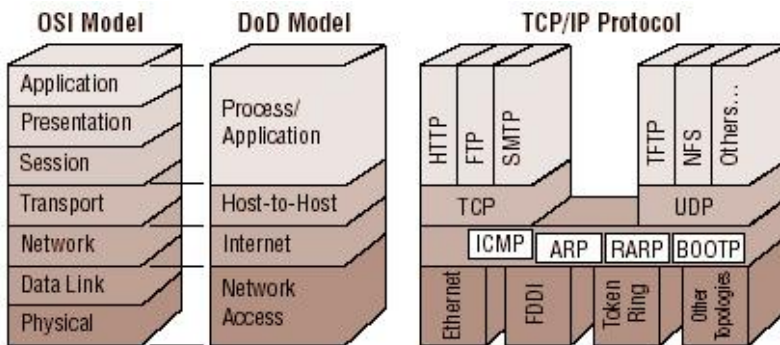
تم ابتكار الـ TCP/IP عام ١٩٧٣ ولكنه لم يكن الـ Standard في الإتصالات عبر الإنترنت حتى ١٩٨٣ حتى أصبح الطريقة الافتراضية في الإتصال عبر الإنترنت او عبر ARPAnet ان صح التعبير. وقد خرج هذا الابتكار من معامل جامعي كاليفورنيا الأمريكية في Berkeley عندما كان علماء الكمبيوتر عاكفون على اخراج نسخة Unix والتي عرفت باسمهم فيما بعد UNIX BSD اي Berkeley Software Distribution ولهذا بدأ انتشار TCP/IP في الجامعات نظرا لبدء انتشار UNIX في الحياة الاكاديمية حتى أصبح الـ TCP/IP هو صاحب الثورة في الإتصال عبر الإنترنت وايضا الشبكات المحلية.

وايضا مما ادى إلى تطوير هذا البروتوكول هو دعم وزارة الدفاع الأمريكية للأمر بحيث وضعت شروطا ومعايير وقيود على التطوير طبقا لمعايير معينة على سبيل المثال:

- ان الـ TCP/IP لا يخضع لشركة معينة او برمج معينة او Hardware معين
- ان الـ TCP/IP يجب ان يحوي في داخله ادوات للصيانة او Failure-Recovery
- حيث ان هذا كان متعلقا بالمسائل العسكرية بوزارة الدفاع حيث إذا حدثت مشكلة في جزء من الشبكة هذا ليس معناه سقوط الشبكة كليا.

- امكانية الإتصال ما بين الشبكات والأجهزة والبرمجيات المختلفة

ويستخدم الـ TCP/IP ما يسمى DoD Model او Department of Defense Model



والذي يصف الإتصال في اربعة طبقات فقط او Layers خلافا للـ OSI Model كما تعلمت سابقا والشكل التالي يوضح الفرق.

وكما ترى من الشكل فإن الـ DoD Model يتمثل في:

### Process/Application Layer

وهي المسؤولة عن البرمجيات مثل FTP, Telnet

### Host-to-Host Layer

طبقة الوسيط للوسيط وهي التي يتم فيها اضافة TCP والبروتوكولات الأخرى للـ Packet

### Internet Layer

يتم فيها اضافة الـ IP للـ Packet

### Network Access Layer

هي المسؤولة عن الربط ما بين وسائط النقل مثل الكوابل وايضا كروت الشبكة

## Transmission Control Protocol (TCP)

هذا الجزء من البروتوكول هو الجزء المسؤول عن نقل البيانات والربط ويقسم هذا الجزء البيانات إلى اجزاء صغيرة للتعامل معها تسمى هذه الأجزاء بـ Datagram ويحوي الـ Datagram معلومات عن المكان الذي سوف ترسل له البيانات وعنوان الراسل وايضا رقم مميز للـ datagram سوف يتم تسلسله فيما بعد كل هذا يسمى الـ Header الخاص بالـ Datagram ويحوي ايضا الـ Datagram ما يسمى Checksum للتأكد من وصول البيانات إلى النقطة المرسل اليها البيانات والشكل التالي يوضح اهم مكونات الـ Datagram في الـ TCP

Source Port		Destination Port		TCP Header
Sequence Number				
Acknowledgment Number				
Offset	Reserved	Flags	Window	
Checksum		Urgent Pointer		
Options			Padding	
Start of Data				

TCP Header

والـ Source Port يعبر عن رقم المكان الذي يرسل البيانات و Destination Port هو رقم المكان او النقطة المرسل اليها البيانات. Sequence Number هو الرقم المسلسل الخاص بالـ datagram لتسهيل عملية اعادة تنظيم البيانات على الكمبيوتر المستقبل.



Acknowledgement Number هو رقم يمكن الكمبيوتر الراسل من معرفة ان البيانات تم نقلها بنجاح.

Offset تعبر عن طول الـ Header ككل

Reversed هو عبارة عن متغير يمكن الإستفادة منه في اي شيء آخر اضافي

Flags تعبر عن ان هذه المعلومات هامة جدا او انها نهاية المعلومات المنقولة

Window تعطي امكانية زيادة حجم الـ Packet مما يؤدي إلى دقة نقل البيانات

Urgent Pointer يعطي تصريحاً بأهمية البيانات

Options مجموعة من المكتغيرات ربما تستخدم فيما بعد من قبل المستخدم

Padding للتأكد من ان الـ Header انتهى عند 32 Bit

Start of Data بداية المعلومات الحقيقية التي سوف يتم نقلها

## Internet Protocol

او IP هو المسؤول عن نقل البيانات من نقطة إلى نقطة اخرى على الشبكة وهو لا يحمل او يحوي اي نوع من البرمجيات الخاصة بالاتصال لكنه يعتمد كلياً على الـ TCP ولكنه فقط يقوم بعمل route او نقل للـ Data او المعلومات.

ودائماً يكون الـ Header الخاص بالـ IP ملتصقاً بالـ Header الخاص بالـ TCP ومن دون الـ Header الخاص بالـ IP لن يتم معرفة اين سيتم نقل الـ Datagram او عمل Routing له، والشكل التالي يوضح تركيب الـ Header الخاص بالـ IP

Version	IHL	TOS	Total Length		} IP Header
Identification			Flags	Fragmentation Offset	
Time to Live		Protocol	Header Checksum		
TCP Header					
Start of Data					

Version تعبر عن رقم اصدار الـ IP المستخدم والإصدار الافتراض المستخدم حالياً هو IP v4 إلا ان هناك الإصدار السادس IP v6 إلا انه لم يدعم إلا من بعض الأجهزة الحديثة حالياً إلا انه سوف يصبح الإصدار الافتراضي قريباً جداً

IHL أو Internet Header Length وهو طول الـ Header والرقم الافتراضي له هو خمسة كلمات من سعة 32 bit

TOS أو Type of Service تعبر عن أهمية البيانات المطلوبة

Total Length تحدد طول الـ Datagram ككل والتي تنحصر ما بين 576 bytes كأقل قيمة و 65.532 bytes كأعلى قيمة

Identification تعريف يسهل على الجهاز المستقبل إعادة ترتيب الـ datagram

Flags أول bit يعبر عن ان الـ datagram لا يمكن ان يكون مقسما إلى اجزاء صغيرة والـ Bit الأخير هو يعبر عن آخر قسم في اي Packet مقسمة إلى اقسام.

Fragmentation Offset تعبر عن المكان المحدد للمعلومات وهي تستخدم في عملية إعادة تجميع البيانات من قبل المستقبل

Time to Live

الوقت المستخدم أو المخصص لنقل الـ Packet بعد ان ينقضي هذا الوقت تصبح بعدها الـ Packet مفقودة أو Lost ولها معنى آخر هو hop ودائما تجدها 32 hops

Protocol تعبر عن نوع الـ Protocol لأنه من الممكن استخدام بروتوكولات اخرى غير الـ TCP/IP القيمة ٦ تعبر عن TCP والقيمة ١٧ تعبر عن UDP أو User Datagram Protocol

Header Checksum قيمة للتحقق من عدم وجود الأخطاء في الـ Header

TCP Header هو كما تعرفت عليه سابقا الـ Header الخاص بالـ TCP

## Application Protocols

سوف نتناول في هذا الجزء من المنهج تعريفا بالبرمجيات التي توجد في الـ TCP/IP.

### SNMP

هو Simple Network Management Protocol ويستخدم هذا البرنامج من قبل الـ Network Administrators لمعرفة معلومات اضافية عن الشبكة وايضا الأجهزة الموجودة على الشبكة من Switches و Routers واي اجهزة اضافية.

وسوف تجد في قسم البرمجيات والأدوات بعض البرمجيات التي تعتمد على هذه التقنيات.

### FTP

وهو مختصر File Transfer Protocol هو اداه مهمة جدا لنقل الملفات عبر الشبكة وما بين الاجهزة التي تدعم هذه التقنية والتي تسمى FTP Servers وبالتاكيد إذا كنت تتعامل مع مواقع الإنترنت فقد سمعت عن الـ FTP

### TFTP

هو مختصر Trivial File Transfer Protocol وهو نسخة مصغرة من FTP تستخدم لنقل الـ Boot Image للأجهزة التي لا يوجد بها Boot Disk وايضا من وإلى الـ Routers

### SMTP

هو مختصر Simple Mail Transfer Protocol وهو المسؤول عن نقل الرسائل الإلكترونية عبر الشبكة ومن جهاز إلى جهاز آخر وهو المسؤول عن الإرسال الخاص بالـ Emails

### POP

وهو مختصر Post Office Protocol ويوفر مساحة تخزينية لإستقبال الرسائل الإلكترونية وهو معروف باسم POP3 وفي بعض الأحيان يستخدم الـ IMAP بدلا من POP3

### IMAP

وهو مختصر Internet Mail Access Protocol ويوفر مساحة تخزينية للمستخدم لتخزين الرسائل وايضا قراءة الـ Email Header وتخزين جزء من الرسالة على الـ Server وهو الموجود في الـ Yahoo مثلا على سبيل المثال.

### Telnet

هو Terminal Emulation ويتيح الإتصال عن بعد بالأجهزة على الشبكة.

### ICMP

وهو مختصر Internet Control Message Protocol والمثال الواضح لهذا البرنامج هو الأمر Ping الذي تستخدمه للتحقق من وجود الـ Host على الشبكة حيث يقوم بأرسال رسالة للـ Host واستقبالها منه مرة أخرى.

### HTTP

هو مختصر Hypertext Transfer Protocol وهو وسيلة التخاطب ما بين الأجهزة والـ Web servers والمستخدم في فتح المواقع على الـ Internet Browser

### ARP

وهو مختصر Address Resolution Protocol وهو أداة أو برنامج يمكنك من معرفة معلومات عن الـ Physical Hardware الخاص بكروت الشبكة والـ IP الخاص بها

### NTP

هو اختصار Network Time Protocol

هذه الأداة مهمة جدا وقد تم ابتكارها من قبل البروفيسور David Mills في جامعة Delaware والغرض الاساسي منه هو جعل جميع الأجهزة في الشبكة تعمل بتوقيت واحد أو Synchronize وهذا التوقيت حسب ساعة معينة وهي الساعة الذرية أو Nuclear Clock لأنه لو حصل اختلاف في التوقيت بين الأجهزة على الشبكة هذا معناه اختلال العمل وضياح المعلومات.

### UDP

هو اختصار User datagram Protocol

هذه الأداة أو البرنامج تعطي اتصال مباشرا بين البرمجيات والـ IP وهي تعمل في طبقة Transport وايضا تتيح الإتصال بخدمة معينة أو برنامج معين عبر Port محدد في كمبيوتر آخر على الشبكة.

## Ports & Sockets

في شبكات TCP/IP تنتقل المعلومات من Port في الكمبيوتر المرسل للمعلومة إلى Port في الكمبيوتر المستقبل للمعلومة حسب رقم الـ Port والبرنامج الذي يستخدمه هذا الـ Port وكما معلوم فأن كل برنامج له Port معين يعمل عليه في الإتصال وكل Port هو عبارة عن رقم 16 bit يتألف من صفر حتى 65535 وايضا للعلم فأن الـ Ports تنقسم إلى TCP Ports و UDP Ports حسب البرنامج الذي يعمل على هذا الـ Port على سبيل المثال جميع الـ Servers التي تتصل على خدمة Telnet تستخدم الـ Port رقم 23 وهو TCP Port وايضا الـ Web servers تعمل على الـ Port رقم 80 وهو خاص ببرنامج HTTP وسوف نوضح لك في الجدول التالي اهم الـ Ports المستخدمة والبرامج التي تعمل عليها

PORT	PROTOCOL
UDP Port 15	NETSTAT
TCP Port 21	FTP
TCP Port 23	Telnet
TCP Port 25	SMTP
UDP Port 53	DNS
UDP Port 69	TFTP
TCP Port 70	Gopher
TCP Port 79	Finger
TCP/UDP Port 80	HTTP
TCP/UDP Port 443	HTTPS
TCP Port 110	POP3
UDP Port 111	RPC
TCP Port 119	NNTP
TCP Port 123	NTP
UDP Port 137	NetBIOS Name Service
UDP Port 161	SNMP (Network Monitor)
UDP Port 2049	NFS

## Understanding IP Address

الـ IP هو الرقم المميز لكل جهاز على الشبكة وإذا استخدمت بروتوكول TCP/IP فهذا يحتم عليك ان يكون هناك رقم مميز لكل جهاز على الشبكة. وهناك نوعان او اصداران من الـ IP ها IPv4 و IPv6.

### IPv4

هذا الإصدار هو الأكثر استخداما الآن وهو عبارة عن ٤ خانات تتكون من رقم 32bit وهو دائما يتم الفصل بين الاربع خانات اما بنقطة او بعلامة عشرية وهو يبدأ بالارقام من 0 حتى 255 في كل خانة على سبيل المثال 192.168.0.1 هو رقم IP مكون من اربع خانات كل خانة تأخذ ارقاما من صفر حتى ٢٥٥ كما ذكرنا وتسمى كل خانة Octet او Byte. وتقسم ارقام الـ IP إلى فئات حسب حجم الشبكات والأجهزة المتوفرة عليها وتسمى IP Classes والـ IP ايضا يحوي معلومات عن رقم الشبكة ورقم الوسيط او الجهاز.

### IPv6

هو التقنية القادمة في الـ IP وتم ابتكاره خصيصا لأن الأرقام المتوفرة في النظام السابق IPv4 اصبحت قليلة لكثرة المستخدمين على الشبكة ويستخدم الـ IPv6 نظام ارقام 128 bit ويعطى حوالى Octillion 79 اي مائة وسبعة وتسعون ألف مليار (79.000.000.000.000.000.000.000.000) الثنائي او الـ Binary فهو يستخدم نظام Hexadecimal في ثمانية خانات منفصلة تتكون كل خانة من اربعة ارقام وحروف على سبيل المثال (3FFE:0B00:0800:0002:0000:0000:0000:000C)

### IPv4 Classifications

الفئات الخاصة بهذا الإصدار من الـ IP هي كما يلي:  
(Class A, Class B, Class C, Class D, Class E)

#### Class A

يستخدم للشبكات العملاقة مثل HP, IBM ومثيلاتها واعلى رقم بهذه الفئة هو 0 ويحوي ١٢٧ شبكة وهو انتهى للأسف لم يعد متاحا تعريف شبكات على هذا النظام جميع الارقام نفذت ولم يعد بالإمكان تعريف شبكات من هذا النوع!

### Class B

يستخدم للشبكات المتوسطة وأعلى رقم فيه هو 10 (ليس عشرة) هو 1 و صفر وعلى سبيل المثال على هذه الشبكات هي Microsoft وهذا النوع من الشبكات انتهى أيضا لم يعد بالإمكان تعريف شبكة من هذا الحجم أو هذه الأرقام لأن الأرقام كلها مستخدمة.

### Class C

هو للشبكات الصغيرة وأعلى رقم بها هو دائما 110 وكل شبكة يمكن تعريف ٢٥٤ جهاز عليها فقط وهو مازال متاح ويمكن استخدامه وهو يستخدم على نطاق واسع في الشبكات المحلية أو LAN

### Class D

هذا النظام ليس لاستخدام الشبكات

### Class E

محجوز للتجارب والشكل التالي يوضح أهم ميزات وخواص الفئات المختلفة.

Class	Bit Allocation					
A	0	<table><tr><td>Network</td><td>Host</td></tr><tr><td>7 bits</td><td>24 bits</td></tr></table>	Network	Host	7 bits	24 bits
Network	Host					
7 bits	24 bits					
B	10	<table><tr><td>Network</td><td>Host</td></tr><tr><td>14 bits</td><td>16 bits</td></tr></table>	Network	Host	14 bits	16 bits
Network	Host					
14 bits	16 bits					
C	110	<table><tr><td>Network</td><td>Host</td></tr><tr><td>21 bits</td><td>8 bits</td></tr></table>	Network	Host	21 bits	8 bits
Network	Host					
21 bits	8 bits					
D	1110	<table><tr><td>Multicast Addresses</td></tr><tr><td>28 bits</td></tr></table>	Multicast Addresses	28 bits		
Multicast Addresses						
28 bits						
E	1111	<table><tr><td>Experimental</td></tr><tr><td>28 bits</td></tr></table>	Experimental	28 bits		
Experimental						
28 bits						
Loopback	01111111	<table><tr><td>Unused</td></tr></table>	Unused			
Unused						

لاحظ أننا نتحدث عن IPv4 وهو 32 Bit Number

والجدول التالي يوضح عدد الشبكات والأجهزة المتاحة في كل فئة من فئات الـ IP وهو مهم جدا وأيضا يوضح لك الأرقام الخاصة التي تبدأ بها أي شبكة لكي تكون على دراية بأي نوع تنتمي هذه الشبكة.



	Class A	Class B	Class C
IP Start	1.0.0.0	128.0.0.0	192.168.0.0
IP End	126.0.0.0	191.255.0.0	255.255.255.0
No. of Networks	126	16,384	2,097,152
No. of Nodes	16,777,214	65,534	254
Network Octet	N,H,H,H	N,N,H,H	N,N,N,H

لاحظ ان H = Host ID و N = Network ID

ويتضح التالي:

الأرقام التي تبدأ بـ 126 فأقل هي تتبع Class A Network  
الرقم 127 محجوز لأعمال الـ Loopback Test على سبيل المثال يمكنك التحقق من  
كارت الشبكة عن طريق ping 127.0.0.1  
الأرقام من 128 حتى 191 تتبع الشبكات Class B  
الأرقام من 192 حتى 223 تتبع Class C Network  
القيم اكبر من 223 كلها ارقام محجوزة لايمكن استخدامها

### Subnets

لم يكن احد ليتخيل كم الشبكات الموجودة حالياً متصلاً بالإنترنت وايضا عدد الأجهزة الموجوده  
على الإنترنت ولهذا كان النظام IPv4 قاصراً في بعض الأحيان فلهذا تم ابتكار تقنية اخرى  
لحل هذه المشكلة سميت Subnetting او تقسم الشبكات!  
وهذا الموضوع ليس سهلاً ويحتاج إلى منهج خاص لكي نشرحه باستفاضة  
ويستخدم الـ Subnet رقم يسمى Host Address عبارة عن Bits اضافية يتم اضافتها  
لأرقام الـ IP لزيادة عدد الأجهزة والشبكات على الفئة او الـ Class  
والشكل التالي يوضح الـ Subnet Mask المختلفة الخاصة بالـ Network Classes

Default Subnet Masks for Standard IP Address Classes

Class	Subnet Mask Bit Pattern	Subnet Mask
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

سوف نأخذ تقسيم او Subnet Mask الخاص بـ Class C Network على سبيل المثال وهو كما ترى 255.255.255.0 ولكن من اين اتى هذا الرقم؟

كما تعلم لان الـ Subnet عبارة عن Bits فهي بالنظام الـ Binary وكما ترى في الشكل السابق الـ Bits الخاصة بالتقسيم الخاص بـ Class C Network هو كما يلي

11111111 11111111 11111111 00000000

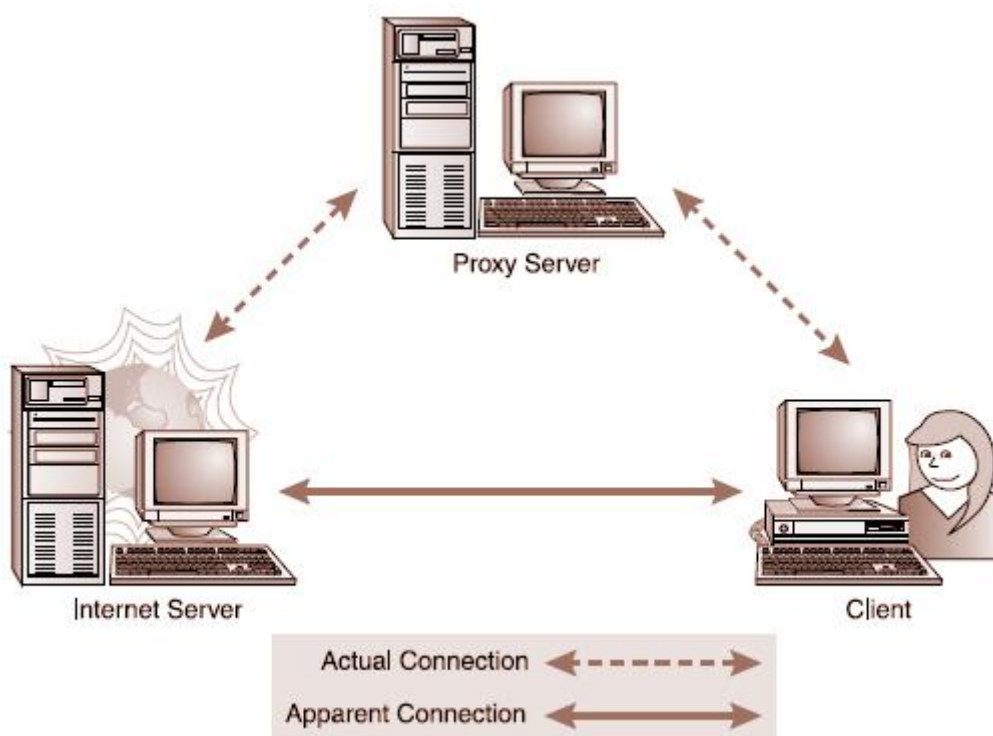
كما ترى امامك هذا رقم Binary وهو بالنظام العشري عبارة عن 255.255.255.0 قم بتشغيل الآلة الحاسبة في الويندوز واختر View → Scientific الآلة العلمية



اختر من اليسار كلمة Bin اي Binary لكي نقوم بكتابة الرقم الثنائي  
ثم قم بكتابة الرقم الأول من اليسار من رقم الـ Subnet Mask وهو 11111111  
ثم بعد ان تكتب الرقم اختر من اليسار كلمة Dec او Decimal وسوف يتم تحويل الرقم إلى  
الرقم العشري وهو كما ستري 255 هل علمت الآن من اين جاءت هذه الأرقام؟

## IP Proxy Servers

الـ Proxy Server هذا نوع من الـ Servers التي يتم توصيلها بالشبكة المحلية او بشبكة شركتك لعمل وظيفة هامة جدا وهي انه يقوم بحجب دخول الإنترنت على المستخدمين داخل الشبكة الموجود عليها عن طريق برمجيات خاصة بمعنى ان المستخدم لا يستطيع ان يتصل بالإنترنت بدون ان يمر على هذا الخادم ومن اهم مميزاته ايضا انه يمنع الدخول من خارج هذه الشبكة إلى داخلها إلا ان هذا يتوافق مع عمل الـ Firewall ايضا الذي يمنع دخول اي Traffic من خارج الشبكة إلى الأجهزة داخلها. والشكل التالي يوضح لك ان الـ Proxy يقوم بعمل محاكاة للمستخدم انه يتصل فعليا بالإنترنت وهذا لا يحدث بالطبع!



لاحظ ان الـ Proxy Server لن يكون فعالا إلا إذا كان هو الوسيلة الوحيدة للاتصال للإنترنت عبر الشبكة المحلية.

## Proxy Server caching

يستخدم الـ Proxy نوعين من استعراض الملفات للمستخدم عبر الشبكة المحلية من الإنترنت وهما Active Caching حيث يقوم بجلب الصفحات التي قد يحتاجها المستخدم في فترات متقاربه وهناك ايضا Passive Caching والذي يقوم بعمل استعراض للصفحة في حالة ما إذا طلبها المستخدم حيث يقرر اما يستعرضها لو مسموح بها ام لا.

لاحظ ان بعض الصفحات لايمكن ان يتم عمل Caching لها مثل الصفحات الخاصة بالمواقع المدفوعة والتي تحتاج إلى اشتراكات وايضا المواقع المحمية.

### ICP

وهو مختصر Internet Cache Protocol وهو عبارة عن رسالة تستخدم ما بين الـ Proxy Servers حيث يستطيع من خلالها معرفة ما اذا كانت هذه الصفحة موجوده ام لا في الـ Proxy Server Cache إلا ان هذا يؤدي إلى مشاكل مع كثرة وجود الـ Proxy Servers وكثرة الرسائل المتبادلة على الشبكة.

### CARP

او Cache Array Routing Protocol هذه التقنية هي التي تستخدم لحل مشكلة الـ ICP السابقة حيث تعتمد على استخدام Cache واحدة كبيرة لكل عدد من الـ Proxy Servers

## Name Resolution Methods

في هذا الجزء سوف نتعرف على اساليب تحول الـ IP إلى اسماء لسهولة تذكرها بدلا من الارقام التي يصعب ان يتذكرها المرء من كثرة المواقع والشبكات على سبيل المثال تستطيع تذكر كلمة [www.ask-pc.com](http://www.ask-pc.com) عن تذكر مثلا 192.168.0.20 الأمر اسهل بالاسماء.

### Internet Domain Organization

هناك مجموعة من النطاقات كما يطلق عليها باللغة العربية او Domains اساسية وهي يطلق عليها Top Level Domains او TLD وهم:

.com وهو للشركات

.edu للجامعات والمؤسسات التعليمية

.gov للمصالح الحكومية

.int للمنظمات العالمية مثل الامم المتحدة

.mil متعلق بوزارة الدفاع الأمريكية

.net متعلقة بالشبكات او جزء من شبكة

.org منظمات غير ربحية مثل منظمة الصحة مثلا

إلا انه للأسف ليست هذه قاعدة في بعض الـ TLD فأنتك قد تجد مؤسسة ربحية تختار لنفسها اسم منتهيا باللاحقة .org نظرا لعد توفر الإسم باللاحقة .com وهكذا.

## Hosts

الـ Host هو الإسم الذي يعبر عنه الـ IP وهو اسم الجهاز كما يطلق عليه على الشبكة وهناك عدة طرق كثيرة للتحويل من الـ IP إلى الـ Host ومن أحدها الـ HOSTS وهو عبارة عن ملف يسمى *HOSTS* تقوم بعمله على الجهاز وتضع فيه سطر لكل جهاز على حدى حيث تضع الـ IP في كل سطر وتضع امامه اسم الجهاز كالتالي

192.168.0.1 Server

192.168.0.2 User1

ونأتي الآن إلى الجزء المرهق وهو ان تقوم بنسخ هذا الملف على كل الأجهزة على الشبكة ولكن الأمر سوف يصبح اكثر ارهاقا اذا فكرت في وضع هذا الملف على الشبكات الأخرى خارج شبكتك! ولكن لا تقلق هناك حل آخر!

## DNS

هو اختصار لـ Domain Name Service وهو يستخدم لتحويل الـ Host إلى IP والعكس حيث يقوم بتحويل الـ IP إلى Host أو Domain Name

حيث انه عندما تكتب في متصفح الإنترنت مثلا [www.ask-pc.com](http://www.ask-pc.com) فهذا يطلب عرض صفحة الموقع الرئيسية ولكن كيف يصل للموقع!

سوف يقوم الـ Browser بمخاطبة الـ TCP/IP Protocol على الـ Port 80 لكي يقوم بمخاطبة الـ DNS Server ليسأل عن الـ IP الخاص بهذا الموقع [www.ask-pc.com](http://www.ask-pc.com) في قاعدة البيانات الخاصة به وعندما يتم استلام الـ IP يقوم الـ Browser بمخاطبة الـ Server صاحب هذا الرقم وتحميل الصفحة تلقائيا ويتم حفظ جميع الـ IPs والـ Host Names الخاصة بها في قاعدة بيانات الـ DNS Servers حول العالم وهذه العملية ما تسمى بالـ Propagation والتي يأخذها الـ Domain ليتم تعريفه على الإنترنت.

على سبيل المثال توجد السجلات أو الـ Records في الـ DNS Server كالتالي

Mail.ask-pc.com IN A 192.168.0.10

وهذا سجل لعنوان بريد على الموقع

ويوجد ايضا ما يسمى MX Record أو Mail Exchange Record والذي يمكنك من تعريف اكثر من mail host على موقع واحد لكي تتيح مرونة في استقبال الرسائل

ايضا هناك الـ CNAME Record والذي يتيح لك تعريف اكثر من عنوان للموقع الواحد مثلا [www](http://www) وايضا FTP وكل هذا يتم تسجيله في ملف أو سجل في الـ DNS Server

يسمى DNS Table ويصبح على هذا الشكل التالي

<a href="http://www.ask-pc.com">www.ask-pc.com</a>	IN	A	204.167.47.2
<a href="http://ftp.ask-pc.com">ftp.ask-pc.com</a>	IN	CNAME	<a href="http://www.ask-pc.com">www.ask-pc.com</a>
Mail.ask-pc.com	IN	A	204.167.47.9
Host.ask-pc.com	IN	MX	10 mail.ask-pc.com
Host.ask-pc.com	IN	MX	20 mail.ask-pc.com

وهكذا يسمى هذا بالـ DNS Table ويتم تخزينه في الـ DNS Server

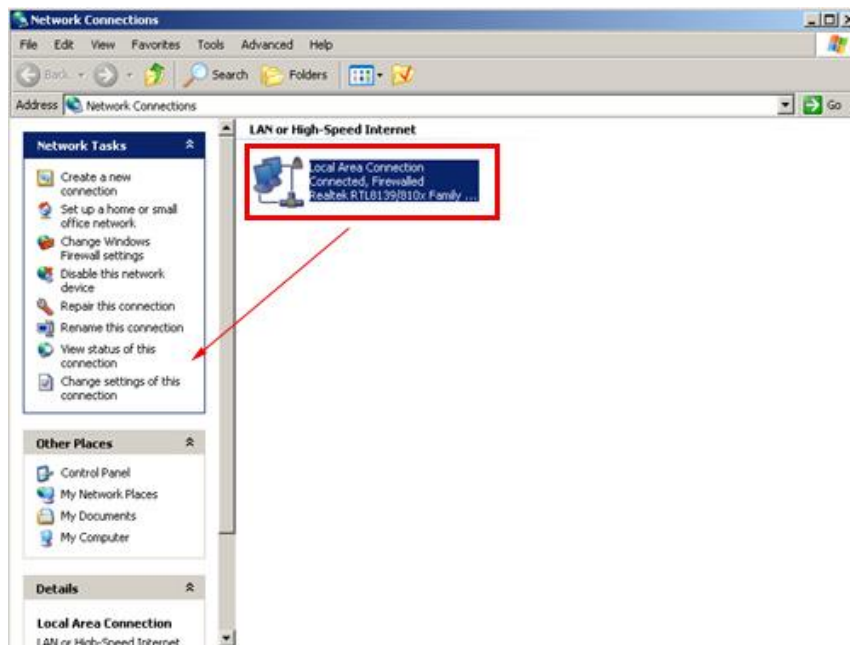
## WINS

هو اختصار Windows Internet Naming Service وهو جزء هام جدا في شبكات Microsoft ويستخدم الـ WINS مع TCP/IP حيث يقوم بتحويل الـ NetBIOS Names إلى IP والعكس وهو خاص بشبكات Microsoft كما عرفت مسبقا.

## Configuring IP Address in Windows XP

سوف نتعرف في هذا الجزء على كيفية تعريف IP لجهاز على شبكة محلية LAN وهذا الجهاز يعمل بنظام Windows XP.

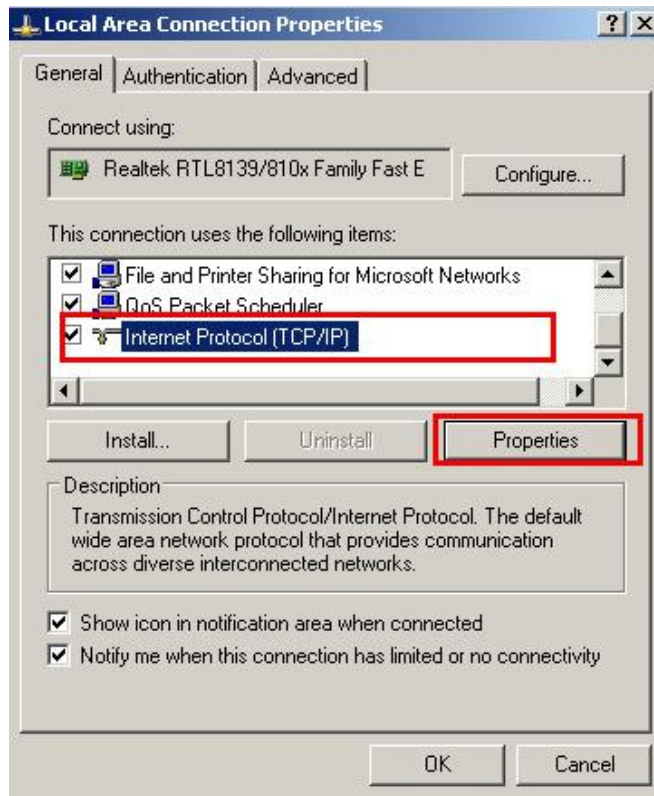
قم بالنقر R-Click على ايقونة My Network Places واختر Properties سوف تفتح لك النافذة التالية:



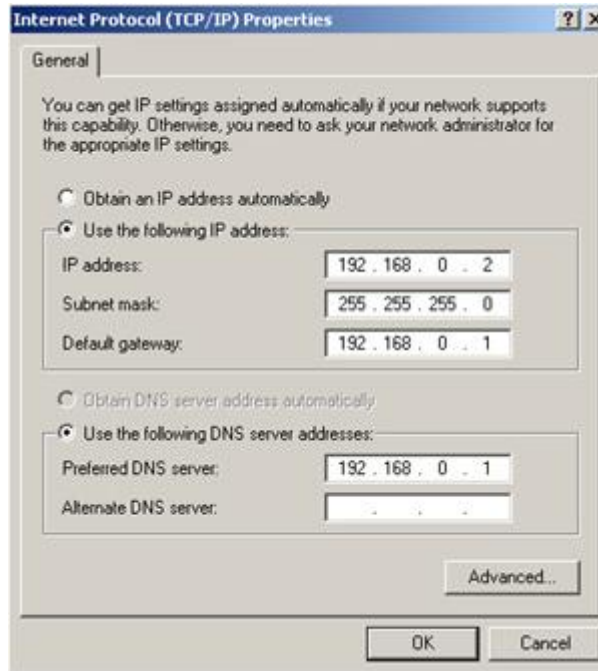


اختر من اليسار Change Settings of This Connection سوف تظهر لك هذه النافذة

كما ترى في الصورة تحوي هذه النافذة اهم اعدادات الشبكة الخاصة بالكارت المتصل بالكمبيوتر حيث ترى الخدمات التي يمكن التعديل فيها مثل File and Printer Sharing وايضا QoS التي شرحناها مسبقا وتجد ايضا TCP/IP والتي يمكنك من خلالها ان تقوم بوضع رقم IP مميز لهذا الكمبيوتر على الشبكة حسب نوع الشبكة التي تعمل عليها فقط اختر Internet Protocol ثم اختر



Properties وسوف تفتح لك نافذة اخرى سوف نتاولها فيما يلي بها الإعدادات الخاصة بالـ IP والتي يمكنك تعديلها.



كما ترى في الصورة فقط انقر على Use the following IP Address لكي تقوم بتعيين Static IP او رقم مميز لهذا الجهاز على الشبكة وضع رقم الجهاز في خانة IP Address وهو كما ترى 192.168.0.2 ثم نأتي للـ Subnet Mask وهو كما تعلمت هذه الشبكة تتبع Class C Network فإذا الـ Subnet Mask سوف يكون كما يلي 255.255.255.0 وانت تعلمت من اين اتى هذا الرقم. اما الـ Gateway فسوف نستخدمها فقط ونضع فيها رقم

البوابة التي توجد على الشبكة إذا كنت تستخدم جهاز كمبيوتر كبوابة للاتصال بشبكة الإنترنت



او رقم ال Router الذي يوصل شبكتك المحلية بالإنترنت وهناك ايضا ال DNS Servers التي يمكن تعريفها إذا كنت تستخدم اي منها وايضا Advanced سوف تفتح لك نافذة يمكن من خلالها عمل اعدادات ال WINS و NetBIOS والكثير من الإعدادات المتقدمة.

## VLAN

اختصار لتقنية تسمى Virtual Local Area Network او Virtual LAN وهي تقنية بدأت في الظهور بعد ان بدأ استخدام ال Switches بكثرة بدلا من ال Hubs في الشبكات المحلية وهي تعتمد على فكرة تقسيم الشبكة إلى شبكتين مثلا او اكثر لكن بشكل تخيلي او افتراضي Virtual وليس حقيقي من هنا جاءت التسمية ولكن كيف؟ لنفرض ان لديك Switch ذو 48 Port ولديك عدد ٢٠ جهاز يقومون بعمل Load على الشبكة وايضا ١٠ اجهزة يستخدمون الشبكة بشكل اعتيادي فيمكنك عن طريق ال Software الخاص بالـ Switch ان تقسم ال PORTS مثلا من PORT رقم ١ حتى ٢٠ مثلا للـ Traffic العالي والباقي للـ Traffic الاعتيادي وبهذا تكون قد قسمت الشبكة إلى اثنتين VLAN1 و VLAN2 بدون الحاجة إلى Switch آخر وبدون الحاجة إلى مد كوابل جديدة.

## TCP/IP Utilities

سوف نتعرف في هذا الجزء من المنهج على اهم الأدوات المستخدمة في الشبكات او ما يعرف بإسم الـ TCP/IP Tools وهي موجوده ضمن مجموعة البروتوكول TCP/IP

### ARP Table

كما عرفت مسبقا هو Address Resolution Protocol وهو جزء من TCP/IP وههز عبارة عن جدول يحيو المعلومات الخاصة بالـ IP والـ MAC address وتحفظ في ذاكرة الحاسب ولنفرض ان الجهاز يريد معرفة اي جهاز على الشبكة له IP معين لإينه سوف يرسل Request او طلب للأجهزة على الشبكة على سبيل المثال Who is IP Address 192.168.0.1 ? وسوف يرد الجهاز الذي يحمل هذا الـ IP بالـ MAC address الخاص به ايضا ويتم حفظ هذه المعلومات في الـ ARP TABLE ويحوي هذا الجدول نوعين من المعلومات هي Static و Dynamic.

### Dynamic Entry

وهو يوجد في الجدول الخاص بـ ARP عندما لا يوجد الـ MAC address ويتم ارسال Request لطلب هذا العنوان او توماتيكيا.

### Static Entry

نفس الخصائص الخاصة بالـ Dynamic إلا ان طلب رقم الـ MAC Address يتم عمله Manually او من قبل المستخدم باستخدام ARP Utility.

### ARP Utility

يمكنك ان تستخدم هذا الأمر بالعديد من المفاتيح او Switches لتحصل على معلومات هامة جدا عن الـ ARP Table ومن اهم الاشياء التي يمكنك ان تقوم بها من خلال هذا الأمر هو معرفة الـ IP المستخدمة على الشبكة هل هي مكررة ام لا لأنه قد يحدث هذا التكرار وان يكون لنفس الجهاز على الشبكة نفس الرقم وتحدث مشاكل إذا كنت تستخدم نظام DHCP او Dynamic Host Protocol والذي يعطي Dynamic IP للأجهزة على الشبكة والحل الوحيد هو ان تقوم بالتعرف على الاجهزة باستخدام الـ MAC Address عن طريق الأمر ARP على سبيل المثال قم باستخدام الأمر التالي في Command Prompt

C:\>arp -a

سوف تظهر لك النتيجة التالية كما في الصورة

```
C:\WINDOWS\system32\cmd.exe
C:\>arp -a
Interface: 192.168.0.2 --- 0x2
Internet Address      Physical Address      Type
192.168.0.1           00-0a-cd-00-0d-1d    dynamic
C:\>
```

IP Address

MAC Address

ARP Entry Type

عندما نقوم بكتابة الأمر ARP فقط منفصلا سوف يعرض لك جميع المفاتيح أو Switches التي يمكنك ان تستخدمها مع هذا الأمر. ويمكنك ايضا ان تكتب او تعدل في الـ ARP Table عن طريق الأمر

C:\>arp -s [IP address] [MAC Address]

وكما ترى الـ S Switch وهو يعني Static حيث سنقوم بالتعديل في الجدول بالقيم التي سوف ندخلها من رقم IP متوافق مع رقم الـ MAC Address وسوف تظل هذه المعلومات في ذاكرة الكمبيوتر حتى يتم عمل Restart وتحسب هذه الفترة بـ TTL او Time To Live وهي الفترة التي تضطل فيها هذه القيم في الجدول الخاص بالـ ARP.

سوف تجد في قسم التدريبات العملية بعض التدريبات على هذه الأوامر لكي تساعدك على فهم العمل بها وننصحك بمراجعتها لكي تفهم المنهج جيدا  
[www.ask-pc.com/academy](http://www.ask-pc.com/academy)

## Netstat Utility

سوف نتعرف على اداة مهمة ايضا وهي netstat والتي تمكنك من معرفة معلومات هامة جدا عن الشبكة والإتصال بالشبكة والجهاز الذي تقوم بتنفيذ الأمر عليه ويمكنك تنفيذه كالتالي:

```
C:\>netstat -a
```

وكما ترى المفتاح a معناه All حيث يقوم بعرض جميع المعلومات الخاصة بالـ TCP/IP وايضا UDP كما ترى في النتيجة التالية

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\MN>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP    naguib:epnap             naguib:0                LISTENING
TCP    naguib:microsoft-ds     naguib:0                LISTENING
TCP    naguib:1025              naguib:0                LISTENING
TCP    naguib:1035              naguib:0                LISTENING
TCP    naguib:nethios-ssn      naguib:0                LISTENING
TCP    naguib:2168              bayn4-cs85.messenger.hotmail.com:1863 ESTABLISHED
ED
TCP    naguib:2368              ats-nab.dial.aol.com:5190 ESTABLISHED
TCP    naguib:2369              kdc.uas.aol.com:https   ESTABLISHED
TCP    naguib:2371              bos-m027b.blue.aol.com:5190 ESTABLISHED
UDP    naguib:microsoft-ds     *:
UDP    naguib:isaknp           *:
UDP    naguib:1026             *:
UDP    naguib:1038             *:
UDP    naguib:1040             *:
UDP    naguib:1728             *:
UDP    naguib:1729             *:
  
```

وكما ترى يوضح لك جميع الـ Connections المتصلة على TCP/IP و الـ UDP والعناوين المتصلة بها وايضا حالتها من حالة الإتصال Established او عدم الإتصال Listening. ولهذا الأمر العديد من المفاتيح يمكنك التعرف عليها وتجربتها عن طريق كتابة الأمر netstat /? في الـ Command Line على سبيل المثال يمكننا استخدام الأمر

```
C:\>netstat -e
```

لمعرفة معلومات هامة عن حجم البيانات التي تم ارسالها واستقبالها عن طريق كارت الشبكة وبالفعل هذا الأمر هام جدا ومن اهم الأدوات التي لاغنى عنها لأي مدير شبكة فتنصحك بتجربة جميع المفاتيح الخاصة بها وفهمها وايضا متابعة الدروس المتفاعلة في قسم التدريبات العملية في الأكاديمية على هذا الرابط [www.ask-pc.com/academy](http://www.ask-pc.com/academy)

## Nbtstat Utility

هذا الأمر من الأوامر الهامة جدا ولعلك تذكر الـ NetBIOS وما شرحناه عنه مسبقا هذا الأمر مفيد جدا في تحويل او عرض الاسماء الخاصة بـ NetBIOS وله ايضا مفاتيح مهمة لكل منها وظيفته الخاصة وهو يعتبر اداة الـ NetBIOS الشهيرة داخل TCP/IP. على سبيل المثال يمكنك ان تعرف اسم الجهاز على الشبكة عن طريق الـ IP باستخدام الأمر

```
C:\>Nbtstat -a 192.168.0.2
```

حيث يقوم بتحويل هذا الرقم او الـ IP إلى الإسم المكافئ له على الشبكة كما ترى

```
C:\>nbtstat -a 192.168.0.5
Local Area Connection:
Node IpAddress: [192.168.0.2] Scope Id: []

NetBIOS Remote Machine Name Table

    Name                Type             Status
    -----
    USER                 <00>             UNIQUE          Registered
    WORKGROUP            <00>             GROUP           Registered
    USER                 <20>             UNIQUE          Registered
    MAC Address = 00-11-43-3A-DE-B5

C:\>
```

Host Name

MAC Address

كما يمكنك ايضا ان تتعرف على العديد من المعلومات الهامة مستخدما مفاتيح الأمر المختلفة عن طريق كتابة هذا الأمر في Command Line

```
C:\>Nbtstat /?
```

## FTP Utility

كما تعرفت عليه مسبقا هو File Transfer Protocol والذي سوف نستخدمه لنقل الملفات بين الأجهزة او الـ Servers او من جهازك إلى الـ Server على الإنترنت وله اوامر كثيرة ويمكنك ان تستخدم إما الـ FTP عن طريق الـ Command Line او تستخدم برنامج خاص مثل CuteFTP وهو برنامج شهير جدا للتعامل مع الـ FTP.

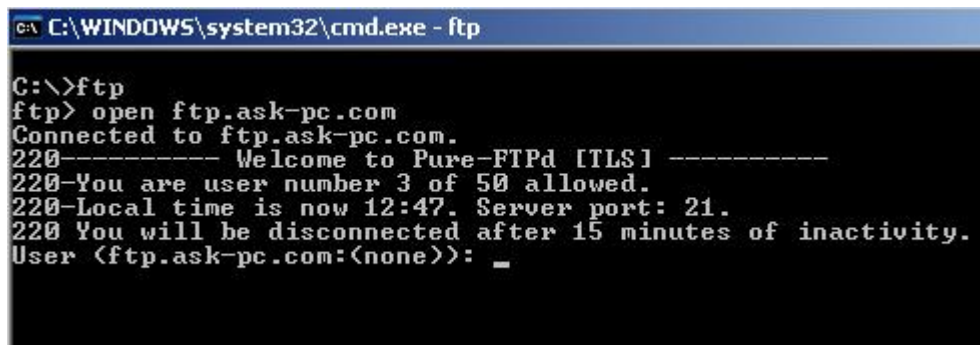
ولكن سوف نعطي مثالا لإستخدام الـ FTP عن طريق الـ Command Line فقط اذهب إلى Command Prompt واكتب الأمر التالي:

```
C:\>FTP
```

سوف يفتح لك الـ FTP يمكنك ان تكتب الأمر التالي

```
FTP>open ftp.ask-pc.com
```

سوف يطلب منك بعد ذلك ادخال اسم المستخدم وكلمة المرور للدخول إلى الـ FTP



```
C:\WINDOWS\system32\cmd.exe - ftp
C:\>ftp
ftp> open ftp.ask-pc.com
Connected to ftp.ask-pc.com.
220----- Welcome to Pure-FTPd [TLS] -----
220-You are user number 3 of 50 allowed.
220-Local time is now 12:47. Server port: 21.
220 You will be disconnected after 15 minutes of inactivity.
User <ftp.ask-pc.com:(none)>: _
```

ولإغلاق الـ Connection اكتب الأمر ftp>close  
ولللخروج للويندوز مرة اخرى اكتب الأمر ftp>bye  
وللمعرفة جميع اوامر الـ FTP اكتب الأمر ftp>help

وهناك العديد من البرمجيات كما ذكرنا سابقا يمكنك استخدامها للتعامل مع الـ FTP إلا اننا ننصح بدراسة اوامر FTP على الـ Command Line لتحصل على خبرة في هذا الأمر. والجدول التالي يوضح لك اهم هذه الأوامر مع شرح مبسط

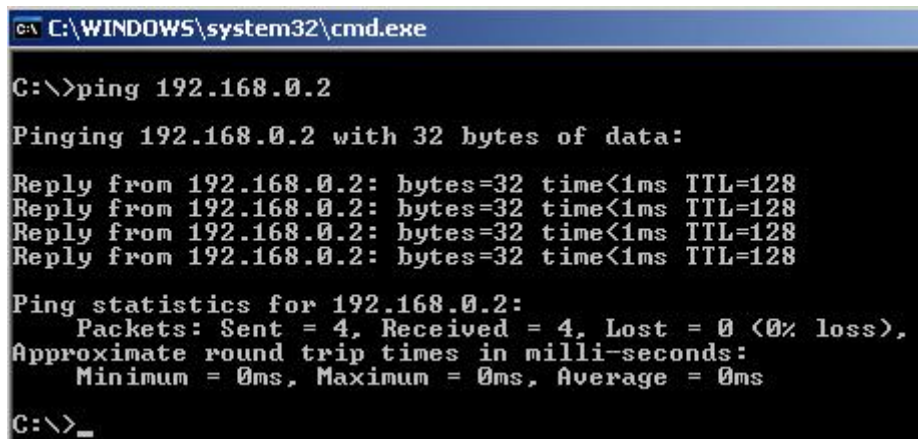
<b>?</b>	<i>to request help or information about the FTP commands</i>
<b>ascii</b>	<i>to set the mode of file transfer to ASCII (this is the default and transmits seven bits per character)</i>
<b>binary</b>	<i>to set the mode of file transfer to binary (the binary mode transmits all eight bits per byte and thus provides less chance of a transmission error and must be used to transmit files other than ASCII files)</i>
<b>bye</b>	<i>to exit the FTP environment (same as quit)</i>
<b>cd</b>	<i>to change directory on the remote machine</i>
<b>close</b>	<i>to terminate a connection with another computer</i>
<b>close brubeck</b>	Closes the current FTP connection with brubeck, but still leaves you within the FTP environment.
<b>delete</b>	<i>to delete (remove) a file in the current remote directory (same as rm in UNIX)</i>
<b>get</b>	<i>to copy one file from the remote machine to the local machine</i>
<b>get ABC DEF</b>	copies file ABC in the current remote directory to (or on top of) a file named DEF in your current local directory.
<b>get ABC</b>	copies file ABC in the current remote directory to (or on top of) a file with the same name, ABC, in your current local directory.
<b>help</b>	<i>to request a list of all available FTP commands</i>
<b>lcd</b>	<i>to change directory on your local machine (same as UNIX cd)</i>
<b>ls</b>	<i>to list the names of the files in the current remote directory</i>
<b>mkdir</b>	<i>to make a new directory within the current remote directory</i>
<b>mget</b>	<i>to copy multiple files from the remote machine to the local machine; you are prompted for a y/n answer before transferring each file</i>
<b>mget *</b>	Copies all the files in the current remote directory to your current local directory, using the same filenames. Notice the use of the wild card character, *.
<b>mput</b>	<i>to copy multiple files from the local machine to the remote machine; you are prompted for a y/n answer before transferring each file</i>
<b>open</b>	<i>to open a connection with another computer</i>
<b>open brubeck</b>	Opens a new FTP connection with brubeck; you must enter a username and password for a brubeck account (unless it is to be an anonymous connection).
<b>put</b>	<i>to copy one file from the local machine to the remote machine</i>
<b>pwd</b>	<i>to find out the pathname of the current directory on the remote machine</i>
<b>quit</b>	<i>to exit the FTP environment (same as bye)</i>
<b>rmdir</b>	<i>to remove (delete) a directory in the current remote directory</i>



## Ping Utility

هذه الأداة أو الأمر من الأوامر الأكثر استخداماً من قبل مديري الشبكات Network Administrators حيث يمكنك هذا الأمر مع اختلاف مفاتيحه من معرفة معلومات عن Host معين أو IP معين دون عناء وبالرغم من وجود برمجيات كثيرة تقوم بعمل هذه الأوامر إلا أنه لا غنى أبداً عن استخدام هذه الأوامر من خلال Command Line ويمكنك هذا الأمر أيضاً من التحقق من وجود Host معين على الشبكة من عدمه أو أنه يستجيب أم لا. ويمكنك استخدامه كالتالي:

```
C:\>ping 192.168.0.2
```



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.0.2
Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>_
```

وتظهر لك النتيجة كما في الصورة بالأعلى إذا كان هذا الـ Host موجود على الشبكة ويستجيب للأمر ويقوم بالرد على الرسالة التي تم إرسالها بالأمر Ping ويمكنك كتابة الأمر /? لعرض قائمة بمفاتيح الأمر وفيما تستخدم.

## Ipconfig Utility

يستخدم هذا الأمر لمعرفة إعدادات الشبكة على الجهاز فقط قم بكتابة هذا الأمر كما يلي

```
C:\>Ipconfig
```

وسوف يقوم بعرض معلومات أو إعدادات هذا الجهاز على الشبكة مثل IP, Subnet Mask, Gateway واسم الجهاز والكثير ولعرض جميع الإعدادات بالتفصيل اكتب هذا الأمر

```
C:\>Ipconfig /all
```

## Tracert Utility

هل فكرت يوما عندما تكتب مثلا [www.ask-pc.com](http://www.ask-pc.com) كيف تنتقل الـ Packet عبر الإنترنت لتصل إلى هذا العنوان ثم تخبر الـ Server بفتح الصفحة؟ هذا الأمر يمكنك من معرفة مسار الـ Packet منذ ان تخرج من جهازك حتى تصل إلى الهدف ويعرض لك جميع الـ Router Interfaces التي تمر بها الـ Packet وهو اختصار Trace Route ولهذا سمي Tracert ويمكنك ان تكتب الأمر كالتالي:

```
C:\>tracert www.ask-pc.com
```

سوف ترى النتيجة بنفسك!

وهذا الأمر مفيد جدا عند حدوث مشكلة ما ولا تستطيع ان تصل إلى موقع ما على الإنترنت او Server معين فيمكنك ان تتحقق اين تقف الـ Packet بالتحديد ولا تكمل المسار.

```
C:\WINDOWS\system32\cmd.exe
C:\>tracert www.ask-pc.com

Tracing route to ask-pc.com [70.85.248.226]
over a maximum of 30 hops:

  0  <1 ns    <1 ns    <1 ns    192.168.0.1
  1  1 ns      <1 ns    <1 ns    host-62-135-114-9.static.link.net [62.135.114.9]
  2
  3  90 ns     83 ns    44 ns    10.171.9.45
  4  8 ns      7 ns     8 ns     172.20.1.33
  5  8 ns      7 ns     7 ns     172.18.1.250
  6  12 ns     11 ns    13 ns    so-0-2-3.0.core1.cai1.flagtel.com [80.77.0.13]
  7  17 ns     11 ns    11 ns    so-0-3-0.0.cjr03.alx001.flagtel.com [62.216.129.186]
  8  12 ns     84 ns    11 ns    62.216.134.26
  9  83 ns     83 ns    84 ns    so-5-3-0.0.cjr02.ldn004.flagtel.com [62.216.129.38]
 10
```

## Telnet Utility

كما عرفت مسبقا هي Terminal Emulation وهي تم ابتكارها من قبل Unix ولكنها ايضا تستخدم من قبل الويندوز للاتصال باي Server يدعم الإتصال عبر Telnet ولتشغيل الأمر

```
C:\>telnet
```

وسوف تبدأ العمل في بيئة Telnet ولعرض الأوامر استخدم العلامة ? وسوف تعرض لك الأوامر المستخدمة في بيئة Telnet.

## Nslookup Utility

هذه الأداة تقوم بتحويل الـ Name Server إلى IP لكي تتمكن من معرفة اي Name يتبع اي IP على سبيل المثال لكي ندخل في بيئة Nslookup ونبدأ في التعامل معه اكتب التالي في Command Line

```
C:\>Nslookup
```

بعدها سوف تظهر علامة بيئة Nslookup وهي كالتالي >  
الآن يمكننا استخدام الأمر فقط اكتب مثلا وانت في هذه البيئة  
>www.ask-pc.com  
وشاهد النتيجة سوف يعرض لك الـ IP الخاص بهذا الـ Name او الموقع  
اي ان هذا الـ IP هو الذي يتعامل معه الـ Browser عندما تطلب الدخول على هذا الموقع

```
C:\WINDOWS\system32\cmd.exe - nslookup
C:\Documents and Settings\MN>nslookup
*** Can't find server name for address 192.168.0.1: Non-existent domain
*** Default servers are not available
Default Server: UnKnown
Address: 192.168.0.1
> www.ask-pc.com
Server: UnKnown
Address: 192.168.0.1
Name: www.ask-pc.com
Address: 70.85.248.226
> _
```

ايضا يمكنك ان تستخدم الأمر set لعرض معلومات عن البريد مثلا او Mail Server على الـ Domain الذي تريده، انت الآن على بيئة الـ Nslookup امام > فقط اكتب التالي

```
>set type=mx
```

ثم بعد ذلك اكتب الموقع مثلا مرة اخرى >www.ask-pc.com وسوف يعرض لك الـ MX Record الخاصة بالـ Host  
للخروج من بيئة Nslookup فقط اكتب الأمر exit

## Overview of Network Operating Systems

سوف نتعرف في هذا الجزء من المنهج على اهم انظمة التشغيل الخاصة بالشبكات وسوف نتعرض لتعريف او نبذة مختصرة عن الأنظمة التالية:

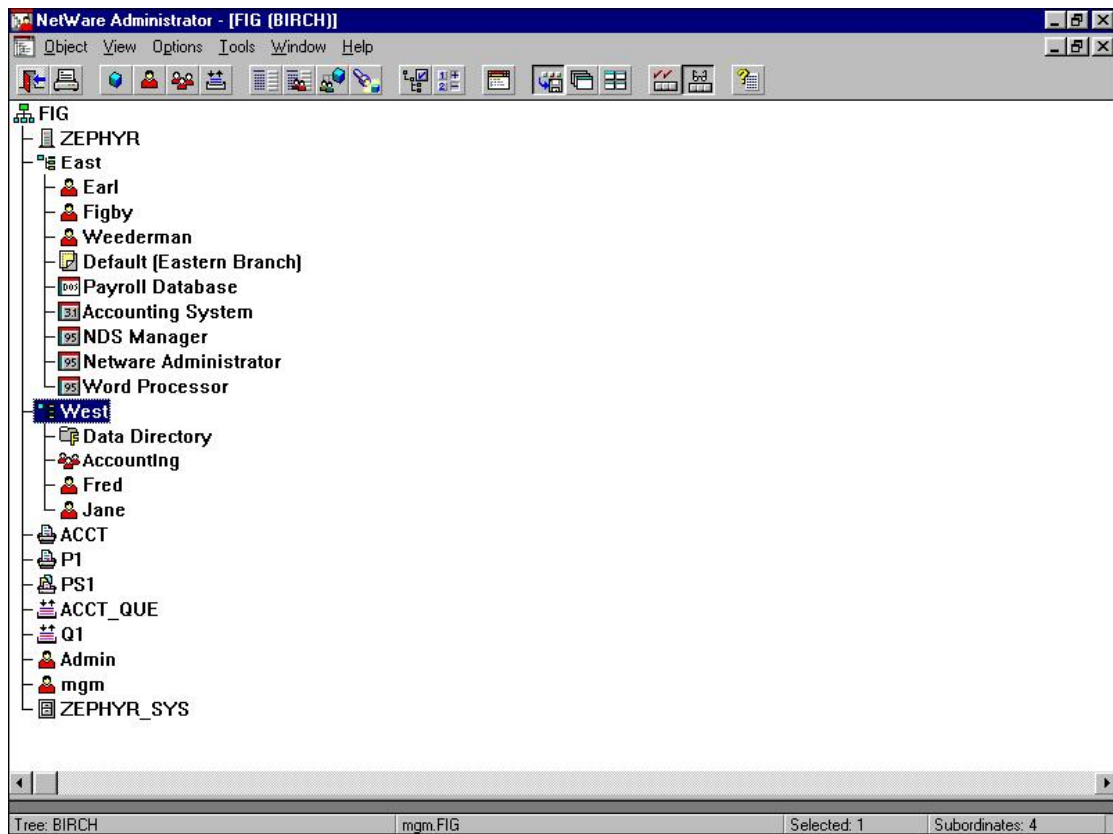
Novell NetWare  
Microsoft Windows NT  
UNIX  
Mac OS

### Novell NetWare

هذا النظام من اكثر انظمة الشبكات واقواها انتشارا هذه الايام وهو تم ابتكاره من قبل Novell واخذ شهرة واسعة نظرا لعمله على اجهزة PC ثم جاء بعد ذلك Windows NT من Microsoft عام 1993 ورغم ان UNIX من اقدم انظمة الشبكات واقواها إلا انه لم ينتشر بقدر انتشار الأنظمة السابقة نظرا لبعض التعقيدات إلا انه بدأ ينتشر هذه الايام بعد ظهور Linux المعتمد على تقنيته ثم نأتي إلى Apple Mac OS وهو يأتي في المرتبة الرابعة من حيث الإنتشار في الإستخدام على الشبكات. إلا ان NetWare من Novell هو من اقوى الأنظمة القادرة على التعامل مع اكثر من مئات الأجهزة على الشبكة بدقة متناهية ويتميز ايضا بسهولة التعامل مع الواجهة User Interface



وكما ترى في الصورة بالأعلى برنامج او ادوات ادارة ومراقبة الشبكات في Novell NetWare إلا انك لا تستطيع تشغيل برمجيات EXE الخاصة بالويندوز على هذا الإصدار ولكن يمكن تشغيل برمجيات الـ JAVA بسهولة. ويدعم NetWare كنظام تشغيل أكثر من ٣٢ معالج او Processor في الكمبيوتر الواحد مما يجعله من أقوى أنظمة الشبكات على الإطلاق ويدعم أيضا تقنية PCI Hot-Pluggable ومعناها انه يمكنك ان تقوم بتركيب وإزالة الكروت بدون اغلاق النظام او اغلاق الجهاز وهذه ميزة هامة جدا في الـ Servers التي تعمل بأنظمة NetWare ويستطيع NetWare التعامل والإتصال مع أي نظام تشغيل آخر مثل Windows, Unix, Mac OS OS/2 والكثير.



يمكنك معرفة المزيد عن NetWare عبر هذا الرابط [من هنا](#)



## Windows NT

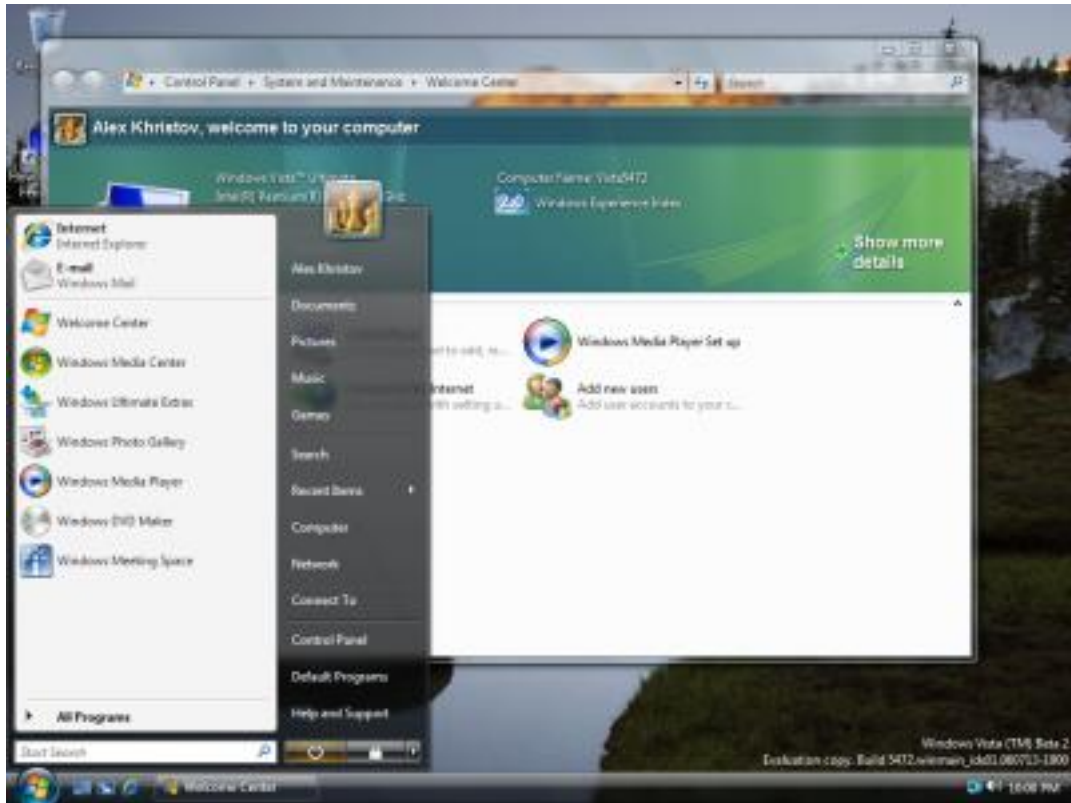
رغم توفر العديد من الانظمة الاخرى من Microsoft بعد هذا النظام إلا اننا سوف نطرق اليه لأنه هو اول نظام انتجته Microsoft عام ١٩٩٣ لإدارة الشبكات كما اسلفنا. وقد اشتهر هذا النظام نظرا لإعتماده على تقنيات Windows 95/98 بالإضافة إلى ادارة الشبكات وايضا نظرا لقرب الشبه الكبير بينه وبين الأنظمة الأخرى من Microsoft فأى مدير شبكات يمكنه ان يتعلمه بكل سهولة وفي وقت ليس كبير مقارنة بالكثير من أنظمة الشبكات الأخرى وايضا يدعم العديد من برمجيات الشبكات الأخرى التي لا يدعمها NetWare مثلا وايضا يدعم التعامل مع NetWare والعديد من أنظمة الشبكات الأخرى



إلا انه في الأونة الأخيرة طرحت Microsoft أنظمة تشغيل متطورة طبقا لتطور الأنظمة الأخرى من Microsoft حيث طرحت Microsoft Windows 2000 Server وايضا Microsoft Windows 2000 Server وايضا Windows XP وقريبا Windows Vista كل هذه الأنظمة مبنية على نواه NT والجدول التالي يوضح تطور NT حسب الإصدار طبقا لـ Microsoft

NT Ver.	Marketing Name	Editions	Release Date	Build
NT 3.1	Windows NT 3.1	Workstation (named just <i>Windows NT</i> ), Advanced Server	July 27, 1993	528
NT 3.5	Windows NT 3.5	Workstation, Server	September 21, 1994	807
NT 3.51	Windows NT 3.51	Workstation, Server	May 30, 1995	1057
NT 4.0	Windows NT 4.0	Workstation, Server, Server Enterprise Edition, Terminal Server, Embedded	July 29, 1996	1381
NT 5.0	Windows 2000	Professional, Server, Advanced Server, Datacenter Server	February 17, 2000	2195
NT 5.1	Windows XP	Home, Professional, IA64, Media Center (2002, 2003, 2004 & 2005), Tablet PC, Starter, Embedded, N	October 25, 2001	2600
NT 5.2	Windows Server 2003	Standard, Enterprise, Datacenter, Web, Small Business Server	April 24, 2003	3790
NT 5.2	Windows XP (x64)	Professional x64 Edition	April 25, 2005	3790
NT 6.0	Windows Vista	Starter, Home Basic, Home Premium, Business, Enterprise, Ultimate	Business: November 2006 Consumer: January 2007	Unknown (the current beta is 5472)
NT 6.0	Windows Server "Longhorn" (codename)	Unknown	2007 (expected)	Unknown
???	Windows "Fiji" (codename)	Unknown	2008 (expected)	Unknown
???	Windows "Vienna" (codename)	Unknown	2011 (planned)	Unknown





والصورة بالأعلى توضح لك صورة من Windows Vista القادم إلى الأسواق قريبا في غضون اشهر وتحديدًا في اوانل 2007.

ومن اشهر الاشياء في Windows هي نوعية الشبكات التي يدعمها وهي اما Workgroup Network او Domain Network والـ Workgroup Network لا تتطلب فقط إلا ربط الأجهزة بالشبكة اما الـ Domain فتحتاج إلى Server لهذا الـ Domain وبعد الإعدادات الهامة الأخرى والتي تحتاج إلى منهج منفصل إلا اننا سوف نحاول ان نتطرق إليها في باب .Installing Network

يمكنك ان تتعرف على اعدادات الشبكة في Windows بمراجعتك لمنهج **Certified Technical**

**Support Engineer** في اكااديمية الكمبيوتر على هذا الرابط

[www.ask-pc.com/academy.php](http://www.ask-pc.com/academy.php)

## UNIX

هذا النظام من اقدم انظمة التشغيل للشبكات على الإطلاق حيث تم ابتكاره في مختبرات Bell عام ١٩٦٩ إلا ان الإصدارات المنبثقة من UNIX والمبنية على الـ Kernel الخاص به قد اخذت في الإنتشار مثل Linux بإصداراته او توزيعاته المختلفة Distributions والـ Linux تم ابتكاره من قبل Linus Torvalds في جامعة هلسنكي في فنلندا عام ١٩٩١ وقد انتج اول نسخة عام ١٩٩٤ وهو يعمل على اجهزة تعتمد معالجات Intel. وهو بالفعل نظام من اقوى الأنظمة التي تتعامل مع الشبكات هذه الايام وبدأت تنتشر بشكل غير عادي نظرا لإقبال المطورين للبعد عن Microsoft! وايضا لأن هذه الانظمة مازالت مجانية ومفتوحة المصدر Open Source. للمزيد عن Linux [اتبع هذا الرابط](#)

## Mac OS

نظام تشغيل Apple Macintosh وهو ايضا نظام قوي ويعتبر من اسهل الانظمة في التعامل مع واجهته الرسومية وتم ابتكاره عام ١٩٨٣ وهو يدعم العمل على اجهزة Mac فقط واليت تعتبر الصديق الوفي للمستخدمين الذين لايملكون الخبرة الكبيرة في التعامل مع الكمبيوتر إلا ان الأمر تغير هذه الأيام بصور Mac OSX وتحول Apple من معالجات Power PC إلى معالجات Intel حيث اصبح هذا النظام من الممكن ان يعمل على اجهزة غير اجهزة الـ Apple والتي اصبحت تعمل بمعالجات Intel للمزيد عن هذا الموضوع [اتبع هذا الرابط!](#)



ويدعم Apple ما يسمى AppleShare للتعامل مع الشبكة ويمكنه ان يتواصل مع أنظمة التشغيل المختلفة على الشبكة ويمكنه ان يعمل كـ Email Server او Print Server او Database Server باستخدام Filemaker Pro. وايضا يتمتع بقدر عالي من الأمان او Security وايضا اكثر ثباتا من نظام Windows لكونه مبني على نواه UNIX.

[للمزيد عن هذا النظام اتبع هذا الرابط!](#)

## Network Installation

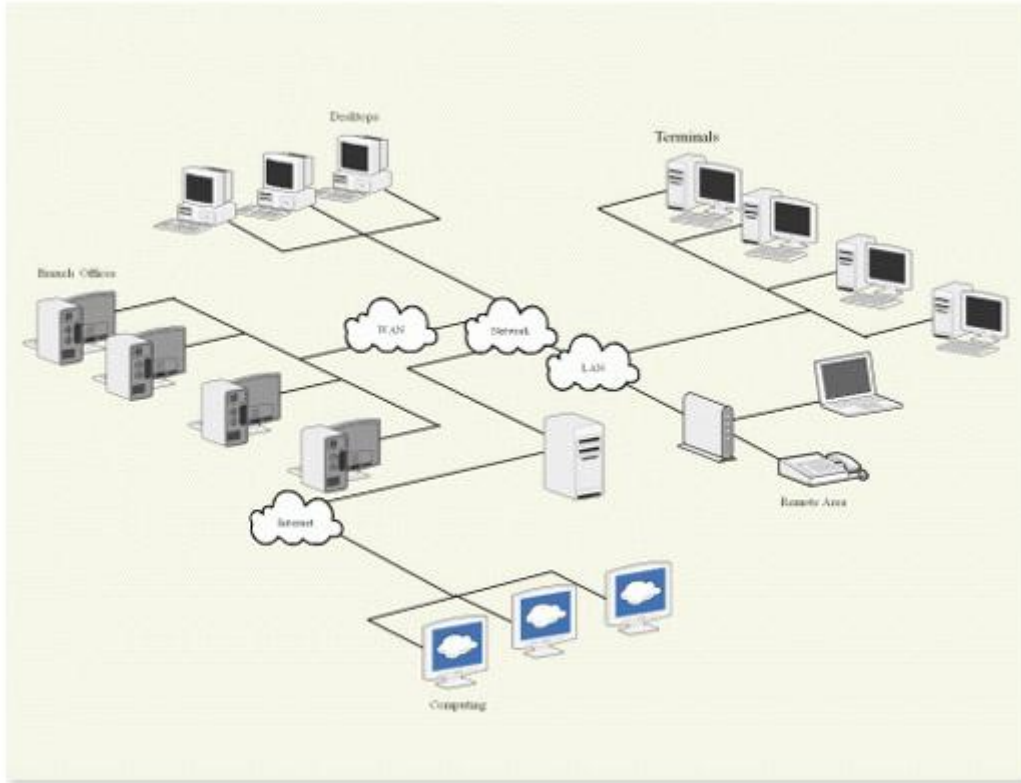
سوف نتعرف في هذا الجزء من المنهج على كيفية تركيب الشبكة بداية من الأدوات المستخدمة وتركيب الـ Hardware والـ Cables نهاية بتركيب الـ Software وتعريف الأجهزة على الشبكة والتعرف على انواع الشبكات في الويندوز وسوف نتناول نظام Windows في هذا القسم حيث انه اكثر الأنظمة شيوعا من قبل المستخدمين اليوم رغم وجود بعض المنافسين مثل Linux.

## Designing Your Network

هذا الجزء من اهم الاجزاء عندما تفكر في تركيب شبكة من اجهزة الكمبيوتر وهو تصميم الشبكة او Network Design وهناك عدة برمجيات سوف تساعدك على اداء هذه المهمة مثل Microsoft Visio او SmartDraw إلا اننا نفضل SmartDraw نظرا لسهولة التعامل ووجود الكثير من الـ Templates المتوفرة بالبرنامج بالإضافة إلى امكانية الحصول على المزيد عن طريق الموقع وللحصول على هذا البرنامج يمكنك الرجوع إلى موقع الشركة من هنا [SmartDraw](#) وسوف تجد في قسم الدروس المتفاعلة في موقعنا بعض التدريبات على هذا البرنامج لتساعدك على فهم كيفية تصميم الشبكة بهذا البرنامج.

ويعتمد تصميم الشبكة على عدة عوامل مهمة كما يلي:

- عدد الاجهزة على الشبكة
- اجهزة الربط Switches
- انظمة التشغيل المستخدمة على الشبكة
- هل الشبكة Workgroup ام Domain
- هل تتصل هذه الشبكة بالإنترنت
- هل هذه الشبكة تستخدم Dynamic IP ام Static IP
- هل لديك مواقع سوف يتم عمل Hosting لها على الشبكة
- هل سوف يكون لديك Mail Server
- هل سوف يكون هناك Storage Devices
- هل سيكون هناك Print Server
- والكثير من العوامل الاخرى التي يتوقف عليها تصميم الشبكة، وسوف نحاول ان ننفذ Case او حالة على ارض الواقع في الجزء التالي لنشرح لك كيف تقوم بتنفيذ وتركيب الشبكة بشكل سليم وسوف نتطرق للعوامل السابقة بشيء من التفصيل.



شكل توضيحي يبين تصميم لشبكة ببرنامج SmartDraw

## Network Components

بعد ان صممت شبكتك وتعلمت الادوات التي سوف تساعدك على التصميم سوف نتناول هنا الاجزاء التي سوف تكون الشبكة المحلية LAN على سبيل المثال وهذا مجرد مثال قد يختلف حسب احتياجات التصميم إلا اننا سوف نتعرض لأهم الأجزاء في تكوين الشبكة.

### NIC

او Network Interface Card او كارت الشبكة كما يطلق عليه مجزاً إذا لابد من توفر هذا الكارت في الأجهزة التي سوف يتم توصيلها على الشبكة ورغم تعدد الأنواع في كروت الشبكات بمعنى أنك سوف تجد كروت Wireless اي لاسلكية وكروت منفصلة تتركب على Motherboard وكروت PCMCIA تتركب في Laptop وكروت Built-in تأتي على اللوحة الرئيسية Motherboard إلا اننا سوف نأخذ على





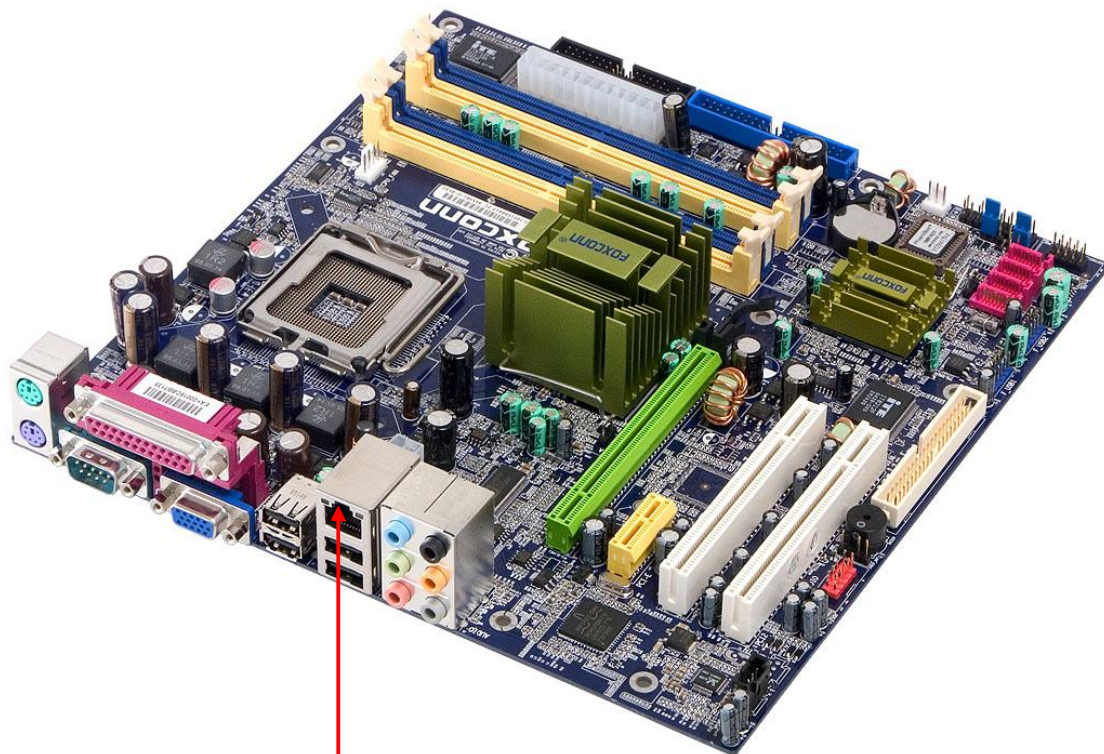
سبيل المثال هنا Built-in LAN Cards



PCMCIA Card



Wireless Network Card

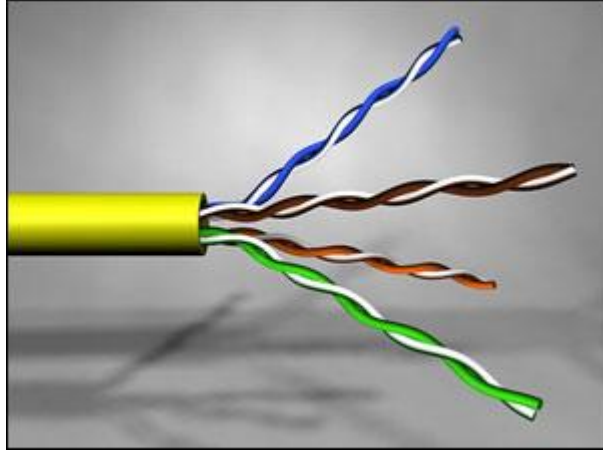


LAN Card

الصورة السابقة توضح شكل كارت الشبكة على اللوحة الرئيسية Motherboard

## UTP Cables

الجزء الثاني من مكونات الشبكة هو الكوابل أو Network cables وسوف نستخدم هنا النوع Unshielded Twisted Pair Cables أو CAT 5 UTP وتتوفر هذه الكوابل في شكل عبوة تحوي عدة امتار من الكوابل حيث يمكنك تقدير المسافات واختيار الأطوال المناسبة حسب المسافة ما بين الـ Node أو الجهاز و الـ Switch إذا كنا نقوم ببناء شبكة من نوع Star. ويفضل ان تحسب المسافات بدقة ولا تقطع الكابل على حسب المسافة بالضبط بمعنى اترك مساحة لاي خطأ قد يحدث



اثاء التركيب لكي لا تضطر إلى الغاء الكابل ككل واعادة عمل كابل جديدة.

## RJ-54 Jacks

هذا هو الجزء الذي سوف يتم تركيبه في النهايات الطرفية لكل كابل من كوابل الشبكة والتي سوف تكون ما بين جهاز الكمبيوتر والـ Switch حيث يتم تركيب الـ RJ-45 في نهايات الكابل وضع في اعتبارك ان الـ RJ-45 Connectors يتم توصيلها في الـ Cable وايضا تجد لها فتحات خاصة في الحائط ايضا تسمى Outlet وهذه الـ Outlets يتم تركيب الكابل الذي يخرج من الـ Switch فيها بطريقة معينة سوف نشرحها لاحقا حيث سنحاول عرض الموضوع بشكل عملي لكيفية تركيب الشبكة وايضا التعرض للمكونات الاخرى المتعلقة بالكوابل مثل الـ Ducts او القنوات التي تمرر فيها الكوابل داخل الحوائط او خارجها.





## Network Switches

هذا الجهاز هو المسؤول عن توصيل الاجهزة ببعضها البعض على الشبكة إذا كنا نقوم بعمل شبكة من نوع Star وتختلف الـ Switches عن بعضها البعض إلا ان الفارق الملحوظ لمعظم العاملين في المجال هو سرعة النقل مثلا 10/100 او 100/1000 وهي كما عرفت مسبقا Mbps 100 او اكثر او اقل حسب نوع الـ Switch ومن الاشياء الاخرى التي تختلف ما بين الـ Switches هي عدد الـ Ports او المخارج التي يمكن توصيل الاجهزة بها فهناك Switches مثلا 8 او 16 او 32 Port او اكثر كما ويمكنك تركيب اكثر من Switch وتوصيلهما ببعضهما ويمكن وضع الـ Switch فيما يعرف باسم RACK للحفاظ عليه وايضا للتبريد وما إلى ذلك وهذه الـ Racks او الصناديق متوفرة بمواصفات مختلفة حسب مواصفات الـ Switch الذي سوف يتم تركيبه به او عدد الـ Switches التي سوف يتم تركيبها في هذا الصندوق كما ويمكنك ايضا تركيب ما يعرف باسم Patch bay وهي يتم تركيبها ما بين الـ Switch والكوابل التي تمتد

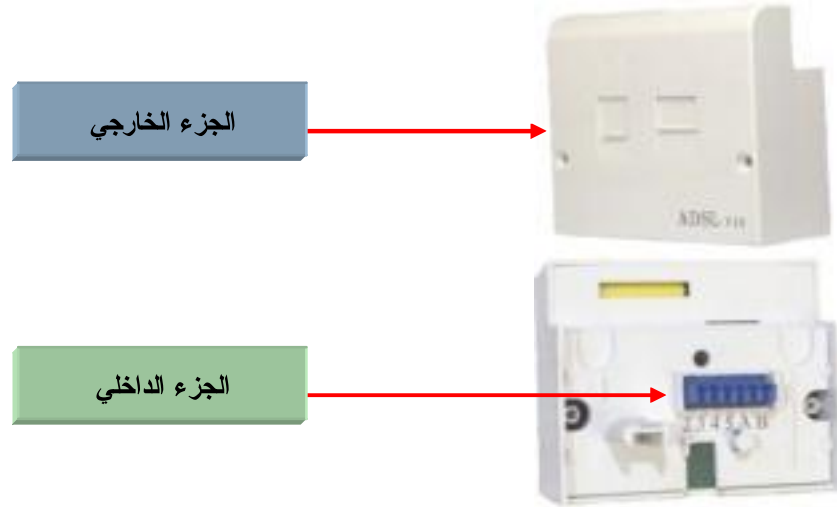


إلى الاجهزة لسهولة التعامل مع الكوابل وايضا سهولة اكتشاف المشاكل المتعلقة بالكوابل.

وتستخدم هذه الانواع من الـ Patch Bays في الشبكات ذات الاحجام الكبيرة والتي تحوي العديد من الاجهزة والـ Switches لتيسير التعامل.

### RJ-45 Outlets

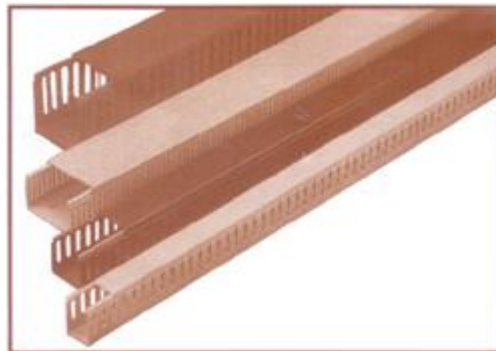
كما شارنا سابقا هذا الجزء سوف نستخدمه حتما إذا اردت ان تقوم بتركيب شبكة بشكل احترافي وهو الجزء الذي يتم تركيبه في الحائط حيث يستلك الكابل من الـ Duct ثم يتم توصيل كابل الكمبيوتر مباشرة بهذا الجزء الـ Outlet "المخرج"



وكما ترى في الصورة ان الـ Outlet تتكون من جزئين الجزء الخارجي والذي يتم تركيب كابل الكمبيوتر به عن طريق الـ RJ-45 والجزء الداخلي الذي يتم تركيب الكابل فيه بشكل مباشر عن طريق اداة معينة سوف نتعرف عليها لاحقا تسمى Punch Down Tool والجزء الداخلي هو الذي يستلم الكابل الذي تم توصيله بالـ Switch من طرفه الآخر.

### Cable Ducts

هذا الجزء هو الذي يتم تمرير الكوابل به على الحوائط في الاماكن التي يعبر فيها الكابل حتى تحافظ على الكابل من الإنقطاع والتلف وايضا بعض الـ Ducts تعزل الكوابل عن المجالات المجاورة مثل المجالات الكهربائية ولمنها باهظة الثمن. والـ Ducts منها ما هو بلاستيكي وايضا معدني ويتم تثبيته في الحوائط عن طريق براغي خاصة بذلك



## Installation Tools

بعد ان قمت بتوفير جميع المكونات السابقة يمكنك الآن البدء في تركيب الشبكة لكن قبل ان تبدأ في التركيب ضع في اعتبارك انك مازلت بحاجة إلى بعض الادوات التي من دونها سوف تصبح عملية التركيب صعبة بل مستحيلة وسوف نتعرف عليها كما يلي:

### Crimping Tool

هذه الاداة تستخدم لتركيب الـ RJ-45 في النهايات الطرفية للـ CAT5 Cables او كوابل الشبكة وهي لها طريقة معينة في تركيب الـ RJ-45 في الكابل حيث يوجد لها مكان مخصص لوضع الـ RJ ثم تقوم بادخال الكابل بالترتيب الصحيح للأسلاك ثم تضغط عليها بضغطة قوية وسوف يتم تثبيت الـ RJ في الكابل كما ترى في الصورة التالية.



وسوف تجد في قسم التدريبات العملية في المنهج مجموعة من التدريبات المصورة "فيديو" لنشرح لك بالتفصيل كيفية تركيب هذه الكوابل والكثير من الاشياء المتعلقة بالشبكات.

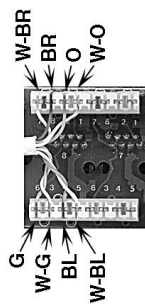
## Network Tester

هذه الاداة يصعب العمل في الشبكات من دونها وهي تستخدم في اختبار الكوابل وتوصيلها هل الكابل موصل بشكل جيد من نهاياته الطرفية ام لا لكي تكون متأكدا من سلامة الـ Cable ويتكون الـ Tester من جزئين الجزء الاول كما ترى في الصورة هو الجزء الذي يحوي زر تشغيل الجهاز وهو يحوي ايضا مكان متوافق لوضع الـ RJ-45 حيث تقوم بوضع بداية الـ Cable في الجزء الاول ونهاية الـ Cable في الجزء الثاني ويحوي الجزئين مؤشرات تومض بنبضات متساوية في كلا الجزئين حيث تخبرك بوجود عطل في الـ Cable في السلك رقم ٢ مثلا لان هذه المؤشرات هي ٨ مؤشرات في كل جزء تختبر ٨ اسلاك في الـ UTP Cable



## Punch Down Tool

تستخدم هذه الاداة في تركيب الكابل من نوع UTP في الـ Patch Bays او في الـ Outlets حيث تعتمد على "حشر" الاسلاك ما بين السنون الخاصة بالـ PORT سواء في الـ Outlet او في الـ Patch bays. وسوف ترى في الصورة التالية بالاسفل توضيح لتركيب الكابل باستخدام هذه الاداة البسيطة.

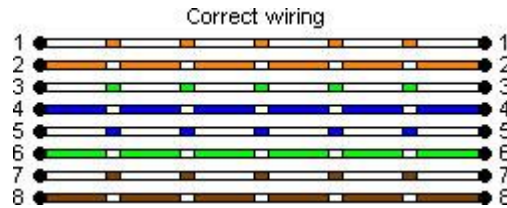


## Network Wiring.

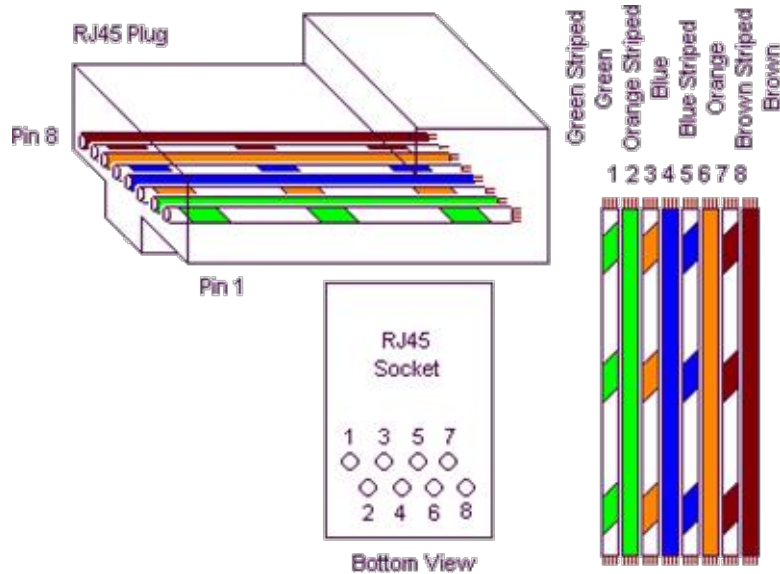
في هذا الجزء قبل ان نبدأ في التركيب لابد ان نتعرف على الشكل الذي يتم ترتيب الاسلاك به لكي نقوم بتركيبها في الـ RJ-45 فكما تعلم بأن الكابل يحوي ٨ اسلاك كل سلك بلون مختلف ولهم ترتيب معين حسب وظيفة الكابل وهذا ما سوف نتعرف عليه في الجزء التالي.

### Straight Cable

هذا النوع من ترتيب الاسلاك هو النوع الافتراضي والذي يستخدم في توصيل الاجهزة بالـ Switch وهو يعتمد ترتيبا معيناً للأسلاك من الطرفين اي ان الطرفين لهما نفس الترتيب كما في الصورة التالية (لاحظ الترتيب بالارقام من ١ إلى ٨)

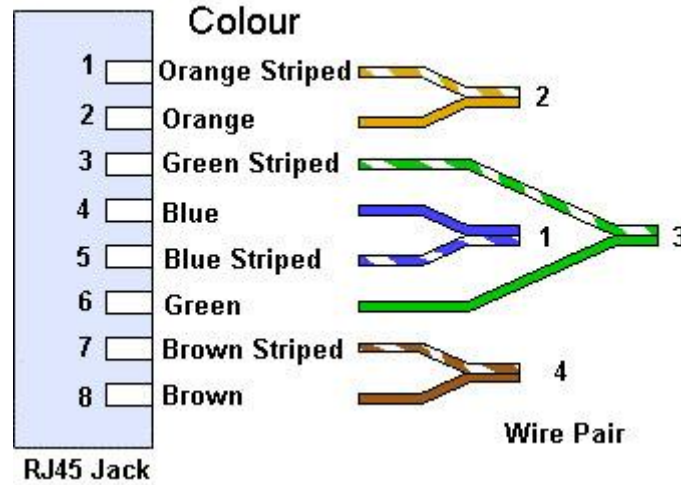


لاحظ ايضا الترتيب في الـ RJ-45 كما في الصورة التالية



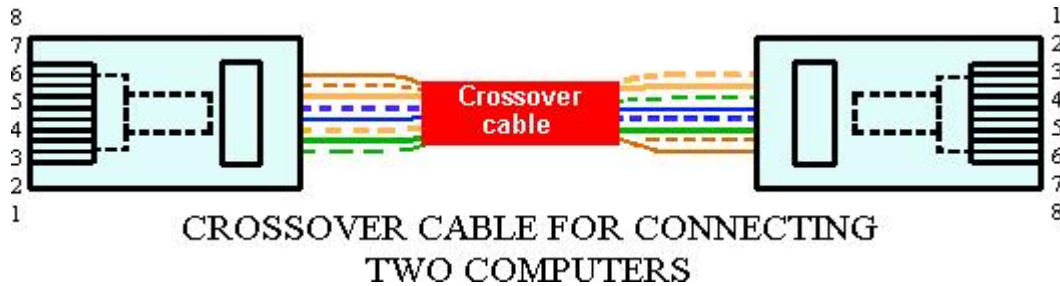
وسوف نتطرق إلى هذا الامر في التدريبات العملية لنساعدك على فهم المنهج اكثر!

والشكل التالي يوضح كيفية تركيب الكابل من زاوية اخرى حيث انه كما تعلم اسلاك الكابل غير متجاورة بالترتيب الذي تريده فسوف تجد صعوبة في عمل هذا الترتيب.

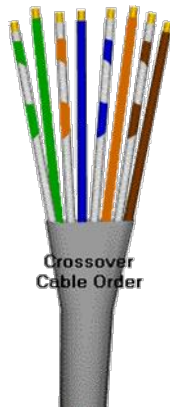


### Crossover Cable

هذا النوع من الكوابل او هذا الترتيب الخاص بالاسلاك يستخدم فقط لتوصيل جهازين كمبيوتر ببعضهما البعض عن طريق LAN Card ولا يستخدم هذا الكابل ابدا في التوصيل العادي او الطبيعي ما بين الاجهزة والـ Switch وهو يختلف في ترتيب الاسلاك في الـ RJ-45



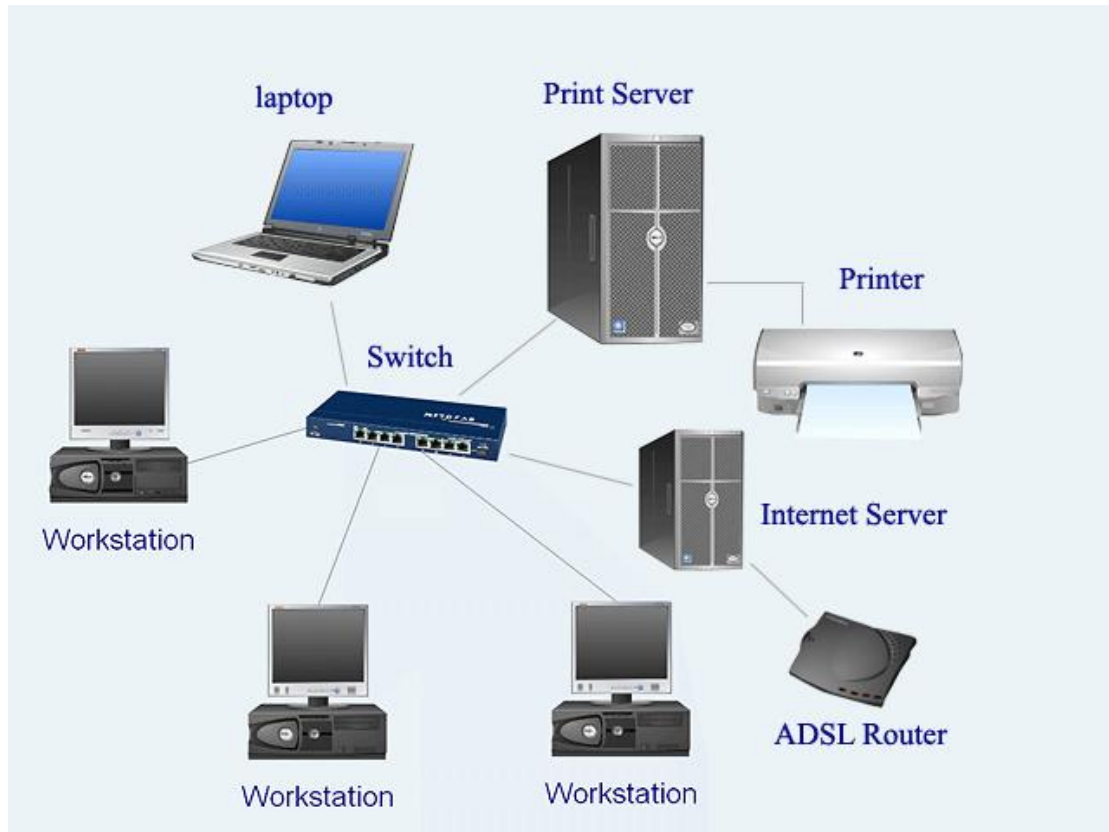
ويتضح اكثر من الشكل التالي. لاحظ ترتيب الاسلاك من اليمين إلى اليسار هذا هو ترتيب الكابل Crossover. وهناك انواع اخرى من الكوابل ايضا مثل Rollover Cable وهو يستخدم للتوصيل بالكمبيوتر احيانا لبرمجة بعض انواع من الـ Routers.





## Installing Network Components

الآن انت جاهز لتكوين جميع اجزاء الشبكة مع بعضها البعض لكي تنتهي من الجزء الخاص بالـ Hardware وسوف نعرض لك فيما يلي شكل للشبكة بعد قمنا بتجميع جميع هذه الاجزاء مع بعضها البعض لتصبح لدينا شبكة جاهزة للعمل ١٠٠% وسوف نأخذ مثال على شبكة بسيطة لكي نفهم الامر ببساطة.



يوضح لك الشكل بالا على تركيب شبكة من طراز Star Topology وتحتوي عدة اجهزة تم توصيلها على Switch عن طريق كوابل UTP وايضا تضم Internet Server للإتصال بالإنترنت وايضا Print Server لأعمال الطباعة ومن ميزات هذا النوع من الشبكات سهولة اضافة اي جهاز آخر للشبكة على سبيل المثال يمكننا اضافة جهاز Network Storage لتخزين البيانات على الشبكة يمكننا ايضا اضافة File Server او اي جهاز آخر بسهولة. لاحظ اننا مازلنا في الجزء الخاص بالـ Hardware والذي يتعلق بتركيب هذه المكونات معا وسوف نتطرق فيما يلي للجزء الخاص بالـ Software.

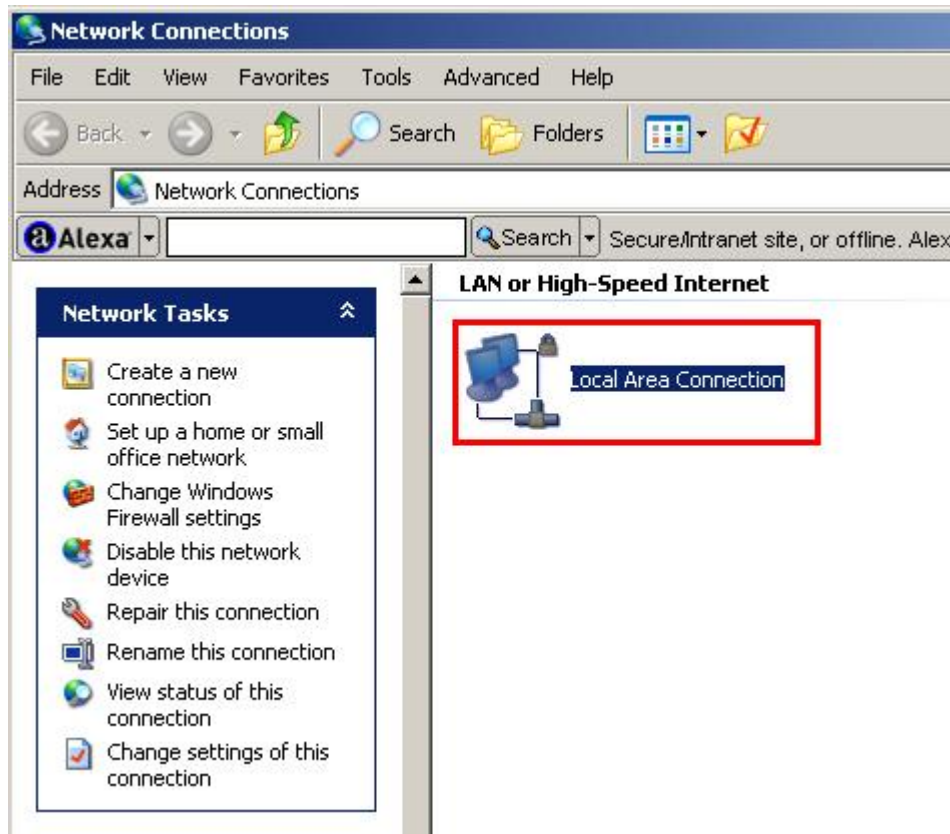


## Configuring Network Devices

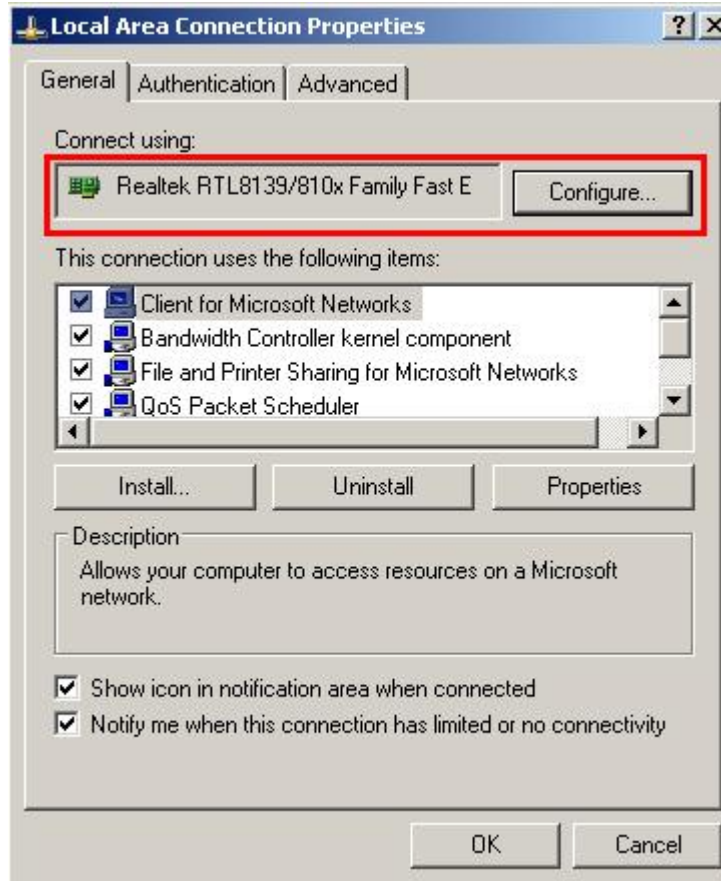
هذا الجزء من المنهج يتعلق بالـ Software او البرمجيات ومالذي يجب ان تتبعه لكي تعمل الشبكة بنجاح بعد قمت بتركيب الجزء الخاص بالـ Hardware بشكل سليم وتأكدت من ان الاجهزة ليس بها مشاكل والكوابل متصلة بشكل جيد وتم اختبارها عن طريق Tester. سوف نستعرض فيما يلي تعريف شبكة من نوع Workgroup باستخدام Windows XP.

### Installing Device Drivers

اول شيء لابد ان تفعله او تتأكد منه هو ان جميع الـ Network cards تم تعريفها على نظام التشغيل بشكل سليم وسوف نتحدث هنا عن نظام تشغيل Windows XP نظرا لانه الاكثر شيوعا وقت كتابة هذا المنهج. وللتأكد من ان الكارت معرف بشكل سليم يمكنك ان تتحقق من ذلك عن طريق الذهاب إلى Network Connections ثم اختر R-Click على LAN Connection كما في الصورة واختر Properties

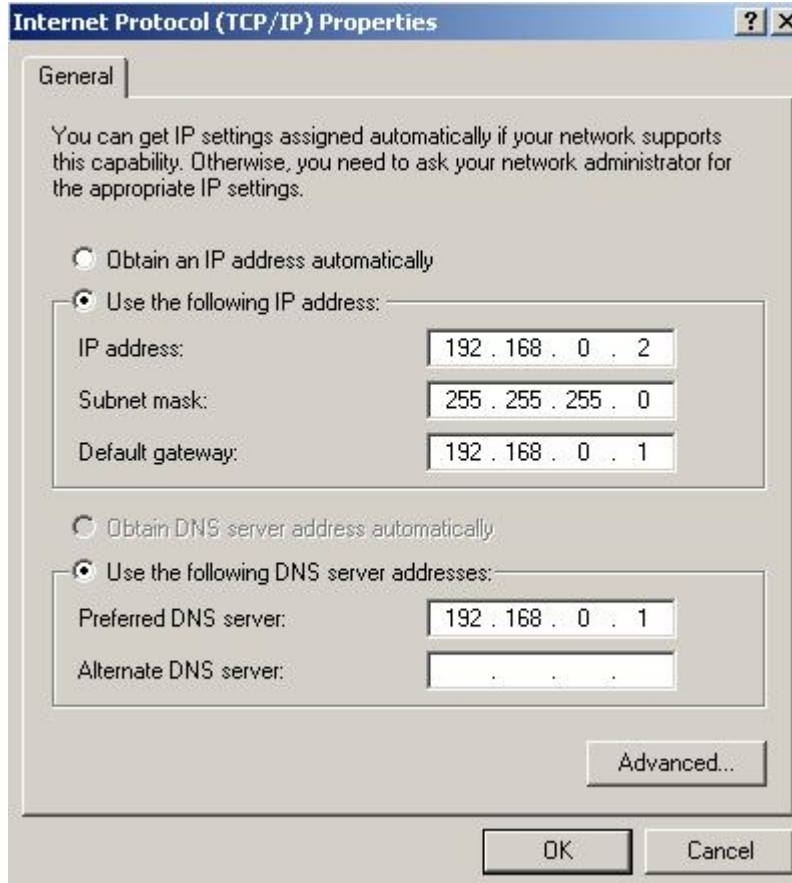


سوف تظهر لك نافذة تأكد من الخيار التالي وان اسم الكارت ظاهر في هذا الجزء كما في الصورة التالية.



### Assigning an IP

بعد ان تأكدت من ان الكروت تعمل بشكل سليم سوف نأتي لأهم نقطة في تعريف الشبكة وهي تعريف الـ IP حيث سنقوم بوضع IP Address محدد لكل جهاز على الشبكة وكما هو معلوم اننا نعمل على شبكة الآن من Class C فلهذا سوف نبدأ العد في الـ IP بالرقم التالي 192.168.0.1 ولاحظ ان هذا الرقم إذا كان لديك Internet Server او Gateway فاعطه هذا الرقم ليكون اول جهاز على الشبكة ثم تبدأ في باقي الاجهزة تباعا 192.168.0.2 وهكذا حتى 192.168.0.254 متبعا الترتيب الخاص بـ Class C Network لاحظ ايضا ان الرقم 192.168.0.1 هو فقط Internal Routing داخل الشبكة. ولتعريف الارقام الخاصة بالاجهزة فقط اختر الخيار السابق لفتح اعدادات الشبكة ثم اختر Internet Protocol واختار Properties سوف تفتح لك النافذة التالية



كما تلاحظ IP Address وضعنا الرقم المميز للجهاز مثلا 192.168.0.2 وبما انك تعمل على هذا الترفيم فسوف يقوم الويندوز اوتوماتيكيا بتعريف الـ Subnet Mask على انه 255.255.255.0 اما خانة Default Gateway فسوف تضع فيها الرقم المميز الخاص بالـ Gateway او الـ Internet Server كما اشرنا مسبقا وهو سوف يكون 192.168.0.1 هذا للرقم الداخلي اما للرقم الخارجي فسوف نتطرق إلى ذلك بالتفصيل فيما بعد عن بناء الـ Internet Server.

### Assigning Computer Name

لن تعمل الاجهزة بشكل سليم على الشبكة إلا اذا كانت لها اسماء مختلفة اي كل جهاز له اسم مميز فتأكد من ذلك عن طريق الذهاب إلى My Computer واختر R-Click ثم Properties ثم اختر Computer Name سوف تظهر لك النافذة التالية:

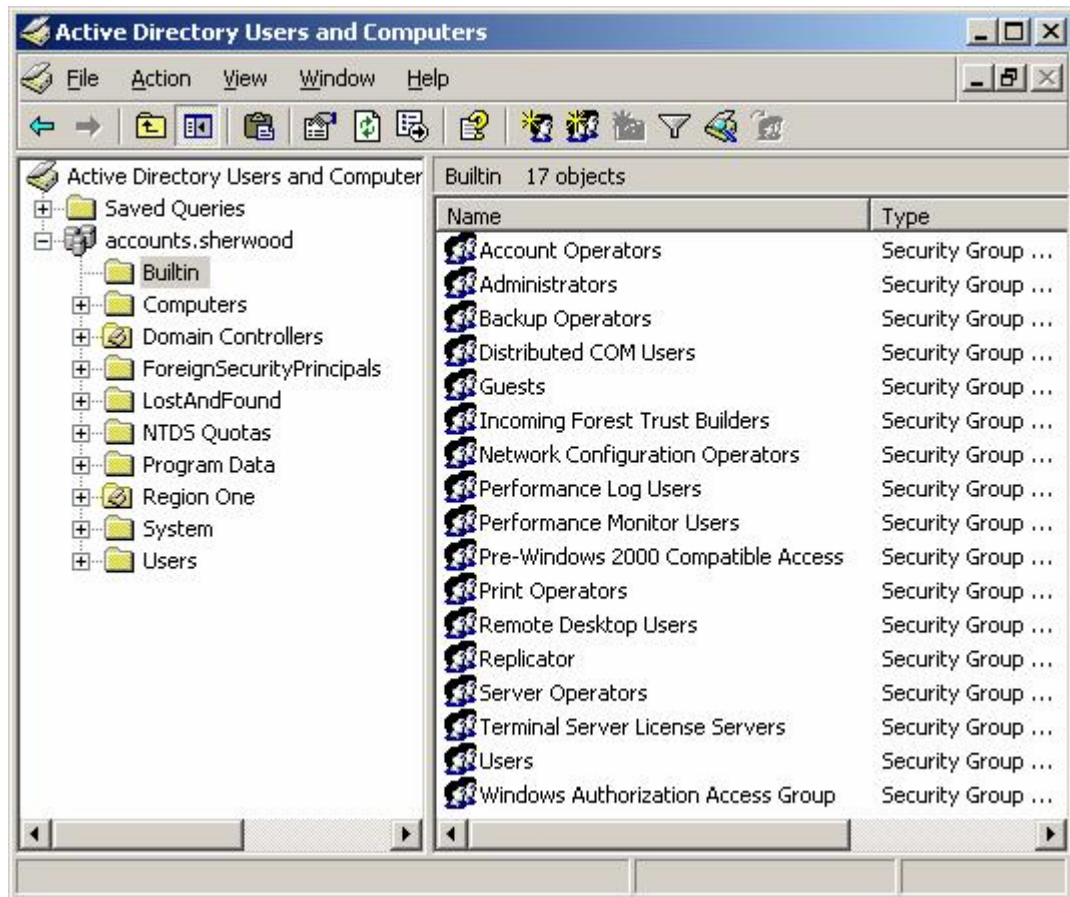


يمكنك ان تختار من هذه النافذة Change لتغيير اسم الكمبيوتر على الشبكة وايضا الاختيار فيما إذا كان هذا الجهاز يعمل على Workgroup او جزء من Domain Network كما يتضح من الصورة المقابلة.



وتعتبر الشبكات من نوع Domain اكثر تعقيدا من Workgroup في ادارتها إلا انها اكثر امنا وتحتاج إلى Domain Server وتعتمد على تقنية Active Directory والتي توجد في Windows Server Edition على سبيل المثال Windows Server 2003 و Windows 2000 Server

وفيما يلي صورة توضح الـ Active Directory في Domain Network



ولمزيد من التفاصيل عن **Windows Networking** ننصحك بمنهج **Certified Technical Support Engineer** على موقعنا على هذا الرابط [www.ask-pc.com/academy.php](http://www.ask-pc.com/academy.php)

### Testing Network Connectivity

الان بعد ان قمت بتعريف الاجهزة وما إلى ذلك سوف تقوم بالتأكد من ان الاجهزة تعمل بكفاءة على الشبكة يمكنك عمل التالي:

اختر Start → Run → cmd ثم Enter

حاول الوصول من اي جهاز إلى جهاز آخر يحمل رقما معيناً عن طريق هذا الأمر

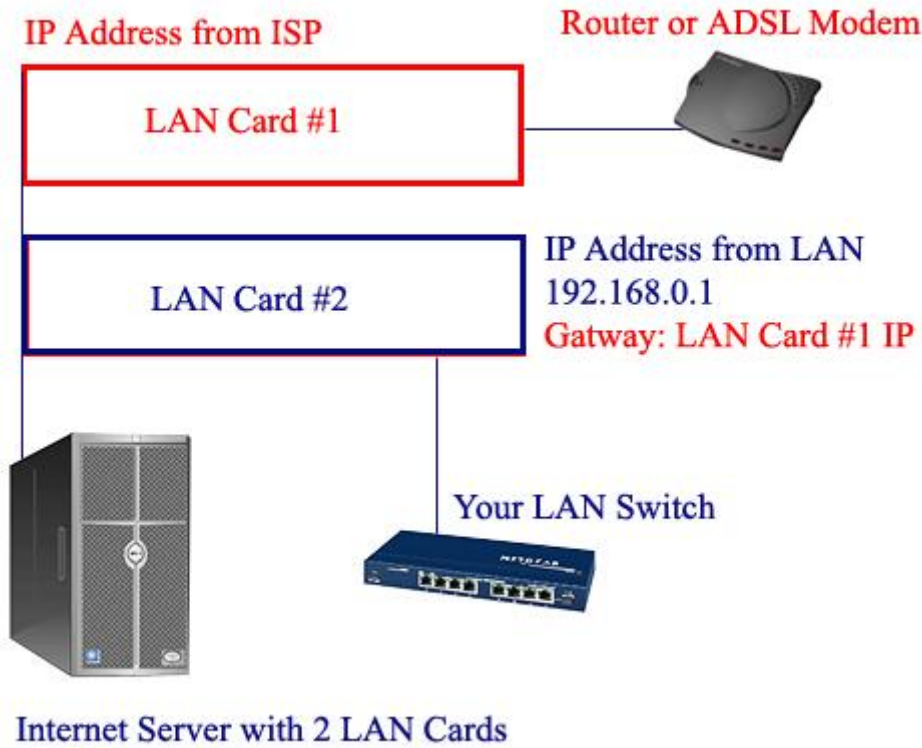
Ping 192.168.0.3

او يمكنك كتابة هذا الأمر net view وسوف ترى جميع الاجهزة على الشبكة او عن طريق اختيار My Network Places من Windows XP وسوف ترى الاجهزة على الشبكة.



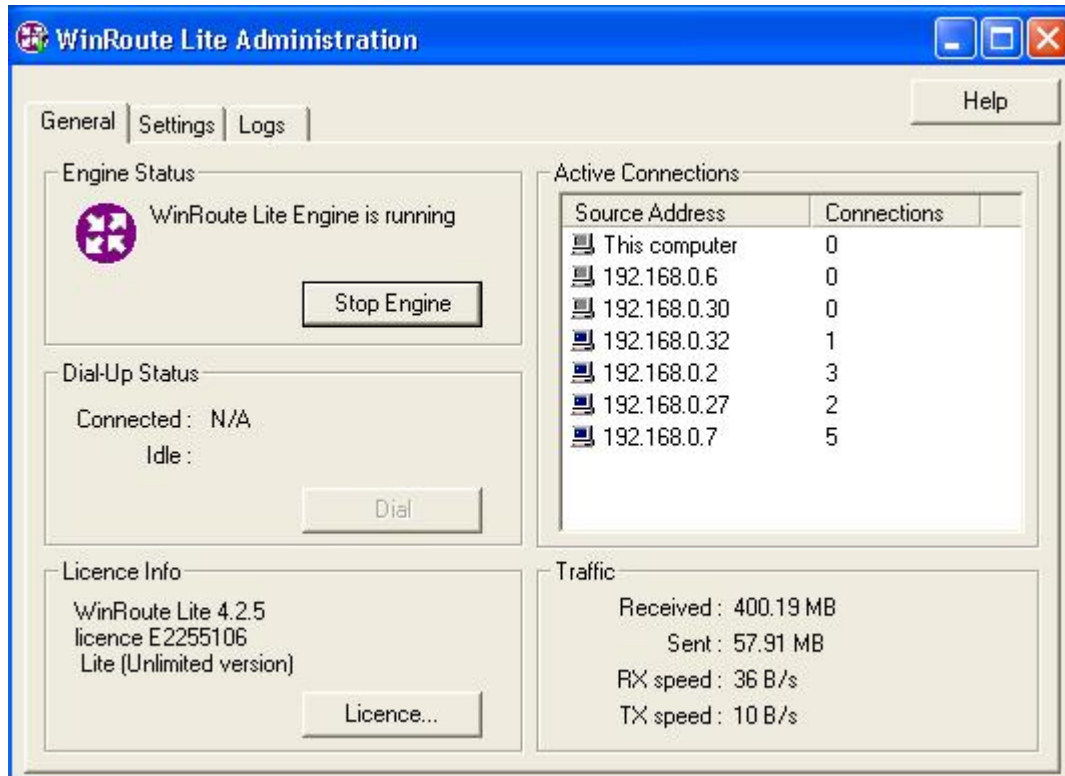
## Setting up Internet Server

في هذا الجزء من المنهج سوف نتعرف على طريقة بسيطة لتعريف Internet Server او Gateway على الشبكة ولكن ماهي وظيفته؟  
لفرض انك تريد الإتصال بالإنترنت عن طريق شبكتك ف لديك خيارين اما ان تقوم بتوصيل الـ Switch مباشرة بـ ADSL Router او مصدر Internet وبهذه الطريقة سوف تكون جميع الاجهزة على الشبكة تستطيع الدخول على الإنترنت! وهذا بالطبع لن يكون عامل امان وسيتسبب في الكثير من المشاكل لكن ماذا لو اردت ان تتحكم في الامر بعض الشيء؟  
هناك عدة طرق لكن اسهلها في الإدارة هي عمل Internet Server او Internet Gateway وسوف نتعرف في الخطوات التالية على كيفية عمله.



من الشكل السابق يتضح لك بأن الجهاز الذي سوف يعمل كـ Gateway سوف يحوي 2 LAN Cards كل منهم له الـ IP الخاص به وكما ترى LAN Card #1 هو الكارت الذي سوف يتم توصيله بالـ ADSL Modem وهو المسؤول عن الإتصال بالإنترنت وهو يأخذ رقم IP الخاص به من مزود الخدمة ISP وليس هناك اية اعدادات اخرى تخصه.

اما الـ LAN Card #2 فهو الكارت المسؤول عن توصيل هذا الجهاز او الـ Gateway بالشبكة المحلية وهو يأخذ الـ IP طبقا لترقيم الاجهزة في شبكتك وغالبا سوف يكون الجهاز رقم واحد على الشبكة بالرقم 192.168.01 ولكن لاحظ جيدا ان هذا الكارت LAN Card #2 الـ Gateway الخاص به هو الـ IP Address الخاص بـ LAN Card #2 حيث يعمل بهذا الشكل الإنترنت على الـ LAN CARD #1 والشبكة المحلية على LAN CARD #2 مع عمل Gateway لكي نقوم بإمداد الأجهزة الأخرى بالإنترنت ونتحكم فيها. ولكن حتى الآن لم تتم عملية الـ Routing بشكل فعلي ١٠٠% اي لم تصل الإنترنت للأجهزة الأخرى على الشبكة، فكيف اذا نقوم بذلك؟ في هذه الحالة انت تحتاج إلى Routing Software يقوم بنقل الإنترنت من LAN Card #1 إلى LAN Card #2 وسوف نستخدم هنا على سبيل المثال برنامج شهير يسمى [WinRoute](#) حيث يقوم هذا البرنامج بمشاركة الإنترنت او Internet Sharing



وباستخدامك لهذا البرنامج فسوف تشارك الإنترنت مع جميع الاجهزة على الشبكة اي سوف تفتح الـ Traffic من جميع الاجهزة على هذا الجهاز او الـ Gateway.

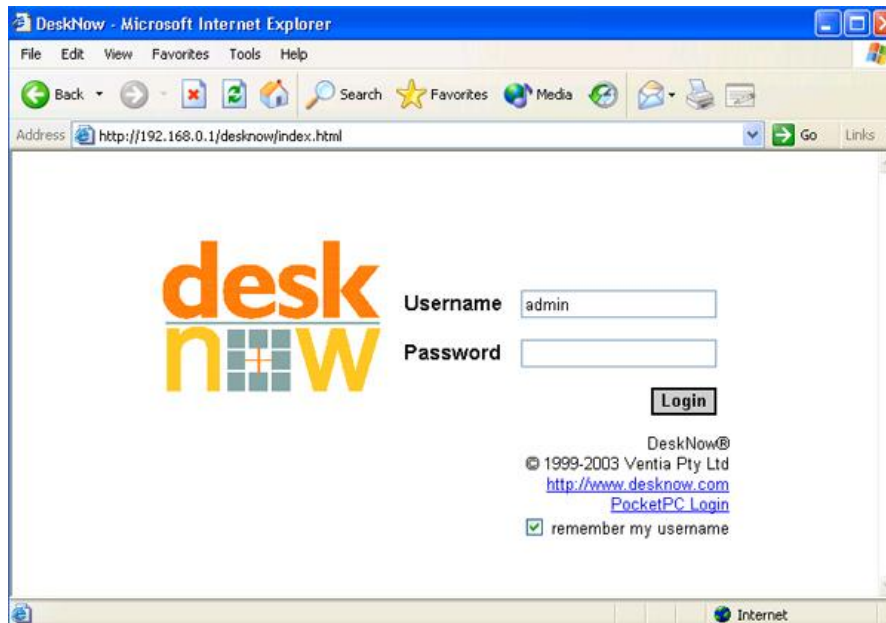
لكن هل من وسيلة للتحكم في الاجهزة والسماح للبعض حجب الآخرين من الدخول على الإنترنت؟



بالطبع هناك عدة طرق وليس طريقة واحدة يمكنك استخدام برنامج مثل ISA Server للتحكم في هذا الامر ويمكنك ايضا استخدام Firewall مثل [MacAfee Personal Firewall](#) حيث تستطيع عن طريق هذا البرنامج حجب الـ IPs التي لا تريد دخولها على الإنترنت وايضا تحديد الـ IPs التي تعتبر Trusted عن طريق اختيار اما Banned IP او Trusted IP. والآن انت لديك شبكة ومتصلة على الإنترنت ويمكنك التحكم في كل ما عليها من اجهزة.

### Setting up your Email Server

هل فكرت في اضافة خاصية الرسائل الإلكترونية إلى شبكتك؟ هناك عدة طرق مختلفة لإتاحة هذه الخدمة داخليا في الشبكة المحلية او LAN عن طريق ما يسمى Email Server وتستخدم تقنيات كثيرة في هذا الموضوع اما عن طريق [Exchange Server](#) من Microsoft او عن طريق العديد من البرمجيات الأخرى المتوفرة على الإنترنت منها ماهو مجاني ومنها مايتكلف مبالغ باهظة حسب الإمكانيات المتاحة مثل [WorkgroupMail](#) وسوف نستعرض في هذا الجزء من المنهج احد هذه البرمجيات المجانية والتي يمكنك استخدامها ببساطة وتركيبها بسهولة على الجهاز المخصص كـ Email Server وهو برنامج [DeskNow](#) يمكنك تركيبه على الجهاز بسهولة بعد ذلك عندما يتم التركيب يمكنك دخول هذا البرنامج عن طريق متصفح الإنترنت بكتابة رقم الـ IP الخاص بالجهاز او الـ Email Server

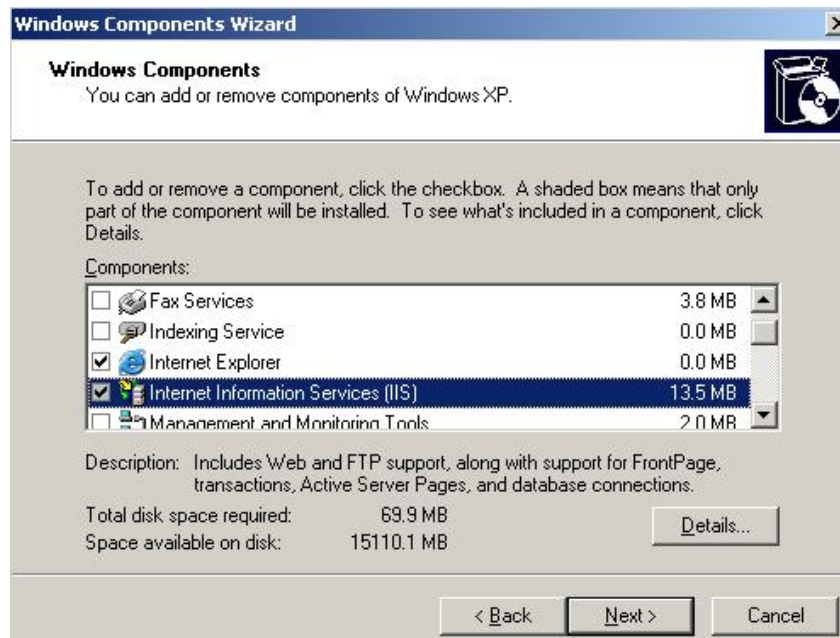


يمكنك التعرف على العديد من Mail Servers [على هذا الرابط!](#)

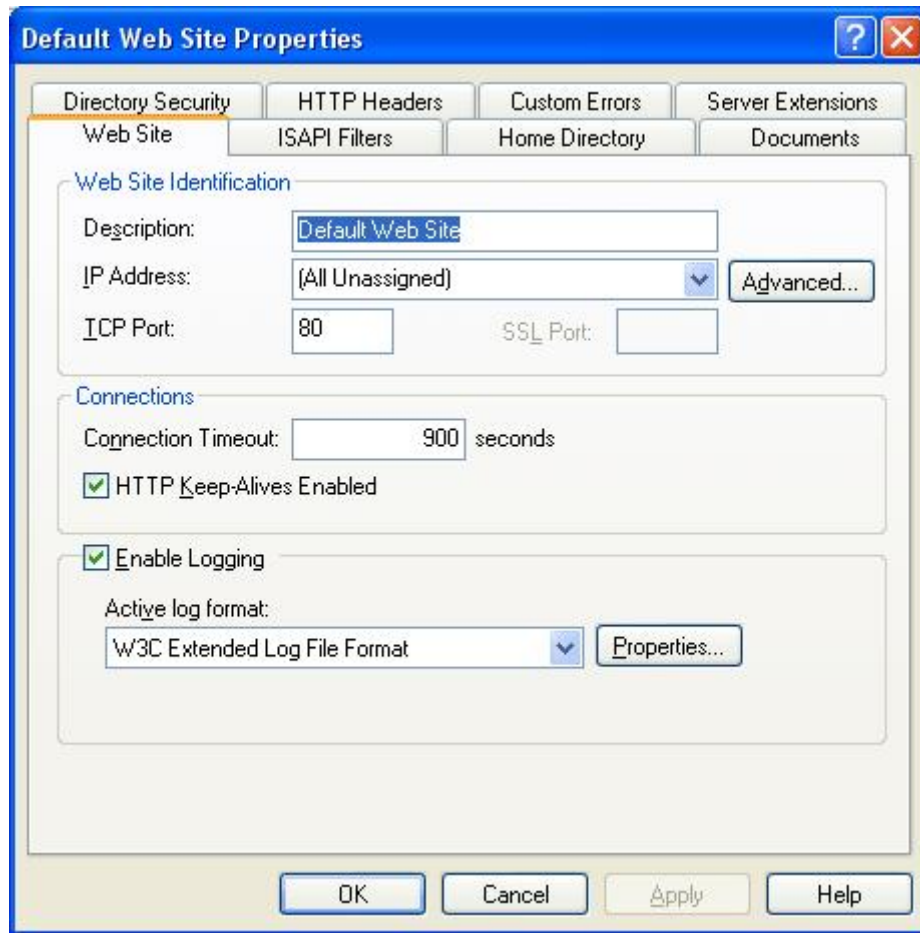
ويمكنك ادخال كلمة المرور الخاصة بالـ Administrator والبدء في اضافة Accounts للمستخدمين في شركتك على شبكتك المحلية عن طريق Administration واطافة New Accounts وتستطيع تعريف هذا الـ Account على برنامج Outlook Express او Outlook عن طريق تعريف المستخدم وسوف يكون الـ POP3 هو نفس رقم الـ IP الخاص بالـ Email Server او اسم الجهاز الذي يعمل كـ Email Server وايضا هو نفسه سوف يكون SMTP في اعدادات الـ Account في الـ Outlook Express.

### Setting up your Web Server

سوف نتحدث في هذا الجزء من المنهج عن كيفية عمل Web Server داخلي على شبكتك حيث تستطيع عمل Hosting لمواقعك لتجربتها على الشبكة المحلية قبل وضعها على الإنترنت او حتى يمكنك ان تقوم بعمل Hosting لمواقعك الفعيلة عليه إذا كنت تمتلك Static IP من ISP او مزود خدمة الإنترنت إلا ان هذا الامر يتطلب دراية عالية بإدارة الخادم ومواصفات خاصة في الجهاز وامن المعلومات وتكلفة عالية فلا ننصحك بذلك ولكن استخدم هذا الامر في تجربة مواقعك على الشبكة المحلية LAN قبل وضعها على الإنترنت. يمكنك عمل ذلك عن طريق IIS او Internet Information Services الموجود في Windows XP Professional والذي يعمل كـ Web Server حيث يمكنك تفعيل هذه الخاصية على الجهاز الذي تريد ان يكون Web Server على الشبكة عن طريق الذهاب إلى Control Panel ثم Add/Remove Programs ثم اختر Windows Components واختار IIS كما في الصورة التالية



وعندما تقوم بتعريف IIS سوف تجد مجلدا يسمى wwwroot هذا المجلد هو الذي يمكنك ان تضع فيه المواقع التي تريدها ان تكون Hosted على الشبكة المحلية عن طريق هذا الـ Web server مثلا اذا كان لديك موقع يسمى test موجود في هذا المجلد ورقم الـ IP الخاص بهذا الجهاز 192.168.0.6 فيمكنك الوصول اليه عن طريق كتابة هذا العنوان في متصفح الإنترنت في اي جهاز من اجهزة شبكتك http://192.168.0.6/test ويدعم IIS المواقع بتقنية ASP وقواعد بيانات Access في المواقع الـ Dynamic. ويمكنك الوصول إلى الموقع من نفس الجهاز او Web Server عن طريق كتابة Localhost/test في متصفح الإنترنت. ويحوي IIS العديد من الإعدادات التي تحتاج إلى مجال اوسع للتحديث عنها كما ترى بالاسفل.



## Remote Access Technology

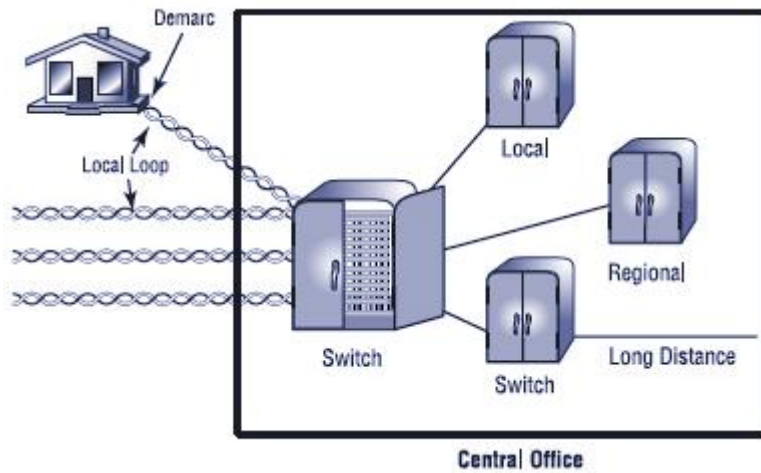
بعد ان انتهينا من الشبكة المحلية سوف نتطرق إلى جزء هام جدا في هذا المنهج وهو الإتصال بالشبكات الاخرى عن بعد عن طريق Remote Access Technologies في الفقرات التالية حيث نتعرف على التقنيات واهم المصطلحات في هذا الأمر.

## WAN Technologies

كما تعلمت مسبقا فإن الـ WAN هي Wide Area Network ولكي تتصل بالـ WAN فسوف تحتاج إلى بعض التقنيات الهامة والتي تساعدك على الإتصال بالعالم الخارجي او Remote Access حيث يتم الإتصال بشبكات WAN. وهناك عدة تقنيات تستخدم في الإتصال هي كالتالي:

### PSTN

وهي اختصار لتقنية Public Switched Telephone Network حيث تستخدم هذه التقنية شبكات التليفون للوصول من الـ LAN إلى الـ WAN واهينا يطلق عليها اسم POTS او Plain Old Telephone Services وهي موجودة في جميع المنازل التي يوجد بها تليفونات



وكما هو واضح من الصورة بالاعلى اتصال المنزل عن طريق شبكة التليفونات بـ Central Office او السنترال كما يطلق عليه والذي بدوره متصل بشبكة تغطي مساحة جغرافية اكبر.

## ISDN

هي تقنية اختصار لـ Integrated Services Digital Network وهي تقنية تعتمد على اتصال رقمي ما بين نقطتين لنقل البيانات وهي قابلة لنقل حوالي 2 Mbps من البيانات بحد أقصى إلا أن الغالب في هذه التقنية هو سرعة 128 Kbps وهي تعتمد على ما يسمى Terminal Adapter والذي يقوم بنقل البيانات عبر النفاذ الرقمية وهو ما يطلق عليه خطأً الـ ISDN Modem وهذه التسمية خطأ لأن الـ ISDN Signal أو الإشارة في الأصل رقمية فلا تحتاج إلى Modem لكي يقوم بالتحويل من Analogue إلى Digital والعكس كمثل الحال في شبكات PSTN والتي تحتاج إلى وجود Modem لأتمام عملية الإتصال.

وتعتمد أيضا تقنية ISDN على Dial-up Technology مثل شبكات PSTN. واهم ما يميز تقنية الـ ISDN عن تقنية PSTN هو أن الـ ISDN يقوم بتقسيم خط التليفون إلى فرعين أحدهما يستخدم للإنترنت والآخر يستخدم للاتصالات العادية أو Voice Call عن طريق جهاز يسمى Line Splitter. وقد ساهمت هذه التقنية في ظهور العديد من التقنيات الأخرى المعتمدة على التكنولوجيا الرقمية مثل xDSL و T-Series و FDDI.

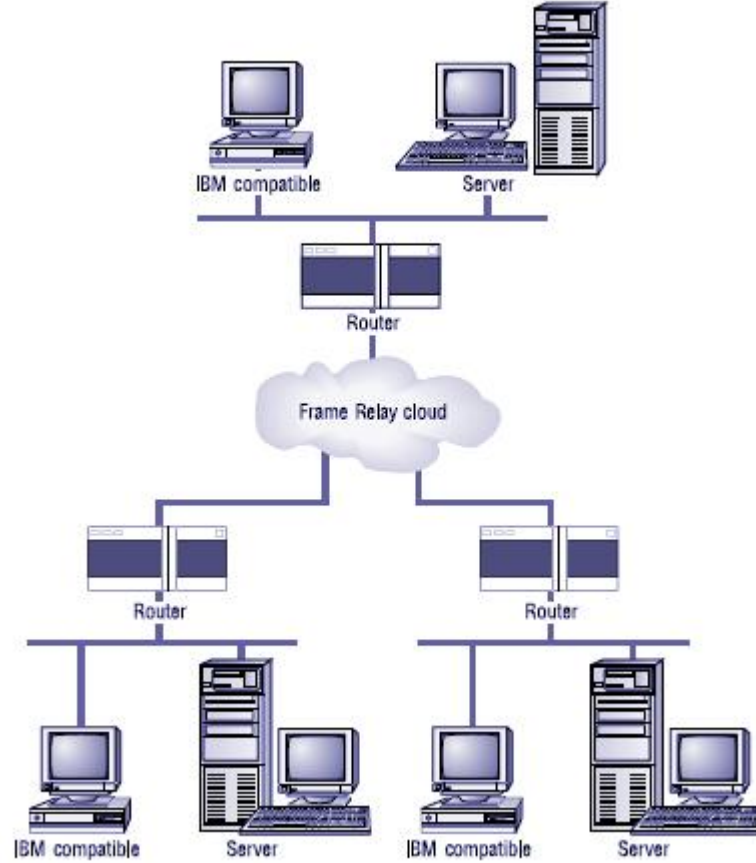
## xDSL

هذه التقنية تعتمد على تكنولوجيا نقل البيانات الرقمية عبر اسلاك النحاس المستخدمة في شبكات الهاتف الحالية وهي رخيصة مقارنة بتقنية مثل T-1 وتقنية xDSL رمزنا لها بالرمز x في البداية لأنها تحوي تقنيات أخرى مختلفة و DSL هي اختصار Digital Subscriber Line أما الـ x فهي تعبر عن بدائل في هذا النظام مثلا HDSL أو High data-rate أو Single line Digital Subscriber Line و SDSL أو Digital Subscriber Line أو VDSL أو Very high data-rate Digital Subscriber Line و ADSL أو Asynchronous Digital Subscriber Line وهو الأكثر شيوعا واستخداما ويدعم سرعات حتى 9Mbps ويمكنك الإتصال عن طريق xDSL Modem أو Router حسب مزود الخدمة لديك ويتم اما توصيله بالـ USB Port الخاص بالجهاز أو LAN Card.

## Frame Relay Technology

هذه التقنية تختلف عن التقنيات السابقة حيث تعتمد على ما يسمى بـ Variable-length packet وهي تقنية خاصة بشبكات الـ WAN وتنقل هذه الـ Packet عن طريق الـ Switching أو التحويل ويتم إرسال الـ Packet عن طريق Routers لاي مكان آخر أو destination به Router آخر مستقبل وهناك ما يعرف باسم Frame Relay Cloud أو

سحابة هي حلقة الوصل ما بين الـ Routers وبالطبع هذه السحابة افتراضية لذا فإن هذه التقنية تعتمد على ما يسمى الدائرة الافتراضية او Permanent Virtual Circuits او PVCs وهي دائرة افتراضية لنقل البيانات على شبكات PSTN (انظر الشكل التالي)



### T-Series Connections

هذه هي خدمة تعتمد على التقنية الرقمية وهي عبارة عن خط رقمي يتم تأجيره من مزود خدمة الاتصالات او من شركة الهاتف مباشرة ويسمى ايضا Leased Line ويمكن ان تستخدم تقنية الاسلاك النحاسية العادية في الهاتف او تقنية Backbone حيث يسمى في هذه الحالة Trunk Line وتستخدم تقنية Time Division Multiplexing او TDM حيث تقسم الـ Bandwidth إلى ٢٤ قناة او Channels بالإضافة إلى Control Line او خط للتحكم ويرمز له بالرمز T-Series حيث يتبع حرف الـ T انواع هذا الخط والسرعات المختلفة كما يتضح من الجدول التالي حيث يقسم الإتصال واقصى سرعة ممكنة لنقل البيانات.



#### T-Series Connections

Connection	Maximum Speed
T1	1.544Mbps
T1C	3.152Mbps
T2	6.312Mbps
T3	44.736Mbps
T4	274.176Mbps

#### ATM

هي اختصار لـ Asynchronous Transfer Mode (وهي ليست ATM Machine او Automated Teller Machine الخاصة بسحب النقود!) ولكنها تقنية في الإتصال وهي تقنية صممت لعمل شبكات عالية السرعة بغض النظر عن الـ LAN Topology وهي تعتمد على تقنية تسمى High Speed Cell Switching والتي تستطيع نقل البيانات وايضا الصوت والفيديو والـ Cell هي المرادف الـ Analogue لـ Frame او Packet وتبلغ سرعة هذه الشبكات حاليا حوالي 51.84 Mbps وايضا 155.52 Mbps وتستخدم عادة في تقنيات الـ Fiber Optics او الاليف الضوئية وقريبا سوف نسمع عن تقنية جديدة تسمى ATM based Fiber Optics والتي قد تصل سرعتها إلى 10Gbps حيث تعتمد تقنية ATM على الـ Hardware اكثر ما تعتمد على الـ Software. كما تعرف ايضا هذه التقنية بتقنية Optical carrier او OC وهي تحوي عدة سرعات مختلفة كما اشرنا والجدول التالي يوضح فرق السرعت المختلفة ما بين الانواع.

#### Common Optical Carrier levels (OC-x)

Level	Data Rate
OC-1	51.84Mbps
OC-3	155.52Mbps
OC-12	622.08Mbps
OC-48	2.488Gbps



## FDDI

هذه التقنية هي اختصار Fiber Distributed Data Interface وتعتمد هذه التقنية على الاليف الضوئية او Fiber Optic Cables لنقل البيانات وتستخدم هذه التقنية غالبا في الـ Backbone او في الشبكات ذات السعة العالية High Bandwidth.

## Remote Access Protocols

هناك بروتوكولات خاصة للاتصال عن بعد ما بين الخادم والجهاز المتصل عن بعد واليك اهم هذه البروتوكولات كما يلي:

### SLIP- Serial Line Internet Protocol

هذه التقنية ابتكرت في معامل جامعة Berkeley في كاليفورنيا وهي تقنية تعتمد على الاتصال بـ TCP/IP عبر Serial Communication او الاتصال التسلسلي مثل الـ Modem في شبكات POTS وهي اصلا ابتكرت من اجل تسهيل الاتصال من قبل نظام تشغيل Unix عام ١٩٨٤ ولكنها لا تدعم التشفير لكلمات المرور مما يعني انها غير آمنة بما فيه الكفاية.

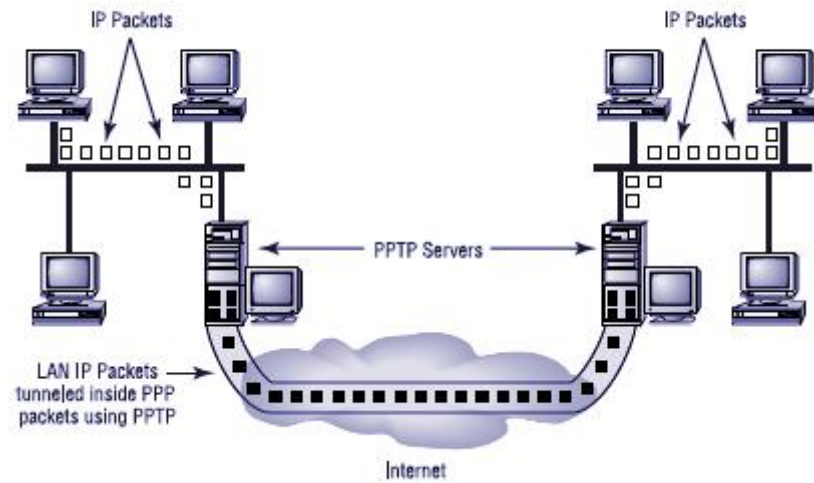
### PPP- Point-to-Point Protocol

هذه التقنية تستخدم للاتصال المباشر بين نقطيتين عن طريق اما Serial او Parallel Connection مستخدمة TCP/IP وهي تستخدم عادة للاتصال عن بعد بمزود الخدمة ISP او بالشبكات المحلية LAN وهي تقريبا قد حلت محل التقنية السابقة وهي ايضا تعتمد على تقنية DHCP او Dynamic host Control Protocol والتي تقوم بتعريف اعدادات الـ TCP/IP اوتوماتيكيا فور الاتصال بالـ Router على سبيل المثال حيث يتم تعريف IP Address, Subnet Mask و DNS Configuration واكثر ما سوف تجد فيه هذه التقنية لو تتذكر استخدامك للاتصال بالـ Modem على Windows 95 مثلا فسوف تجد هذا البروتوكول في الاتصال وهو المسؤول عن الإعدادات المختلفة التي يتم تعريفها اوتوماتيكيا من مزود الخدمة.

### PPTP- Point-to-Point Tunneling Protocol

وهو من ابتكار Microsoft وهذه التقنية تعتمد على ربط شبكتين مثلا عبر الإنترنت بشكل افتراضي او Virtual Connection عن طريق TCP/IP و PPP وتستطيع الشبكتين استخدام الإنترنت كوسيلة اتصال مابينهما لتكوين WAN Link كما تستخدم هذه التقنية طريقة امته في تأمين نقل البيانات عبر الإنترنت تسمى تقنية VPN او Virtual Private Network إلا ان هذه التقنية ليس سهلة في التعامل ولست مقبولة على جميع الـ Servers

A PPTP implementation connecting two LANs over the Internet



والصورة كما ترى توضح اتصال شبكتين عن طريق الإنترنت بواسطة PPTP ومخدمات تدعم هذا البروتوكول.

### RAS – Windows Remote Access Services

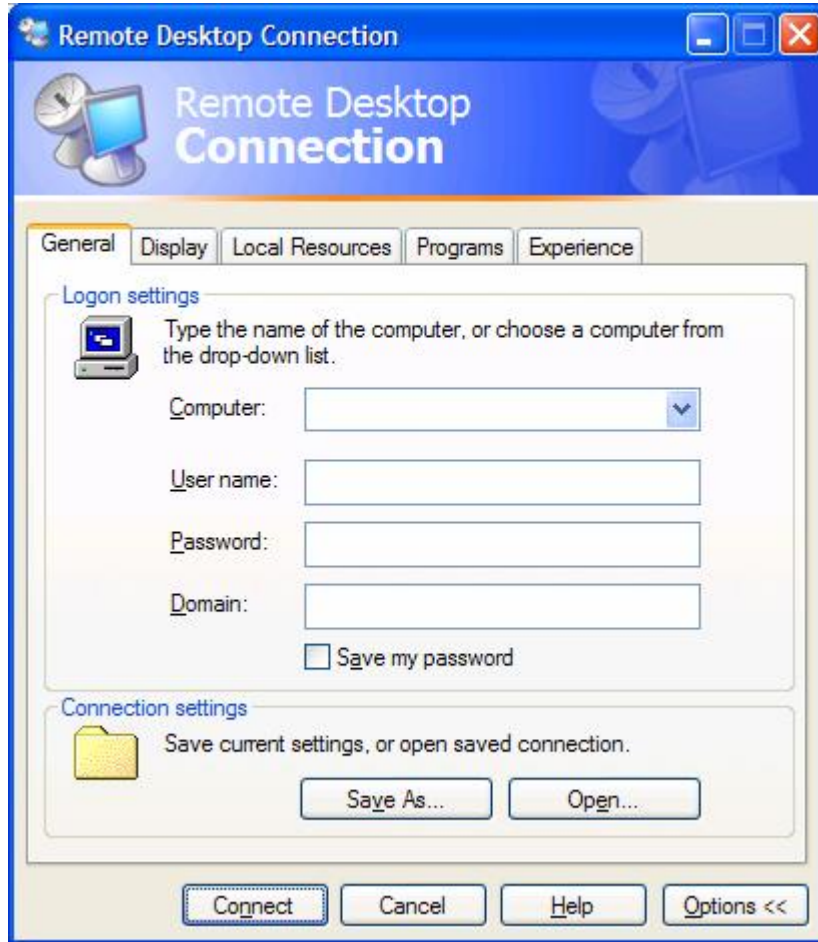
في Windows NT, Windows 2000 تقنية تسمى RAS تستخدم للاتصال ما بين الاجهزة ويمكنك ان تستخدم MODEM في هذه التقنية ولكن ليس للاتصال بالإنترنت بل للاتصال بخادم آخر مثلا عن طريق RAS ولا يمكن استخدام هذا الـ Modem في اتاحة الإتصال بالإنترنت لباقي الاجهزة على الشبكة.

### ICA- Independent Computing Architecture

هذا البروتوكول تم تصميمه من خلال شركة Citrix للاتصال بالمخدمات عبر الشبكة وليس متعلق بنظام معين فهو يعمل على جميع الانظمة تقريبا.

## RDP- Remote Desktop Protocol

تستخدم هذه التقنية للإتصال بالاجهزة التي تعمل بنظام Windows XP, Windows 2003 Server وبدأ استخدامه منذ ظهور Windows 2000 Server حيث تستطيع العمل على الجهاز وكأنما تجلس امامه وتتحكم في جميع امكانياته عن طريق هذه التقنية والصورة بالاسفل توضح لك اكثر. كما ويمكنك الإتصال برقم الـ IP الخاص بالجهاز على الشبكة او باسم الجهاز على الشبكة رغم انه هذا النظام مازال قيد التطوير من ميكروسوفت لوجود بعض الثغرات الامنية.

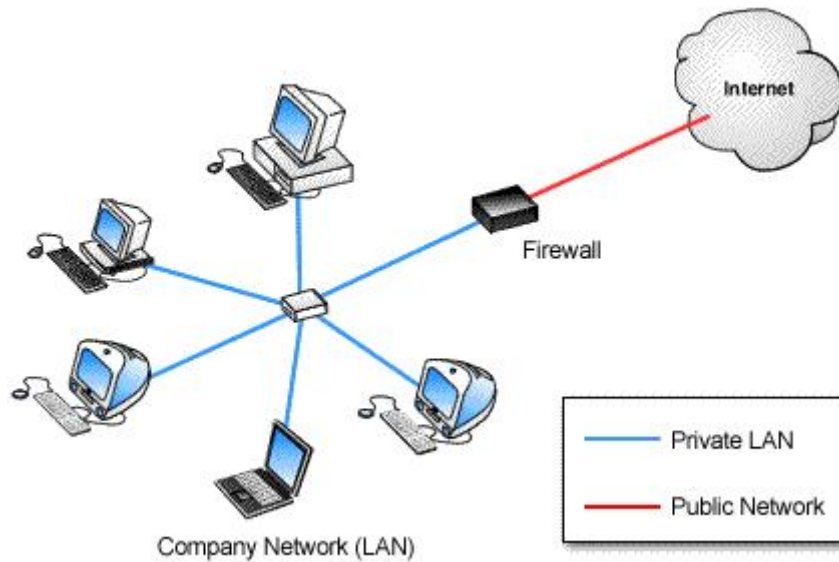


## Basic Network Security

في هذا الجزء من المنهج سوف نحاول التطرق إلى بعض الاساسيات في امن المعلومات والحماية الخاصة بالشبكات لان هذا الموضوع يحتاج إلى مناهج خاصة، فقط اردنا ان نقلي نظرة على هذا الموضوع بشيء من الإختصار لكي تكون ملما ببعض المعلومات عن الحماية.

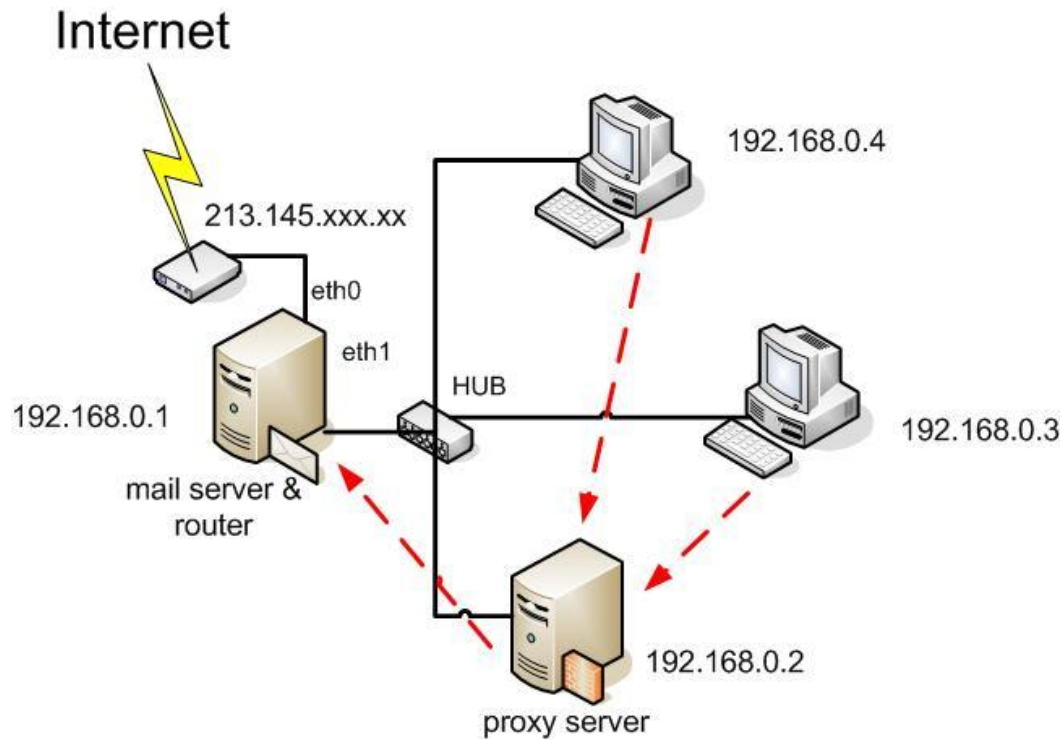
### Firewalls

ال Firewall او الجدار الناري كما يسمى باللغة العربية هو عبارة عن برنامج او Hardware يتم تركيبه في الشبكة لأغراض الامن والحماية حيث يعمل هذا الحاجز او الجدار على صد الهجمات الخاصة بالإختراقات والهاكرز والدخول غير الموثوق لشبكتك او Unauthorized Access ومن اشهر انواع ال Firewall برنامج [ISA Server](#) من ميكروسوفت وهناك ايضا برامج متوفرة مجانا مثل Windows Firewall الموجود في Windows XP على سبيل المثال وهناك ايضا انواع من ال Firewall مثل Personal Firewall و Network Layer Firewall و Network Firewall و Application Layer Firewall. والصورة التالية توضح طريقة العمل بشكل مبسط



## Proxy Server

هو عبارة عن كمبيوتر يقوم باتاحة الإتصال للأجهزة بشبكات أخرى لكن بطريق غير مباشر indirect connection ولنوضح أكثر لنفرض أنك متصل بالإنترنت عن طريق Proxy Server وطلبت معلومات معينة من موقع معين فأن ال Proxy سوف يقوم بإحضار هذه المعلومات من الخادم الآخر وعرضها لك إذا كان مسموح لك بعرضها او يحضرها لك من ال Cache الخاصة به حيث ان ال Proxy Server قد يؤدي إلى زيادة سرعة استعراض المواقع على الإنترنت عن طريق ما يسمى Proxy Cache والتي يخزن فيها المواقع والصفحات الأكثر طلبا من مستخدمي الشبكة وعندما تطلبها فبدلا من ان يحضرها لك من الخادم الخاص بالموقع فسوف يحضرها لك مباشرة من ال Cache. ويسمى هذا النوع بـ Web Proxy وهناك انواع كثيرة من ال Proxy وهو يحتاج إلى منهج منفرد لشرحه.



## Security Protocols

سوف نتناول في هذا الجزء بعض البروتوكولات الخاصة بالحماية وامن المعلومات وهي عدة انواع وتستخدم في حماية نقل المعلومات عبر الشبكة.

### L2TP

هذا البروتوكول يستخدم في الـ VPN عندما لا يوجد دعم للـ TCP/IP وهو يجمع ما بين تقنية PPTP الخاصة بميكروسوفت وايضا تقنية Cisco Layer 2 Forwarding Technology او L2F.

### IPSec

وهو اختصار IP Security وهو صمم خصيصا لفرض الحماية على نقل البيانات وايضا التشفير الخاص بالبيانات عند نقلها على الإنترنت وهو صمم للعمل مع IPv4 و IPv6

### SSL

وهو اختصار Secure Sockets Layer وهو صمم من قبل Netscape ليكون ضمن متصفحهم وهو مبني على تقنية RSA Public Key Encryption لتشفير وحماية البيانات لتوفير حماية لنقل البيانات عبر الإنترنت وهي خدمة يمكن استخدامها في المواقع لحماية نقل البيانات الحساسة مثل Credit Card Numbers وسوف تجد الموقع المحمي يحمل عنوانا مثل HTTPS

### Kerberos

هو ليس بروتوكولا على الإطلاق انما هو عبارة عن نظام متكامل لحماية وامن المعلومات عبر الإنترنت ويستخدم نظام تشفير فائق القوة والذي يميزه انه مجاني ويمكنك تحميل الـ Source Code الخاص به من الإنترنت.



## Attack and Defense

سوف نتطرق في هذا الجزء إلى طرق الهجوم المستخدمة من قبل القراصنة وايضا بعض طرق الحماية. واعلم ان اي عمل يكون ورائه Hacker فهو عمل تخريبي ينطوي على نية مبيتة بالإختراق على سبيل المثال دخول الهاكر إلى شبكتك هذا معناه اختراق او Attack اما الفيروسات فهي على سبيل المثال لا تعتبر Direct Attack او هجوم مباشر فهي تنتقل بسبب بعض المستخدمين على الشبكة واليك فيما يلي بعض الحيل المستخدمة في الهجوم.

### IP Spoofing

تعتمد هذه الطريقة على الخداع حيث يتم ارسال Packet من عنوان IP مزيف بمعنى انه قد يتم الإحتيال على الشبكة بأن هذا الـ IP من داخلها وهو في الاساس ليس من داخل الشبكة بل هو عنوان مزيف للخداع وللأسف الـ Router على سبيل المثال سوف يعطي هذا الـ IP السماح بالمرور إلى الشبكة على انه من داخلها إلا ان الـ Firewall سوف يمنع ذلك.

### Ping of Death

هذه الطريقة تعتبر نوعا من الهجوم الخاص بطريقة Denial of Services Attack وهي تمنع اي مستخدم حتى مستخدمي الشبكة الموثوق بهم من استخدام النظام وتستخدم فيها طريقة Ping فمثلا عندما تقوم بالتحقق من جهاز على الشبكة لإنك تستخدم Ping وسوف يتم ارسال Packet عادية إلى هذا الجهاز للتحقق من وجوده ام لا إلا ان هذه الطريقة تعتمد على ارسال Large Packet تؤدي إلى سقوط النظام وهناك عدة Patches يمكن استخدامها لمنع هذا النوع من الهجمات.

### WinNuke

هو عبارة عن برنامج يستخدم لإرسال Packet خاصة عن طريق TCP/IP مستخدما Header خاطيء خاص بالـ TCP وعندما تصل هذه المعلومات إلى النظام فسوق يقع النظام في الحال نظرا لعدم وجود طريقة لتعامله مع الـ Invalid Header وهذا يحدث عادة في Windows 98, Windows 2000 وسوف تظهر لك الشاشة الزرقاء القاتلة BSoD وهناك تحديثات من Microsoft لمنع حدوث هذه المشاكل مع الانظمة.

## SYN Flood

هو ايضا نوع من انواع هجوم DoS Attack وفي الطبيعي عندما تقوم بالإتصال بكمبيوتر ما فهو يرسل Packet بـ  $SYN = 1$  وبعدها يستقبل الكمبيوتر الآخر هذه الـ Packet ثم يبدأ في الإتصال ولا تستخدم SYN في وسط الإتصال او التحميل لملف مثلا وتعتمد طريقة SYN Flood على ارسال العديد من الـ SYN متتالية للكمبيوتر فلن يستطيع التعامل معهم لانه سوف يرتبك ولن يعرف اي واحدة سوف يرد عليها بالإتصال وسوف يقع النظام.

## Defense Techniques: Intruder Detection

بعد ان تعرفت على بعض الحيل الخاصة بالإختراق دعنا نتحدث عن بعض الحيل ايضا الخاصة بالدفاع والحماية.

### Active Detection

هي طريقة تعتمد على وجود (بشكل تشبيهي) حارس للشبكة يقوم دوما بتفقد الشبكة والبرمجيات والكشف عن اي عمليات غير آمنة وايضا مشكوك فيها والبحث عن الثغرات في البرمجيات على الشبكة وتسمى هذه النوعية من البرمجيات Active Intrusion Detection ومنها Cisco NetRanger و Memco SessionWall و SATAN ولكن احذر من البرنامج الأخير فيما انه مجاني فسوف يستخدم ايضا من قبل الهاكرز لإكتشاف الثغرات!

### Proactive Defense

وهي طريقة تعتمد على اكتشاف الثغرات في الشبكات واغلاقها عن طريق برامج معينة مثل SATAN ولكن الامر اكثر تعقيدا ففي الوقت الذي تقوم انت فيه بسد ثغرات الشبكة يقوم الـ Hacker باكتشاف ثغرات اخرى للدخول إلى الشبكة وهذه هي حرب المعلومات!

### Passive Detection

تعتمد على بعد البرمجيات التي تقوم بتخزين معلومات عن جميع الملفات والبرامج على الشبكة فيما يسمى log file ويمكن التحقق من هذا الملف عند حدوث اي شيء غير موثوق به على الشبكة حيث تتم المراقبة لهذا الملف بصفة دورية ومقارنته بما يحدث على الشبكة.

## Encryption

سوف نحاول في هذه الفقرة ان نقدم بعض المعلومات الهامة عن الـ Encryption او تشفير المعلومات وهي مدخل فقط لان موضوع الـ Encryption من الموضوعات المقدمة والتي تخرج عن اساسيات هذا المنهج.

والـ Encryption بشكل عام هو طريقة تشفير المعلومات سواء سوف تنتقل على الإنترنت ام لا وهذه الشفرة لها معادلة رياضية لعملها وايضا لفكها وارجاع البيانات إلى حالتها الطبيعية. والعملية الخاصة بالتشفير يطلق عليها Encrypt اما اعادة فك التشفير فيطلق عليها Decrypt والمعادلة الرياضية تحول هذه البيانات إلى ارقام عن طريق مايعرف باسم الـ Key او المفتاح وعملية التشفير موجوده منذ زمن بعيد حتى قبل ظهور الكمبيوتر واستخدمت في نثر الرسائل المشفرة لمابين الجيوش في الحروب على سبيل المثال

### ولكن كيف يعمل التشفير او Encryption؟

يتم عمل التشفير بتحويل الحروف إلى ارقام طبقا لمعادلة معينة تسمى الـ Key وهناك عدة طرق للتشفير وعلى سبيل المثال هذه الجملة

The Quick Brown Fox

سوف نقوم بتحويل الحروف إلى ارقامها الاصلية المعبرة عنها مثلا  $A=1$   $B=2$  وهكذا وسوف تصبح الارقام كالتالي

17 5 8 20 وهكذا حتى نهاية الجملة واذا اردت ان تفك التشفير فسوف تقوم باستخدام نفس المفتاح Key المعادلة لحل التشفير وهي تحويل الارقام إلى حروف فسوف تترجم كالتالي  
 $E=5$   $H=8$   $T=20$  وهكذا ولكن بالطبع الامر اكثر تعقيدا من هذا المثال فهذا مثال على تشفير مثلا من نوع 8 bit وكلما زاد الـ bit كلما كانت المعادلة اكثر تعقيدا وكان حلها من اصعب مايمكن.

### Private Key

ويرمز له بالمعادلة الخاصة او المفتاح الخاص بفك الشفرة وتستخدم طريقة Private Key نفس المفتاح ما بين الـ Sender والـ Receiver لفك الشفرة وتسمى ايضا Symmetrical Keys.

### Data Encryption Standard (DES)

تبارى العلماء على مدار عمر الحاسوب في ابتكار طرق للتشفير وابتكرت شركة IBM عام ١٩٧٧ نظام DES وكان يستخدم 56 bit Private Key ليعطي اكثر من ٧٢ كدرليون احتمال لحل شفرة المفتاح (كدرليون - واحد امامه ١٥ صفرا) وتم كسر هذه الشفرة عام ١٩٩٧ بعد عمل ١٨ كدرليون احتمال في مسابقة لشركة RSA.

ثم بعد ذلك استبدل نظام DES بآخر سمي Skipjack او EES او Escrowed Encryption Standard واستخدم 80-bit key ومعلومات الفك اصبحت معقدة وغير معروفة واعتمدتها شركة التليفونات الامريكية لتكون برنامج التشفير في رقائق اجهزة الإتصالات ولكن هذا لن يكون في صالح المواطنين! لانهم سوف يصبحون اي الحكومة قادرة على فك شفرات المكالمات!

### Public Key Encryption

او كما تعرف هذه الطريقة بطريقة Diffi-Hellman Algorithm وهذه الطريقة تستخدم مفتاحين لتشفير المعلومات وهما Public key و Private Key. وقد ظهرت هذه الطريقة على يد العالمين Diffi و Hellman في بحث قدماه عام ١٩٧٦.

### RSA Data Security

هذه الطريقة هي اختصار لاسماء العلماء Rivest, Shamir, Adleman الذين ابتكروا هذه الطريقة والتي تعتمد على Public Key وللمزيد عن هذه الطريقة [www.rsa.com](http://www.rsa.com)

### PGP- Pretty Good Privacy

هذه الطريقة PGP هي ادوات Utilities للتشفير مبنية على قاعدة Public Key للتشفير قام بابتكارها العالم Phil Zimmerman عام ١٩٩٠.

طبقا لجمعية امن المعلومات العالمية ICSA فأن معظم الإختراقات او نسبة ٨٠% من الإختراقات داخل شبكات الكمبيوتر تتم من داخل الشبكة وليس من خارجها!

## Network Disaster Recovery

في هذا الجزء من المنهج سوف نتحدث عن حماية المعلومات على الشبكة من الضياع او الكوارث الطبيعية او اي شيء قد يتسبب في تلف المعلومات او فقدانها. وقبل ان نتعمق اكثر في طرق حماية البيانات لابد ان تضع في اعتبارك عدة عوامل مهمة وهي نوعية النظام الخاص بك وماهي المدة التي لن تتضرر منها إذا توقف النظام عن العمل وما هي المدة التي تتطلب ان يكون النظام يعمل بكفاءة عالية دون اخطاء او بمعنى آخر نوع الـ Business او العمل وسوف نوضح ذلك فيما يلي.

### Hot Sites

هذا النوع من العمل يطلب ان يكون النظام يعمل بنسبة ١٠٠% بدون اخطاء او مشاكل ويعتبر هذا النوع من الاعمال لا يخضع لنظرية Disaster Recover لانه لا يجب ان يحدث اي من الاشياء المتعلقة بضياع المعلومات ويعتمد هذا النظام على اكثر من مكان او Redundant لتخزين البيانات ويتكلف هذا النظام مبالغ باهظة للمحافظة على المعلومات على سبيل المثال اجهزة الكمبيوتر التي تعمل في المطارات والحكومات والبنوك. وتعتمد على Clustering Technology والتي تعتمد على وجود اكثر من جهاز مرتبطين ببعضهما البعض للحصول على اداء عالي ودقة في معالجة البيانات والحفاظ عليها.

### Warm Site

يعتمد هذا النظام في العمل على كون المعلومات متوفرة بنسبة ٨٥% بمعنى انها متوفرة في اغلب الاوقات. والمعلومات التي توجد في هذا النظام هي اقل اهمية من المعلومات التي توجد في نظام Hot Site ويعتمد هذا النظام على وجود ما يسمى Duplicate Server فهو جاهز ليعمل او ليحل محل اي جهاز آخر في المنظومة عند حدوث المشكلة وعندما يتم تصليح الجهاز الي حدثت به المشكلة يصبح هو Duplicate Server حتى تحدث مشكلة يحل محل جهاز آخر وهكذا. وهذا النظام اقل كلفة من سابقه إلا ان احتمال ضياع البيانات في هذا النظام محتمل لانه يعتمد على تقنية الـ Backup فلو لم يحدث الـ Backup او حدث بشكل خاطيء هذا معناه ضياع المعلومات او فقدانها.

### Cold Site

هذا النوع من الانظمة يعتمد على خبير الدعم الفني او الصيانة فهو لا يعدو يعتمد إلا على نظام لاستعادة البيانات عند فقدانها فإذا حدثت مشكلة ما فسوف يحاول خبير الدعم الفني حل المشكلة بأي وسيلة حتى يعود النظام إلى العمل ولحين اصلاح المشكلة سوف يظل الـ Server معطل او Down وهذا يدل على ان نوعية البيانات في هذا النظام ليس كمثيلاتها السابقة بل اقل وهذا النظام لا يضمن ابدا اداء عال في الخدمات او Server Uptime.

### Fault Tolerance Elements

في هذا الجزء من المنهج سوف نتعرف على العوامل التي تساعد في المحافظة على البيانات وتعتبر Fault Tolerance مقياس لاهمية البيانات فكلما زادت عوامل الـ Fault Tolerance او المحافظة على المعلومات كلما ارتفعت قيمة هذه المعلومات.

### Power Management

من اهم الاشياء التي يجب ان نتبعها للمحافظة على البيانات هي مصادر الطاقة مثل UPS او Power Surges Protectors والعديد من الاجهزة الاخرى التي تحمي الاجهزة من تذبذب التيار او انقطاعه او حتى من الصواعق وكل هذا يختلف حسب درجة او اهمية البيانات الموجودة في المنظومة المعلوماتية.

### Disk System Fault Tolerance

ايضا من اهم عوامل المحافظة على نظام المعلومات هو الـ Disk ونظام الملفات عليه وكيفية تخزين البيانات عليه لان معظم مشاكل ضياع البيانات تكون بسبب الـ Hard Disk ولهذا فأن استخدام وسائل Disk management او ادارة الاقراص في انظمة التشغيل مثل Mirrored او Stripped او RAID وتعني Disk Fault Tolerance امكانية استعادة البيانات من القرص عند حدوث اية مشكلة.



### Backup System

من اهم العوامل في المحافظة على معلوماتك في المنظومة المعلوماتية هو النسخ الاحتياطي او Backup System ويمكنك استخدام برمجيات في النظام مثل System Backup او يمكنك استخدام برمجيات منفصلة تدعم اعدادات اكثر احترافا في التعامل مع البيانات وايضا يمكنك ان تستخدم اكثر من Medium او وسيط لنقل وتخزين البيانات مثل Hard Disks و Backup Tapes او حتى Removable Media مثل الـ DVD

### Virus Protection

الحماية من الفيروسات احد اهم العوامل في المحافظة على البيانات من التلف وعليك باتخاذ الحيلة بتركيب برنامج فعال في مكافحة الفيروسات مثل Symantec Norton Antivirus وتقوم بعمل التحديثات او مايسمى Virus Definitions باستمرار لضمان عدم وجود اي فيروس على الانظمة.

### Software Patches

تسمى عادة Fix او Service Pack او Patch وهي مجموعة ملفات يتم تحميلها من مصنع البرنامج لسد بعض الثغرات في البرامج او الانظمة والتي تعتبر ذات خطورة على امن المعلومات والتي قد يتمكن الهاكر عن طريقها من اختراق النظام. لكن احذر فدايما ليست التحديثات متوافقة مع جميع النسخ فقد يتسبب التحديث في حدوث مشكلة في النظام وتعطله عن العمل فاولا عليك حساب عوامل المخاطرة قبل الإقدام على هذه الخطوة.

## Network Troubleshooting

في هذا الجزء من المنهج سوف نتعرف على كيفية تحليل مشاكل الشبكة وكيفية ايجاد الحلول لهذه المشكلات لكن هناك نصيحة مهمة جدا وهي انه لن يوجد مكان او كتاب سوف يخبرك بكيفية حل جميع مشاكل الشبكات الامر يتعلق بالتدريب، نعم كثرة التدريب والتعرض للمشكلات هي التي سوف تساعدك على اكتساب الخبرة والمهارة في التعامل مع هذه المشكلات وايضا ايجاد الحلول لها.

### Simplify the Problem

من اهم الاشياء في التعامل مع المشكلة هو محاولة تبسيطها حيث انه لن تستطيع ان تحل المشكلة طالما انها معقدة فحاول التبسيط بمعنى ان كان على بسيل المثال احد الاجهزة لايمكن ان تراه على الشبكة عن طريق مثلا Browse My Network Places فبسط الامر اولا فقم مثلا بعمل Ping على هذا الجهاز هو موجود اصلا على الشبكة ام لا؟  
إذا كان موجود هذه علامة جيدة يمكنك ان تفتح الجهاز عن طريق Start→Run ثم اكتب اسم الجهاز او رقم الـ IP الخاص به كالتالي [\\IP](#) او [\\ComputerName](#) إذا فتح الجهاز فالمشكلة لا تكمن في الجهاز ربما تحتاج غلى عمل restart للـ Switch اما إذا لم يستجب الجهاز للأمر Ping في البداية فربما كانت المشكلة في الـ Cable تفقد الكابل اولا قبل ان تفعل اي شيء قد باختباره عن طريق Network Tester اما إذا لم يكن الـ Cable فربما يكون كارت الشبكة غير معرف ويحتاج غلى تعرف قم بتفحص هذا ايضا ويمكنك ايضا ان تقوم بتفقد الـ IP ربما يكون هناك Conflict اي ان هناك جهاز آخر له نفس الرقم على الشبكة، وهكذا حتى تصل إلى سبب المشكلة يجب ان تبدأ بالجزء البسيط اولا.  
وضع في اعتبارك دائما ان الامر Ping من اهم الاوامر التي تساعدك على معرفة هل الجهاز موجود على الشبكة ام لا ثم بعد ذلك تبدأ بالتحرك في اتجاه آخر للمشكلة حسب النتيجة. وفيما يلي بعض المشاكل التي تواجهك في العمل على الشبكات والحلول المقترحة.

لا تستطيع ان ارى الاجهزة على الشبكة إلا انني استطيع الدخول على الإنترنت؟

هذه المشكلة في اغلب الاحيان تكون مستخدما Subnet Mask مختلف عن بقية الاجهزة على الشبكة فلماذا انت لا تراهم او انك تنتمي إلى Workgroup وهم ينتمون إلى Workgroup اخرى على نفس الشبكة.

لا استطيع دخول الإنترنت عبر الشبكة ولكن احدهم يستطيع ذلك؟

هذا الامر يتوقف على عدة اسباب:

- ١- ربما تكون معلومات الـ Gateway غير صحيحة على جهازك
- ٢- ربما قام الـ Network Administrator بحجبك عن الإنترنت
- ٣- ربما تكون اعدادات الـ IP غير صحيحة

لا استطيع الإنضمام إلى Domain على شبكتي؟

هذا الامر يحدث غالبا إذا كنت لا تملك Administrator Password للدخول إلى الـ Domain.

الأمر Ping على 127.0.0.1 لا يستجيب؟

هذا معناه ان TCP/IP غير موجوده قم بتركيبها من Network Connections ثم properties

عندما اقوم بتوصيل كابل الشبكة في الجهاز لإن لمبة البيان لا تضيء **Link Light**؟

هذا الامر يحتمل ثلاثة احتمالات كما يلي:

١- نهاية الكابل من ناحية الـ Switch بها مشكلة او غير متصلة بالـ Switch

٢- كارت الشبكة ربما يكون غير معرف او غير مركب بشكل مضبوط

٣- هناك مشكلة في الـ Cable اختبره بـ Cable Tester

تظهر لي دائما رسالة **IP Address Conflict**؟

هذا معناه ان هناك جهاز آخر على الشبكة يحمل نفس رقم الـ IP الخاص بجهازك قم بتغيير رقم الـ IP الخاص بجهازك هذا اذا كنت تستخدم Static IP اما اذا كنت تستخدم

Automatic IP فعليك ان تذهب إلى Start→Run→cmd ثم تكتب

Ipconfig /release ثم تكتب Ipconfig /renew

لدي كارت شبكة 10/100 ودائما سرعته 10Mbps فقط؟

قد يكون الـ Hub او الـ Switch الذي تستخدمه 10Mbps فقط او قد يكون الجهاز الآخر الذي تتصل به هو 10Mbps فقط لهذا تتصل انت بسرعة هذه الاجهزة.

وكما اشرنا سابقا مشاكل الشبكات تحتاج إلى خبرة وتدريب اكثر منها قراءة بمعنى انك تتعرض للمشكلة ثم تبدأ في البحث عن الحل لانه من الصعب جدا ان تجد جميع الحلول لجميع المشاكل في مكان واحد. [تابع منتدى الاسئلة والحلول لمزيد من المشاكل والحلول](#)

## Network Monitoring & Troubleshooting Tools

سوف نتناول في هذا الجزء من المنهج مجموعة من البرمجيات الهامة جدا والتي سوف تسهل العمل لك كـ Network Administrator او خبير في الشبكات من برمجيات لإختبار اداء الشبكة وبرمجيات لمراقبة الشبكة حتى برمجيات خدمية تساعدك في تسهيل مهمتك. وسوف تجد ميزة هامة في جميع هذه البرمجيات انها مجانية ولا تتكلف اي شيء!

### NetworkActivePortScan

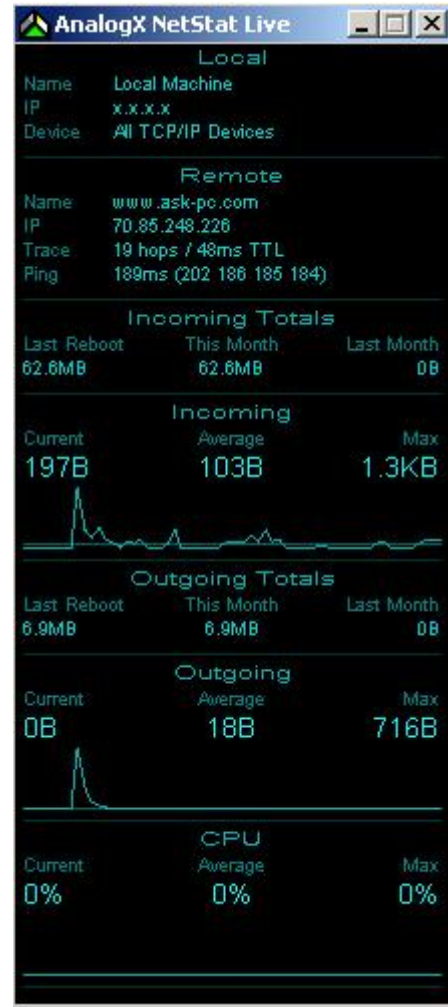
برنامج من البرامج المجانية والتي يمكنك تحميله من [هذا الرابط](#)



يمكنك ان تقوم بوضع الـ IP الخاص بالجهاز على الشبكة وسوف يقوم هذا البرنامج بالبحث عن الـ Ports المفتحة على هذا الجهاز ويمكنك ايضا ان تستخدم Ping بإعدادات مختلفة ويمكنك ايضا ان تقوم بالبحث عن جميع الـ IPs على الشبكة المحلية وعمل Scan لهم والكثير من المهام الاخرى التي تستطيع ان تتعرف عليها بسهولة في هذا البرنامج.

هذا البرنامج المجاني يمكنك تحميله [من هنا](#) وهذا البرنامج يتيح لك الحصول على معلومات فورية عن حجم الـ Traffic والـ Packets التي تنتقل عبر الشبكة عن طريق كارت الشبكة الموجود في الجهاز كما يمكنك ايضا ان تحصل على معلومات عن Remote Machine اي جهاز في مكان آخر او حتى موقع ويمكنك بسهولة التعامل مع البرنامج وتغيير الإعدادات عن طريق R-Click على البرنامج وسوف تظهر لك قائمة يمكنك اختيار Remote مثلا لإدخال الـ IP او اسم الجهاز الـ Remote Machine او تعديل الإعدادات الاخرى عن طريق القائمة التي تظهر لك كما يعرض لك البرنامج ايضا معلومات عن استهلاك الـ Processor او المعالج كما يتيح لك ايضا معرفة حجم الـ Packets التي ارسلت او استقبلت عن طريق كارت الشبكة من وإلى هذا الجهاز في خلال شهر مثلا والكثير من المعلومات المهمة التي تغنيك عن استخدام بعض الاوامر في الشبكات.

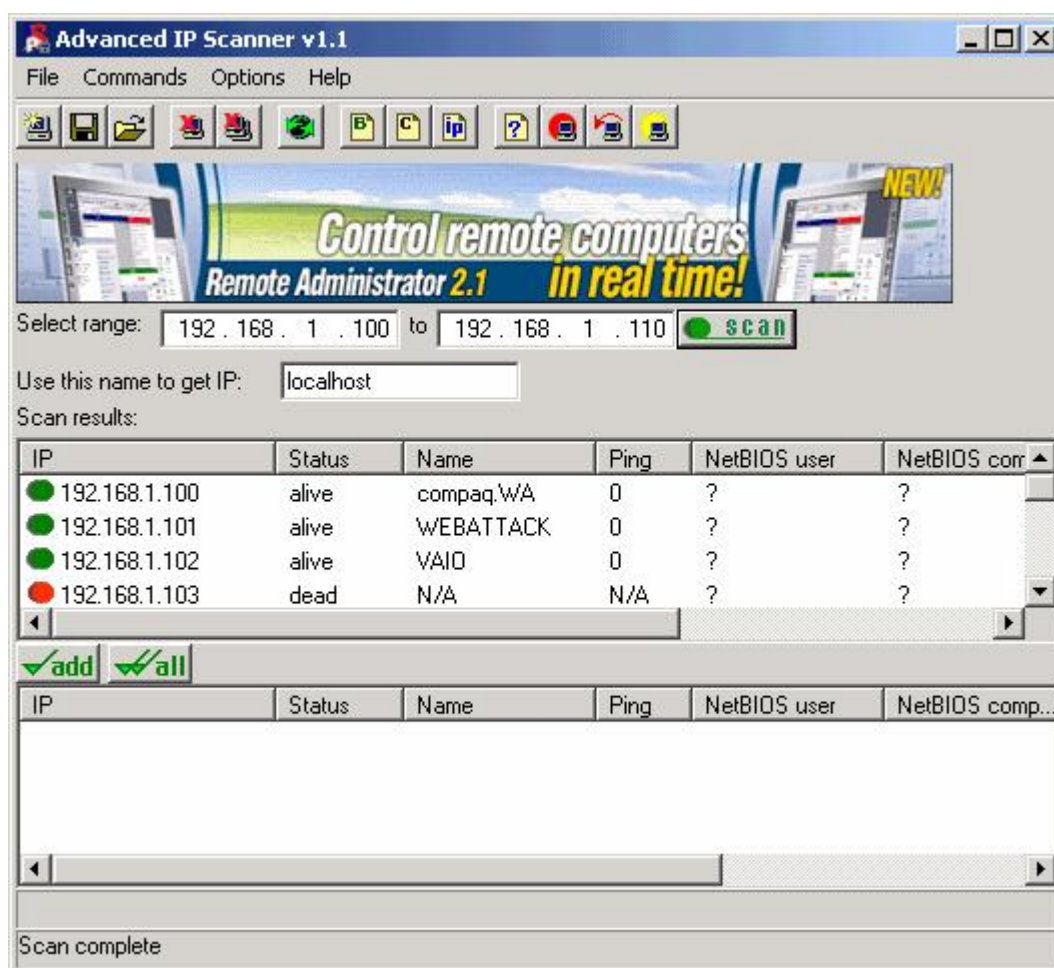
### AnalogX NetStat Live



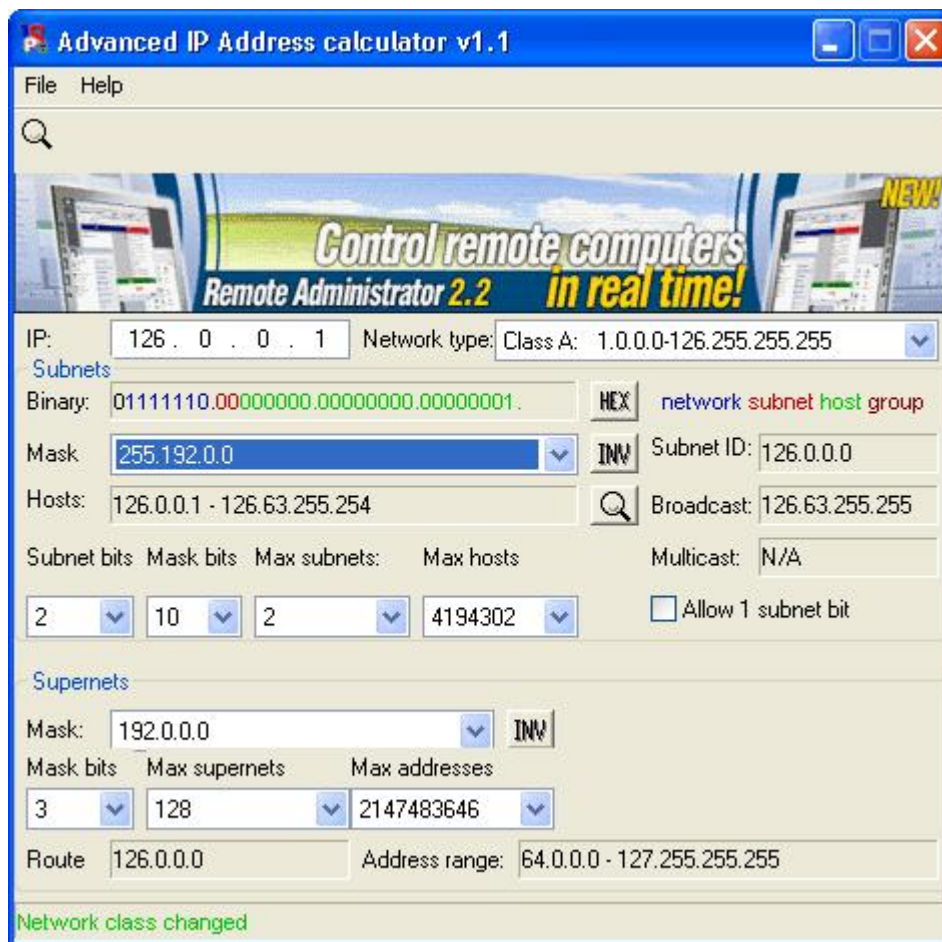


## Advanced IP Scanner

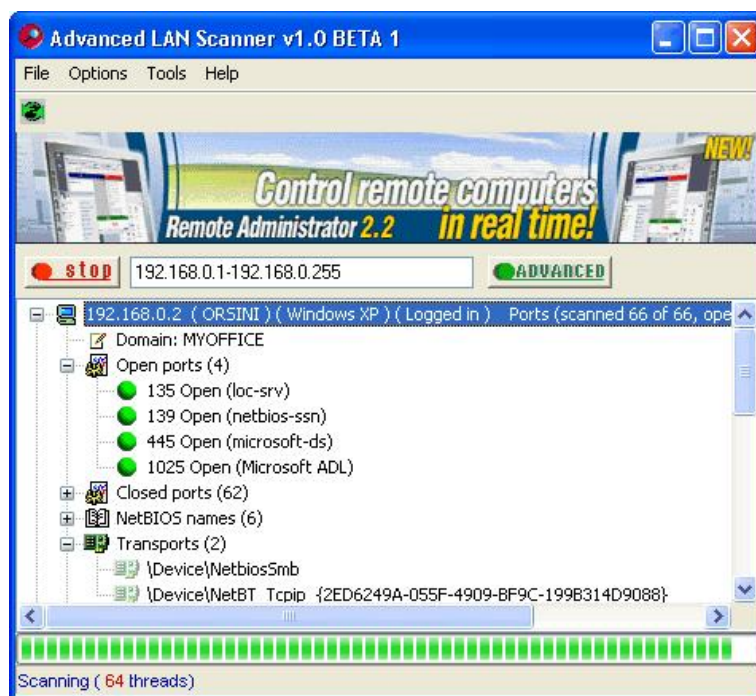
يمكنك تحميل هذا البرنامج المجاني مع عدد آخر من البرمجيات [المجانية على هذا الرابط!](#)



يتيح لك هذا البرنامج امكانيات هائلة في التعامل مع الـ IPs والاجهزة على الشبكة حيث يتيح لك معرفة معلومات هامة عن الاجهزة كما يتيح لك التحكم ايضا في بعض العمليات على الجهاز على الشبكة حتى ولو من بعد! وهناك مجموعة برمجيات هامة ننصحك ايضا بالقاء نظرة عليها وهي ايضا احد منتجات نفس الشركة وهي موجودة على الرابط بالا على مثل برنامج Advanced IP Calculator وهو هام جدا في التعامل مع Subnet وارقام الـ IPs وايضا برنامج Advanced Port Scanner و Advanced LAN Scanner.



Advanced IP Calculator

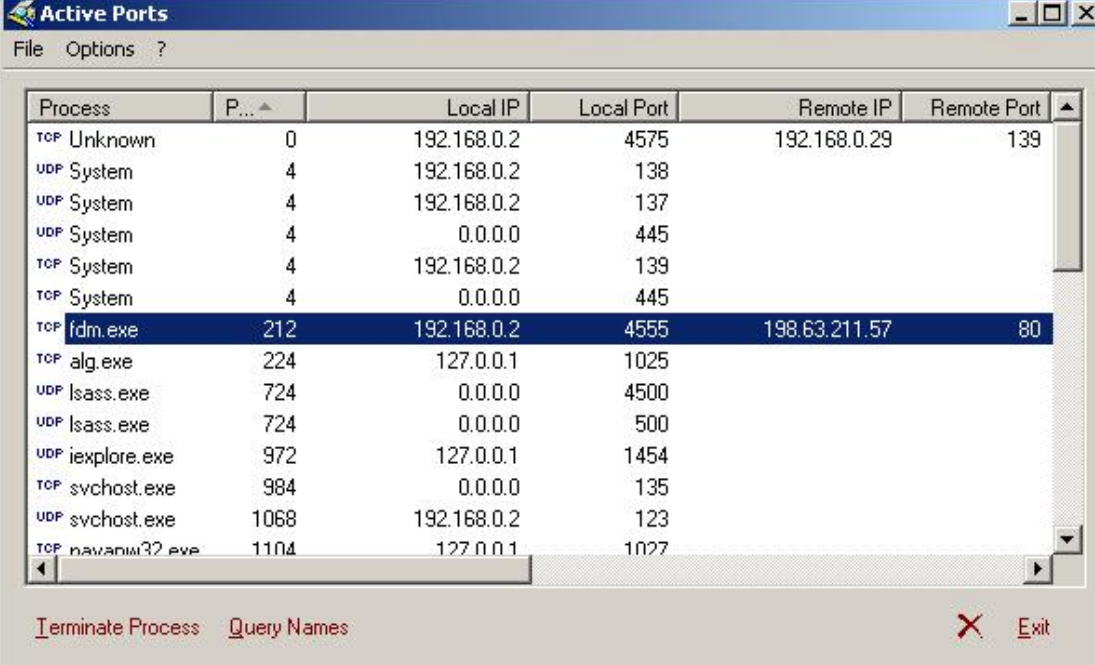


Advanced LAN Scanner

## Active Ports

هذا البرنامج من البرامج المهمة جدا والتي تعرض لك معلومات الـ Ports المفتوحة في الجهاز والبرمجيات التي تعمل عليها وحتى اتصالها باي IP خارج الشبكة او داخلها.

ويمكنك تحميله من [هذا الرابط!](#)



The screenshot shows the 'Active Ports' window with a menu bar (File, Options, ?) and a table of active network connections. The table has columns for Process, PID, Local IP, Local Port, Remote IP, and Remote Port. The 'fdm.exe' process is highlighted, showing it is using TCP on local port 4555 to connect to remote port 80 on IP 198.63.211.57.

Process	PID	Local IP	Local Port	Remote IP	Remote Port
TCP Unknown	0	192.168.0.2	4575	192.168.0.29	139
UDP System	4	192.168.0.2	138		
UDP System	4	192.168.0.2	137		
UDP System	4	0.0.0.0	445		
TCP System	4	192.168.0.2	139		
TCP System	4	0.0.0.0	445		
TCP fdm.exe	212	192.168.0.2	4555	198.63.211.57	80
TCP alg.exe	224	127.0.0.1	1025		
UDP lsass.exe	724	0.0.0.0	4500		
UDP lsass.exe	724	0.0.0.0	500		
UDP iexplore.exe	972	127.0.0.1	1454		
TCP svchost.exe	984	0.0.0.0	135		
UDP svchost.exe	1068	192.168.0.2	123		
TCP navadm32.exe	1104	127.0.0.1	1027		

At the bottom of the window, there are buttons for 'Terminate Process', 'Query Names', and 'Exit'.

كما يعرض لك ايضا اسم الـ Port ورقمه والمتصل به سواء كان موقع او برنامج او حتى Server خارج الشبكة وهو مهم جدا حيث تستطيع عن طريقه كشف الإختراقات على الاجهزة بسهولة دون عناء.

بالطبع الإنترنت مليء بالبرمجيات المجانية التي سوف تجدها في مواقع مختلف نحن فقط قصدنا ان نقدم لك نبذة عن البرمجيات التي يمكنك الاستعانة بها لتسهيل العمل

## Advanced Network Topics

سوف نحاول في هذا الجزء الاخير من المنهج ان تعرض لبعض الموضوعات المتقدمة في الشبكات ولعل اغلبها متعلق بانظمة التشغيل وكيفية التعامل مع الشبكات بشكل احترافي.

### Windows Domain Network

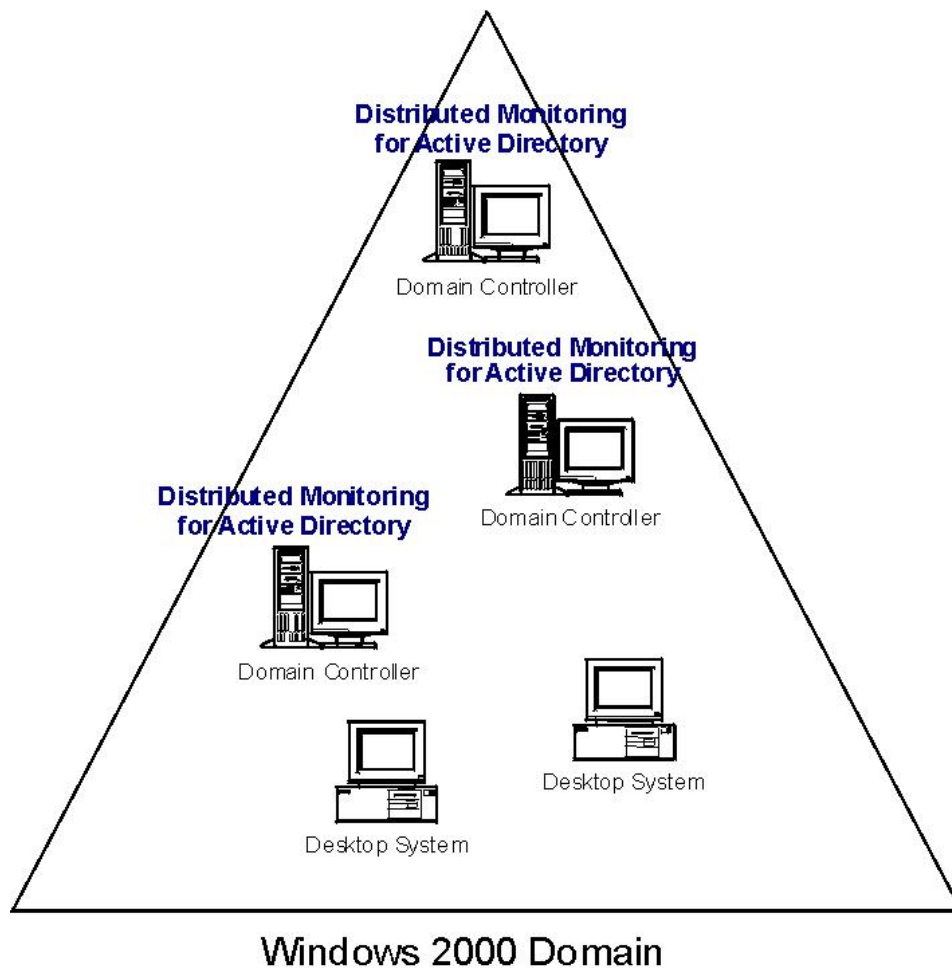
تعتبر شبكات Domain من اكثر انواع الشبكات امنا وثباتا إلا انها ايضا من اعقدها نظرا لإحتياجها لخبراء لإدارتها وتتطلب معرفة عالية بالـ Hardware وايضا انظمة التشغيل. وسوف نتناول في هذا الجزء بعد التفاصيل والإعدادات المتعلقة بهذا النوع من الشبكات والتي هي Client-Server Network نظرا لان الشبكة تحوي خادما او اكثر يقوم كل خادم بعمل مخصص له وتستطيع الاجهزة الاخرى على الشبكة الوصول إلى هذا الخادم للاستفادة من خدماته مثل Domain Controller Server والذي قوم بتوفير الـ Domain او النطاق لعمل الشبكة والذي يحوي معلومات الدخول لموارد الشبكة وايضا Print Server الخاص بالطباعة والكثير ويكون دخول الاجهزة على هذه الشبكات متوقف على الحصول على تصريح من الـ Administrator او مدير الشبكة وهو ما يجعل هذه الشبكات اكثر امنا.

### Active Directory

من اهم الاشياء التي يجب ان نتعرف عليها في التعامل مع Domain Network هو الـ Active Directory والذي يوجد في الـ Domain Controller او الخدم الخاص بالـ Active Directory وهو المكان او كما يطلق عليه المجلد Directory وهو يحوي قاعدة بيانات للمستخدمين على الشبكة والاجهزة وكلمة المرور واسم المستخدم الخاص بكل جهاز على الشبكة ويحوي ايضا هذا الـ Directory نطاق Domain او اكثر كل منهم له الـ Security الخاصة به وما إلى ذلك من الإعدادات ويوفر الـ Domain استخدام الـ Security Policy الخاصة بالمستخدمين على الـ Domain والتحكم فيها كما يساعد على التحكم بشكل افضل في الشبكة ومواردها في شركتك او مؤسستك.

## Domain Controller

هو عبارة عن كمبيوتر يعمل بنظام Windows 2000 Server او Windows 2003 Server وقد تم تركيب الـ Active Directory عليها ولهذا يفهم ان شبكة الـ Domain قد يكون عليها اكثر من Domain Controller على سبيل المثال شركة صغيرة بها LAN سوف تحتاج إلى Domain واحد واثنين Domain Controller. والصورة التالية توضح شبكة Domain تعمل في بيئة Windows 2000 Server





## Installing Domain Controller

فيما يلي سوف نشرح لك خطوات تركيب Domain Controller

- ١- ادخل على Administrative Tools في Windows 2000 Server
- ٢- اختر Configure Your Server
- ٣- اختر Active Directory
- ٤- انقر Start لتبدأ عملية تركيب Active Directory
- ٥- اتبع التعليمات حتى انتهاء التركيب

### لكن لماذا نقوم بعمل Domain Controller؟

- ١- اما لعمل Domain جديد في الشبكة
- ٢- انشاء Domains جديدة في بيئة الشبكة Forest
- ٣- تحسين اداء الشبكة في كل الاتجاهات

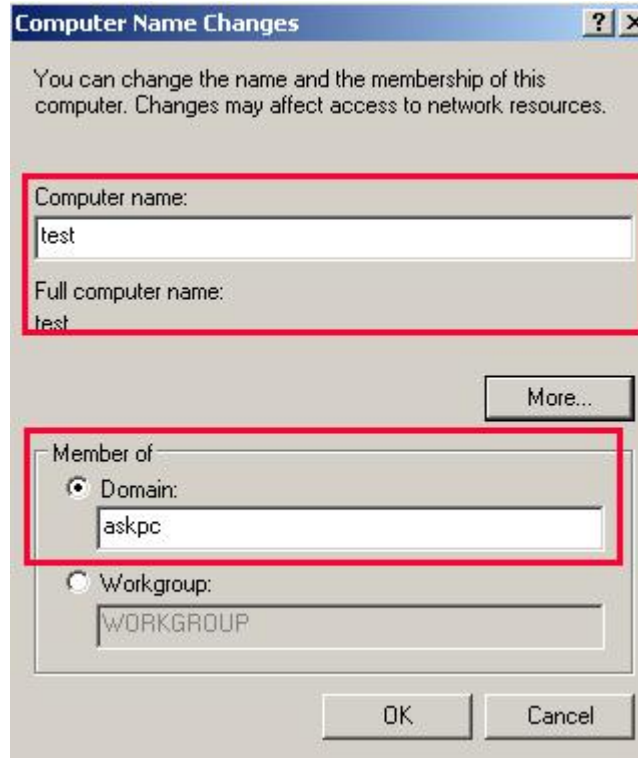
## Adding Windows XP to a Domain

سوف نتعرف في الخطوات التالية على كيفية اضافة جهاز يعمل بـ Windows XP في داخل Domain فقط اختر R-Click على MY Computer ثم اختر Properties  
تفتح لك نافذة النظام System اختر منها Computer Name كما بالصورة





سوف تظهر لك نافذة اكتب فيها اسم الكمبيوتر ثم بعد ذلك اختر اسم الـ Domain الذي يوجد على الشبكة والذي سوف يصبح هذا الكمبيوتر جزءا منها كما يلي



بعد ذلك سوف يسألك الويندوز عن الـ User name والـ Password الخاصة بالـ Domain وهذه المعلومات سوف تكون خاصة بالـ Domain Administrator بعدها سوف يطلب منك الكمبيوتر عمل Restart ثم بعد ذلك عندما يقلع مرة أخرى وتستطيع اختيار اسم الكمبيوتر الخاص بك وللمرة السر.

عن طريق Active Directory Users and Computers تستطيع عمل مستخدم جديد وكلمة مرور للأجهزة على الشبكة أي الأجهزة التي سوف تنضم إلى الـ Domain كما في الصورة المقابلة من Active Directory.



## System Administrators Tools

كخبير في الشبكات ننصحك باستخدام هذه البرمجيات الخاصة بمديري الشبكات على الوصلات التالية والتي تعتبر من اهم الادوات التي لا بد لك من التعامل معها إذا كنت تدير شبكة تعتمد على Windows Technology.

[Windows Server 2003 Resource Kit Tools](#)  
[Windows Server 2003 Service Pack 1 32-bit Support Tools](#)  
[Windows Server 2003 Service Pack 1 Administration Tools Pack](#)  
[Internet Information Services \(IIS\) 6.0 Manager for Windows XP](#)  
[Microsoft Management Console 3.0 for Windows Server 2003](#)  
[Group Policy Management Console with Service Pack 1](#)  
[Windows Server 2003 Group Policy Infrastructure](#)  
[User Profile Hive Cleanup Service](#)  
[Windows XP Remote Desktop Connection software](#)  
[Microsoft Windows Server 2003 Performance Advisor](#)

بهذا نكون انتهينا من منهج شهادة "مهندس الشبكات المعتمد من ASK PC" أو **ASK PC Certified Network Engineer** وننصحك بمراجعة قسم التدريبات العملية بالفديو لفهم المنهج بسهولة وحظ سعيد في الإختبار.

## المراجع References

هذا المنهج تم اعداده من قبل المؤلف من واقع الخبرة العملية الخاصه به والتي تتعدي العشر سنوات في مجال الكمبيوتر وبخاصة الدعم الفني ومشاكل الكمبيوتر بالاضافة الى بعض الكتب والمراجع العلمية الخاصة بالكمبيوتر وبالتعاون مع اكبر بيوت الخبرة في مجال الدعم الفني والصيانة والشبكات

Computer Hardware Architecture & Organizations, Prentice Hall  
Microsoft KB, Microsoft Corp.  
Microsoft TechNet, Microsoft Corp.  
Network Troubleshooting, O'Reilly  
Sybex - Network+ Study Guide, 3rd Edition  
Ethernet Network Analysis and Troubleshooting, Sniffer University  
Network - Computer Networks Problem Solutions, PRENTICE HALL  
New Riders - Understanding the Network

## ASK PC & Copyright Notice

---

Copyright © 2006 [www.ask-pc.com](http://www.ask-pc.com) All Rights Reserved

No part of this work may be reproduced, copied, transmitted, edited, printed, or altered by any mean without written permission from the author.

ASK-PC.COM as a website and its logo is registered internationally and it's property of ASK PC, USA

Microsoft is a registered trademark of Microsoft Corporation in USA and or other countries, all brands and trademarks mentioned are property of their respective owners.

## About ASK PC

---

ASK-PC.COM is the largest Arabic IT Community online, providing technical solutions and training for individuals and enterprise to help spreading information technology usage in Middle East. ASK PC headquarter is located in GA, USA and we're operating online at [www.ask-pc.com](http://www.ask-pc.com)

Mailing Address:

ASK PC

11770 Haynes Bridge Rd, STE 205-388,  
Alpharetta,  
GA 30004,  
USA

