الــشــبــكـــات

الشبكة تتكون ببساطة من ثلاث مكونات:

(١) رابط بين اجهزة الكمبيوتر مثلا: كبيل او خط ISDN

(٢) البروتوكول للاتصال: قوانين الاتصال

(٣) خدمات الشبكة: او ما هو جاهز للمشاركة كملفات او طابعات

الـبـروتـوكـولات

إن الإنسان والكمبيوتر لهما ميزتان متشابهتان، وهي أن كل منهما يستعمل لغة معقدة للتفاهم. فإذا أراد شخصان يتحدثان لغة واحدة أو لغتين مختلفتين، ولنقل العربية واليابانية مثلا أن يتفاهما، فإن عليهما أن يستخدما مترجما بينهما، أو أن يتحدث الاثنان بلغة ثالثة. و بالمثل إن أجهزة الكمبيوتر عندما تريد التعامل سواء موحدة في طريقة صنعها أو غير موحدة في طريقة صنعها أو تشغيلها، (منها نظام دوس ونظام يونكس ونظام ماكينتوش) ، ولكي نجعل هذه الأجهزة تتصل مع بعضها بواسطة شبكة واحدة وتتفاهم فيما بينها من خلال تلك الشبكة، فإن الشبكة تستخدم مجموعة مجموعة من المعايير أو القواعد لتبادل المعلومات تسمى البروتوكولات .

فالبرتوكولات تشبة لغة الإنسان لكنها تعتبر لغة أجهزة الكمبيوتر للتعامل مع بعضها .

**** البروتوكول هو مجموعة من المعايير أو القواعد أو المقاييس المستخدمة لتبادل المعلومات بين جهازي كمبيوتر أو لتحقيق الإتصال بين مجموعة من الأجهزة على الشبكة **.**

---- وهناك بعض الأمور التي تتعلق بالبروتوكولات هي :

.اختلاف الكثير منها في عملها ووظيفتها .
.لكل بروتوكول مزاياه وعيوبه.

ولذلك من الممكن أن تعمل عدة بروتوكولات معاً لتنفيذ عمل ما وفى هذة الحالة تسمى هذه المجموعة من البروتوكولات التي تعمل سويا اسم Protocol Stack أو Protocol Suite.

و يمكن تخيل هذه المجموعة من البروتوكولات كبناء مكون من عدة طوابق و في كل طبقة يوجد بروتوكول معين يقوم بوظيفة محددة ويتكامل مع غيره من البروتوكولات في الطوابق الأخرى.

وتسمح عملية ربط البروتوكولات معاً بمقدار كبير من المرونة في إعداد الشبكة، كما يمكن إعداد عملية الربط لتتناسب مع احتياجات المستخدم، ومن الممكن إعادة تنظيم عملية الربط لتتناسب مع مكونات أو بروتوكولات جديدة.

Protocol Stack

إن Protocol Stack هي مجموعة من البروتوكولات المتكاملة في عملها معا، و كل طبقة في هذه المجموعة تحتوي على بروتوكول مختلف يقوم بوظيفة مختلفة.

تحدد الطبقات السفلى من Protocol Stack الكيفية التي تسمح لمصنعي الشبكات إعداد أجهزتهم للإتصال مع أجهزة مصنعين آخرين و يطلق على بروتوكولات الطبقات السفلى من المجموعة اسم البروتوكولات منخفضة المستوى Low-Level Protocols.

بينما تحدد الطبقات العليا من Protocol Stack الطريقة التي تتفاهم فيها برامج الإتصال، و يطلق على بروتوكولات الطبقات العليا اسم البروتوكولات مرتفعة المستوى Protocols High-Level.

كلما ارتفعنا في طبقات Protocol Stack كلما زاد تعقيد البروتوكولات في هذه الطبقات.

يطلق مصطلح Binding على الطريقة التي يتم بها ربط البروتوكولات و ترتيبها معا لتكوين Protocol Stack.

ترتيب ربط البروتوكولات معا يحدد الترتيب الذي يسلكه نظام التشغيل في تنفيذه لبروتوكولات الشبكة.

فإذا كانت هناك مجموعة من البروتوكولات مرتبطة معا لتعمل مع بطاقة الشبكة ، فإن هذا الإرتباط يحدد الترتيب في تشغيل هذه البروتوكولات لتحقيق اتصال ناجح.

وظـيـفـة الـبـروتـوكـول

في الجهاز المرسل تكون البروتوكولات مسئولة عن القيام بالمهام التالية:

١- تقسيم البيانات الى حزم.

٢- إضافة معلومات العنونة الى الحزم.

٣- تحضير البيانات للإرسال.

بينما تقوم البروتوكولات في الجهاز المستقبل بالعمل التالي:

١- التقاط حزم البيانات من وسط الإتصال.

٢- إدخال حزم البيانات الى داخل الكمبيوتر عبر بطاقة الشبكة.

٣- تجميع كل حزم البيانات المرسلة و قراءة معلومات التحكم المضافة الى هذه الحزم.

٤- نسخ البيانات من الحزم الى ذاكرة مؤقتة لإعادة تجميعها.

٥- تمرير البيانات المعاد تجميعها الى البرامج في صورة مفهومة قابلة للإستخدام.

تنقسم البروتوكولات حسب وظيفتها الى ثلاث أقسام:

١- بروتوكولات تطبيقات Application Protocols.

٢- بروتوكولات نقل Transport Protocols.

٣- بروتوكولات شبكة Network Protocols.

تعمل بروتوكولات التطبيقات في الطبقات العليا من Protocol Stack و تتلخص مهمتها في تبادل البيانات و تحقيق التفاعل بين التطبيقات و من أمثلتها :

1- Server Message Block (SMB).
2- Novell's NetWare Core Protocols (NCPS).
3- File Transfer Access and Management Protocol (FTAMP).

و من بروتوكولات التطبيقات الخاصة بالإنترنت :

1- File Transfer Protocol (FTP).
2- Telnet.
3- HTTP

أما بروتوكولات النقل فتستخدم لتوفير جلسات الإتصال بين الكمبيوترات على الشبكة و هي مسئولة عن صيانة جودة و دقة المعلومات المنقولة بين الأجهزة، و من أمثلتها :

1- NWLink. الجزء الناقل من بروتوكول ميكروسوفت
2-NetBEUI. الجزء الناقل من بروتوكول
3- Sequenced Packet Exchange (SPX).
4- Transmission Control Protocol (TCP).

بينما تقدم بروتوكولات الشبكة خدمات ربط Link Services و تتلخص مهامها بما يلي :
١- عنونة و توجيه المعلومات .
٢- البحث عن إخطاء في عملية الإرسال .
٣- التعامل مع طلبات إعادة الإرسال .
٤- تحديد قوانين الإتصال في بيئات محددة من الشبكات مثل إثرنت و Token Ring.

من الأمثلة على هذه البروتوكولات ما يلي :

1- Internet Protocol (IP).
2- Internet work Packet Exchange (IPX).

بروتوكول الـــ TCP/IP (Transfer Control Protocol / Internet Protocol)

** وهو عبارة عن باقة من البروتوكولات التي تسمح للشبكات والأنواع المختلفة من الأجهزة بالاتصال فيما بينها.
ويوفر بروتوكول TCP/IP خصائص تشبيك وتوجيه ووصول لشبكة الإنترنت والاستفادة من مواردها.
وقد طور بروتوكول TCP/IP أساساً في عام ١٩٦٩ من قبل وكالة مشاريع البحوث المطورة للدفاع الأمريكي US Defense Advanced Research Projects Agency (DARPA).وقد استخدم هذا البروتوكول في البداية لبناء شبكة مشاريع البحوث المطورة للدفاع الأمريكي Advanced Research Projects Agency Network (ARPANET)، وهي عبارة عن شبكة كانت تربط بين أربع جامعات أمريكية تجري بحوثاً في مجال الدفاع.

** TCP/IP هو مجموعة من البروتوكولات التي تمكن الكمبيوترات من الاتصال.
في الحالة العادية وعندما لا تحتاج الكمبيوترات الي ان تتصل ببعضها لا توجد حوجة نهائيا الي بروتوكولات متفق عليها بين الاجهزة.
ولكن عندما تتصل الكمبيوترات ببعضها في شبكة تظهر الحوجة الي برتوكولات يتفق عليها.
يستطيع اليوم مدير اي شبكة كمبيوترات ان يختار من اكثر من بروتوكول ولكن بروتوكول ال TCP/ IPهو الاكثر استخداما .
جزء من السبب هو ببساطة ان ال TCP IPهو الذي تستعمله اكبر شبكة في العالم ال . INTERNET اذا اردت ان يتصل
جهازك مع الانترنت يجب ان تستخدم ال. TCP/ IP
عندما تعمل مجموعة من البروتوكولات مع بعضها فان المجموعة بشكل جماعي تعرف بـ Protocol Suite OR Protocol Stack .

الـ TCP/ IP مثال ل حزمة البروتوكول او Protocol Suite وصف لمجموعة من البروتوكولات التي تعمل مع بعضها .
يطلق علي TCP/ IP مصطلح Protocol suite او Protocol Stack وكلا المصطلحين يستخدمان بصورة متبادلة اي يعطيان نفس المعني رغم انهما يختلفان بعض الشئ.

سبب اخر ل شهرة ال TCP IP هو انه يتوافق تقريبا مع اي كمبيوتر في العالم TCP/ IP stack . مدعوم من كل اصدارات
انظمة التشغيل الكبري وانظمة تشغيل الشبكات وتشمل Windows 95\98 , Windows NT, Windows 2000,
Windows XP, Windows 2003, Linux, Unix, Netware.

TCP/ IPتسمي ايضا لغة الانترنت.

وهي ايضا لغة لكثير من الشبكات الصغيرة.

كل الكمبيوترات التي يلحق بها الانترنت لكي تتصل بفاعلية يجب ان يتفقوا علي لغة . مثلها مثل اي لغة بشر لها قواعد حتـــي يـــستطيع النـــاس الـــذين يـــشتركون فـــي المحادثـــة ان يفهـــوا مـــاذا يقـــول الاخـــرون.

لغة الكمبيوتر تحتاج الي مجموعة من القواعد حتي تستطيع الكمبيوترات ان تتصل بفاعلية . وبعض قواعد اللغة التي تـستخدمها الكمبيـوترات للاتـصال تـشتمل علـي متـي يـتم ارسـال البيانـات ومتـي يـتم اسـتقباله .

ومنذ ذلك الحين أصبح بروتوكول TCP/IP هو البروتوكول القياسي المستخدم لضمان التوافق بين الأنواع المختلفة من الأجهزة .

وتتكون باقة بروتوكولات TCP/IP من مجموعة من البروتوكولات، ولكن تعتبر بروتوكولاتTCP و IPهي البروتوكولات المحورية في هذه الباقة .

في الواقع عبارة عن بروتوكولين مختلفين ولكنهما يعملان معا دوما في نظام الإنترنت، ولهذا السبب فإنهما أصبحا مقبولين لأن يوصفا بأنهما وكأنهما نظام واحد.

TCP : يقوم هذا البروتوكول بأخذ مجموعة كبيرة من البيانات من برنامج معين ومن ثم تكسيرها إلى أجزاء صغيرة وتُرقم هذه الأجزاء وترتبها. وعندا يتم ارسال هذه الأجزاء المرقمة، فإن TCP في الجهاز المرسل ينتظر رسالة تأكيد وصول من الـ TCPفي الجهاز المُستقبل فإن لم تصل رسالة تأكيد وصول إلى TCP جهاز المرسل، فإن TCP يقوم بإعادة ارسال الأجزاء التي لم يأتي تأكيد بوصولها .

قبيل عملية بدأ الارسال، يقوم TCP الجهاز المرسل بارسال رسالة إلى TCP الجهاز المستقبل مستفسرا عن امكانية ارسال الرسالة الآن. فإن أتت الإجابة بالايجاب يقوم TCP الجهاز المرسل ببدأ عملية الارسال .وإن كانت الإجابة بلا، فإن TCP الجهاز المرسل ينتظر قليلا قبل أن يرسل رسالة استفسار مرة أخرى. وإن لم يأت الجواب على رسالة الاستفسار، فـإن TCP الجهـاز المرسـل يقـوم بإعـادة ارسـال رسـالة الاستفـسار .
وعندما تأتي رسالة الإيجاب، فإن TCP الجهاز المرسل يقوم بارسال الأجزاء المرقمة .ويتفق TCP الجهاز المرسل مع TCP الجهاز المستقبل على كمية الأجزاء المرسلة قبل الحصول على رسالة تأكيد وصول آخرى من الجهاز المستقبل. وفي هذه الأثناء ومع بدأ الارسال فإن TCP المرسل يكون دائرة واقعية Virtual Circuit مع TCP المستقبل.

IP : بعض أجهزة الكمبيوتر وهي التي تسمى رويتر Router أو الموجهات، تستعمل هذا البروتوكول لكي تقوم بتحريك رزم المعلومات في اتجاهاتها الصحيحة. إن كل رزمة لها عنوان IP خاص بالكمبيوتر الذي أرسل تلك الرزمة، وكذلك عنوان IP بالكمبيوتر المرسلة إليه تلك الرزمة. إن لكل كمبيوتر عنوان IP يتفرد به. وهو يتكون من أربعة أرقام يفصل بين كل رقم وآخر علامة الصفر. ونظرا لصعوبة تذكر هذه الأرقام، فقد تم اعتماد أسماء موازية لها، هذه الأسماء أسهل للحفظ، كما أنه يمكن أن يكون لها مدلولا معينا، سواء كان تجاريا أو تعليميا أو حكوميا أو غيره. وعندما تكتب اسما لكمبيوتر ما، وهو في الواقع عنوانه، فإنه في الواقع يترجم إلى اسمه الرقمي الأساسي.

من أهم مميزات حزمة بروتوكولات TCP/IP

- الموثوقية والانتشار
-يوفرالوصول إلي شبكة الإنترنت .
- دعم توجيه حزم البياناتRouting .
- توفير القابلية للإتصال لأنظمة التشغيل والأجهزة المختلفة .
- الدعم والتفاهم مع غيره من البروتوكولات .

أما العيوب الأساسية لحزمة TCP/IP فتتمثل فى الأمرين التاليين :

- حجم الحزمة الكبير وتعقيدها .
- سرعته المتواضعة .

لتسهيل عملية تصور كيفية نقل البيانات من جهاز إلى جهاز آخر تم تقسيم برتوكول TCP/IPإلى أربع طبقات وهما:

مكونات بروتوكول الـ TCP/IP

١) طبقة البرامج والعمليات (Process/Application Layer)

٢) طبقة النقل (Transport Protocols)

٣) طبقة الانترنت (Internet Layer)

٤) طبقة دخول الشبكة (Network Access Layer) أو (Physical Layer)

١/ طبقة البرامج والعمليات:
Process/Application Layer

البروتوكولات الموجودة في هذه الطبقة تستعمل في عمليات نقل البيانات وتتحكم في مواصفات الواجهة الأمامية للمستخدم (user interface) وهى أيضاً تعمل كوسيط بين البرنامج والشبكة .

٢/ طبقة النقل
Transport Layer

البروتوكولات الموجودة في هذه الطبقة تستعمل في خدمة النقل للبرامج. وتقوم الطبقة بانشاء وسائل اتصال معتمد عليها بين جهازين كما إنها تضمن نقل و توصيل البيانات بصورة خالية من الخطأ. ومن مسؤوليات الطبقة ترقيم الرزم والحفاظ على سلامة البيانات.

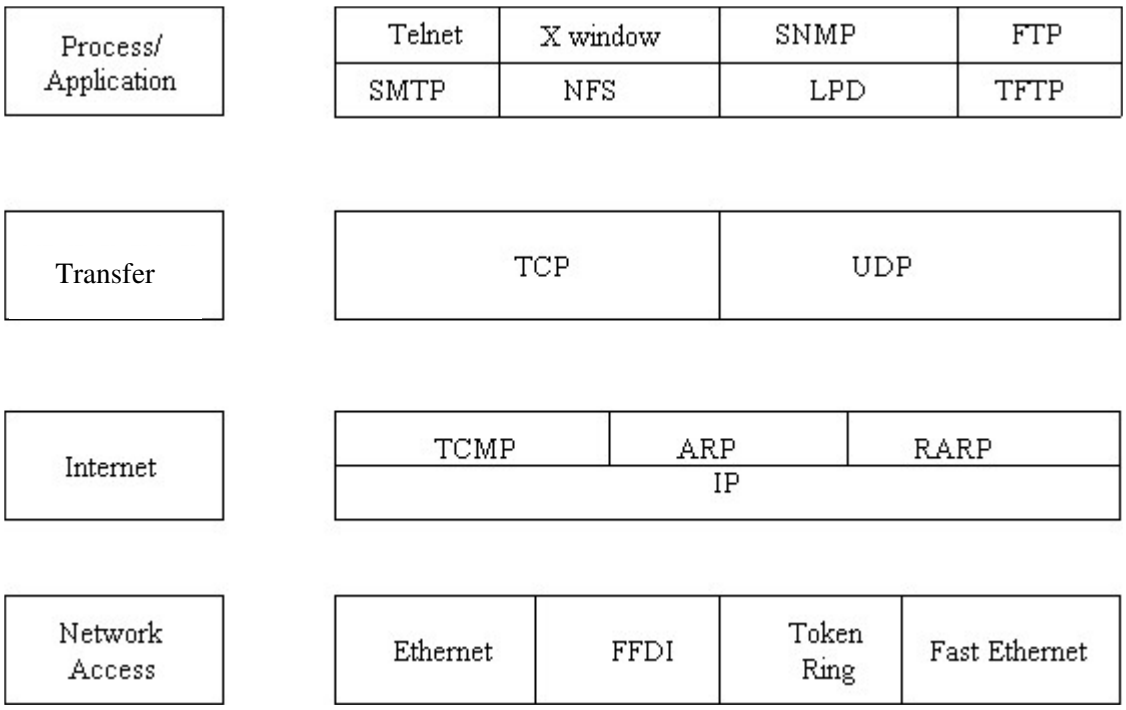
٣. الانترنت:
Internet Layer

البروتوكولات هنا مسؤولة عن النقل المنطقي للرزم في الشبكة وإعطاء أرقام الأي بي للمضيفين. وتقوم الطبقة أيضا بتوجيه الرزم في الشبكات المختلفة وتتحكم الطبقة أيضا في مجرى الاتصال بين مضيفين اثنين.

٤. دخول الشبكة:
Network Access Layer

هذه الطبقة تراقب عملية تبادل البيانات بين المستضيف والشبكة. وهي مسؤولة عن عنوان الهاردوير. البروتوكولات الموجودة في هذه الطبقة مسؤولة عن النقل المادي للبيانات، وهى أيضاً مكونة من الأجزاء الفيزيائية المكونة للشبكة مثل الأسلاك Cables ،الـ Router .

شكل توضيحى لطبقات بروتوكول الـ TCP/IP مع بروتوكولات كل طبقة



أولا: بروتوكولات طبقة البرامج والعمليات:
Process/Application Layer Protocols

١/ الشبكة التلفونية (Telnet.. (Telephone Network

من خلال هذا البروتوكول، يستطيع مستخدم الشبكة التليفونية باستعمال الموارد المتاحة في جهاز آخر يسمى بخادم الشبكة التليفونية.

٢/ بروتوكول نقل الملفات (FTP.. (File Transfer Protocol

وهو البروتوكول الخاص بنقل الملفات بين الأجهزة. وهو ليس فقط بروتوكول بل هو أيضا برنامج لتعديل الملفات. في أغلب الأوقات يُستعمل بروتوكول نقل الملفات مع الشبكة التلفونية للاتصال بخادم لبروتوكول نقل الملفات. بروتوكول نقل الملفات يعطيك الكثير من الحرية في تغيير ترتيب الملفات وتغيير اسم الملفات.

٣/ بروتوكول بسيط لنقل الملفات (TFTP.. (Trivial File Transfer Protocol

هذا البروتوكول عمله كبروتوكول نقل الملفات، إلا أن مميزاته محدودة، الخاصية الوحيدة هي القدرة على نقل الملفات فقط.

٤/ نظام ملف الشبكة NFS.. (Network File System)

هذا النظام يسمح لأنظمة الملفات المختلفة أن تعمل مع بعضها هكذا: لنفترض أنه عندنا شبكة خادم/زبون ونظام NT يعمل على الخادم وأنظمة الزبون هي Unix. نظام ملف الشبكة يسمح لجزء في ذاكرة RAM الخادم بتخزين ملفات Unix وبذلك تستطيع أجهزة الزبون استعمال هذه الملفات. فعلى الرغم من أن نظام الملفات في NT وUnix تختلفان من ناحية طول اسم الملف، أمن، وطريقة تسمية الملف - فإن مستخدمي NT وUnix يستطيعون الوصول إلى هذه الملفات بصورة طبيعية وبدون الحاجة لتغييرات.

٥/ بروتوكول نقل البريد البسيط SMTP .. (Simple Main Transfer Protocol)

يُستعمل هذا البروتوكول في نقل البريد الالكتروني.

٦/ Printer Daemon Line

صمم هذا البروتوكول من أجل المشاركة في الطابعات. فـLPD بالاضافة إلى LRP يستخدمان لارسال أوامر الطبع إلى طابعات الشبكة عن طريق TCP/IP

٧/ نافذة اكس X- Window

صممت نافذة اكس من أجل عمليات الخادم/الزبون. فهي تُعرف البروتوكول المسؤول عن استخدام واجهة تصويرية للمستخدم Graphical User Interface في علميات الخادم/الزبون.

٨/ بروتوكول بسيط لادارة الشبكة SNMP.. (Simple Network Management Protocol)

هذا البروتوكول مسؤول عن جمع وتحليل البيانات الموجودة في الشبكة. ففي أوقات مختلفة، يقوم هذا البروتوكول بطلب بيانات معينة من الأجهزة الموجودة بالشبكة. اذا كان كل شيء على ما يرام، فإن البروتوكول يستلم تقرير يسمى بـ"الخط الأساسي" Baseline وهذا التقرير يؤكد على صحة الشبكة. وإن كانت هناك مشاكل في الشبكة فإن البروتوكول يرسل رسائل مستعجلة إلى المسؤولين عن الشبكة تعلمهم بوجود خلل في الشبكة.

٩/ خدمة نطاق الاسم DNS .. (Domain Name Service)

أستحدثت هذه الخاصية لتسهيل حياة الانسان. فالفرد يتسطيع أن يصل لأي جهاز على شبكته عن طريق كتابة رقم الأي بي، ولكنه من الصعب حفظ أرقام الأي بي للكثير من الأجهزة، فتم استحداث خدمة نطاق الاسم بحيث يتم ايجاد واجهة أمامية للأي بي، فلا يحتاج الفرد إلى حفظ الأي بي، ولكنه يستطيع معرفة اسم الجهاز ومن خلال ذلك يستطيع الوصول إليه.

البروتوكول HTTP… hyper text transfer protocol

وحتى تستطيع تعلم بروتوكول http جيدا، يجب أن تعرف بأن كل شخص له رقم معين هذا الرقم يسمى بعنوان الآيبي Address IP وذلك فى بروتوكول الـ TCP/IP عندما يتم تبادل البيانات بين جهازين فإنه يتم توجيه حزم من البيانات بين الطرفين كل حزمة من البيانات تسمى باكت Packet، وتكون الحزمة مختومة بعنوان IP المرسل إليه حتى تعرف طريقها عبر الشبكة، والجهاز الذي يوجه هذه الحزم يسمى router، وهو لا يهمنا كثيرا الآن.

الأمر الثاني الذي يجب أن تعرفه عن بروتوكول TCP/IP هو أنه ينص على أن الإنترنت مقسمة إلى عدة منافذ Ports لتبادل البيانات، عدد هذه المنافذ يقارب ٦٥٠٠ منفذ، وقد جرى العرف على إعطاء منفذ لكل خدمة من خدمات إنترنت الأساسية، فمنفذ بروتوكول http هو ٨٠، لذلك فإن المتصفح الذي تستعمله يقوم تلقائيا بتوجيه طلباته عبر المنفذ ٨٠، والمنفذ القياسي لبروتوكول نقل الملفات FTP هو ٢١، وهكذا.

الأمر الثالث الذي يجب أن تعرفه عن الإنترنت هو عناوين إنترنت، تخفي عناوين إنترنت الكثير من الأسرار عن أعيننا، يتكون عنوان إنترنت من عدة أجزاء وبنيه الأساسية كالتالي :

Protocol: hostname: port

أول كلمة هي البروتوكول المستخدم لتبادل البيانات، من هذه البروتوكولات HTTP و FTP كما تعلم، وأما القسم الثاني فهو إسم المكان الذي نريد أن نتصل به وفائدة الإسم هو تسهيل حفظ الأسماء، بدلا من استخدام أرقام IP، أما القسم الثالث فهو رقم المنفذ.

وينقسم إسم الجهاز hostname بدوره إلى عدة أقسام، وكأنها شجرة من الأعلى إلى الأسفل إلا أنها تكون من اليمين إلى اليسار، يكون هنالك في البداية جهاز رئيسي، هذا الجهاز الرئيسي يقودك إلى جهاز فرعي من شبكته، والفرعي إلى فرع آخر وهكذا، الإسم الذي يقع في أعلى الشجرة يسمى إسم النطاق الأعلى Upper domain، وهي عبارة عن com أو org أو net أو uk أو kw وهكذا، كل هذه أسماء رئيسية، تحوي الأسماء الرئيسية أفرع تخرج منها، إسم الفرع يأتي دائما قبل إسم الأب ويفصل بينها بنقطة، فيكون microsoft.com مثلا، الفرع فيه هو Microsoft والأب هو com وهكذا.

هنالك عدد محدود من النطاقات العليا تتحكم فيها منظمة خاصة، هذه المنظمة هي المسؤولة عن توزيع الأسماء الفرعية من إسم النطاق الرئيسي، وبمجرد أن تبيع الإسم الفرعي لجهة ما تصبح هذه الجهة هي القادرة على إعطاء أسماء فرعية من اسمها، مثلا msdn.microsft.com هنا قامت شركة Microsoft بشراء الإسم الفرعي Microsoft من الجهة المالكة للإسم الرئيسي com، وقامت الشركة بعد ذلك بإعطاء إسم فرعي وهو msdn من اسمها الرئيسي وهو microsoft.com، وهذا يمكن أن يكون هنالك أي عدد من التفريع في العنوان.

ولكننا عندما نريد أن نذهب إلى مكان ما فإننا نكتب مثلا .. http://www.microsoft.com/windows/ie/،
فما علاقة هذا الإسم بالوصف السابق؟

في العنوان السابق إسم البروتوكول هو http وبعده جاءت النقطتين كما قلنا سابقا، بعد إسم البروتوكول جاء إسم الجهاز، وابتدأ اسم الجهاز هنا بعلامتي // أي أن الجهاز الذي نريد الوصول إليه جهاز خارجي متصل بنا عن طريق الشبكة، بعد ذلك يأتي إسم الجهاز، كما بينا، وبعد ذلك كان من المفترض أن نضع نقطتين ونكتب اسم المنفذ، ولكن

المتصفح يعرف بأنه يجب أن يرسل الطلبات عبر المنفذ رقم ٨٠ ما لم تخبره خلاف ذلك، لأنه يعرف أنه المنفذ القياسي، وأما الجزء الباقي من العنوان فهي عبارة عن جزء من المعلومات التي يتم إرسالها إلى المزود، وهي ليست جزءا من العنوان.

وأيضاً عندما يطلب المستخدم من المستعرض أن يجلب له صفحة من الانترنت، فإن المستعرض يجلب هذه الأوامر باستخدام بروتوكول يدعى بروتوكول التحكم في نقل البيانات .TCP هذا البروتوكول هو بروتوكول نقل للبيانات وهو يضمن أن البيانات قد تم إرسالها ووصولها بشكل صحيح.

وقبل أن يتم إرسال البيانات عبر الشبكة يجب عنونتها، والبروتوكول الذي يقوم بعنونه البيانات يدعى .HTTP يقوم هذا البروتوكول بوضع عنونه للبيانات لكي يعرف البروتوكول TCP أين سينقل البيانات (فهو لايستطيع نقل البيانات إذا لم يكن لها هدف أو مكان.

يستخدم البروتوكول HTTP عن طريق الويب في عملية نقل البيانات من كمبيوتر إلى آخر . عندما ترى الصفحة متبوعة بـ http:// فإنك تعلم مباشرة أن الانترنت يستخدم البرتوكول HTTP لإحضار هذه الصفحة، يمكنك أن تأخذ صورة بأن الTCP عبارة عن ساعي بريد الذي يقوم بإيصال رسالة.. هذه الرسالة فيها طابع بريد وعنوان وهو مانسميه بال.HTTP

يتم تمرير الطلب من المستعرض إلى ملقم أو سيرفر الويب وهو ما يعرف بـ .HTTP request ويقوم السيرفر برؤية مستودع البيانات لديه لكي يحصل على البيانات المطلوبة ..

فإذا وجد الصفحة في المستودع قام بإرسالها على شكل حزم إلى الجهة التي قامت بالطلب باستخدام بروتوكول TCP وتُعنون هذه الحزم لمستعرض الانترنت لديك باستخدام بروتوكول) http ننبه دائماً إلى أنه يرسلها على شكل حزم لكي تعرف السبب عند عدم ظهور صفحة ويب كاملة أن هناك حزمة لم ترسل بشكل جيد)، ولكن إذا لم يجد السيرفر الصفحة المطلوبة فإنه يقوم بإرسال صفحة تحتوي على رسالة الخطأ ٤٠٤، وهذه الصفحة التي أرسلت من ملقم الويب إلى المستعرض لديك تسمى. HTTP response .

رغم ما أخذناه من معلومات كثيرة وقصص كثيرة تشبه قصص ألف ليلة أو حكايات الأطفال إلا أنه رغم ذلك يفوتنا الكثير من التفاصيل في هذا الموضوع لذلك دعنا نغوص قليلاً في التفاصيل عن بروتوكول HTTP بشكل خاص.

عندما تقوم بعملية طلب لصفحة من السيرفر هناك أمور إضافية ترسل مع عملية الطلب http request غير الـURL وهي ترسل كجزء من http request .
نفس الموضوع مع الhttp response هناك أمور أخرى تصل معه كجزء منه .

الكثير من هذه المعلومات تولد تلقائياً في رسالة الـHTTP ولايقوم المستخدم بالتعامل معها مباشرة ، إذن لايحتاج أن تقلق نفسك بشأن هذه المعلومات إذا أنت لم تنشأها في الأصل ويجب أن تأخذ أيضا في معلوماتك أن هذه المعلومات ترسل كجزء من الـHTTP request والـHTTP response لأن سكربت الـPHP الذي نصنعه يمنحنا تحكماً إضافيا بهذه المعلومات .

كل رسائل الـHTTP تأخذ تنسيقاً معيناً سواء كانت Request أو Response . نستطيع أن نقوم بتقسيم هذا التنسيق إلى ثلاثة أقسام :

١ - Request/response line
٢ - Http header
٣ - Http body

المحتوي من هذه الأشياء الثلاثة يعتمد على نوع الرسالة إذا كانت Http Request أو HTTP response لذلك سنتكلم عنهم بتعمق أكثر .

لنتوقف لحظات وننتظر لكي يتضح إلينا مفهوم المعاجلة التي تتم:

أولاً عملية الطلب HTTP Request:

يجب أن يحتوي ال request على الأقل ال request line (سطر الطلب) وال HOST .

يرسل مستعرض الانترنت طلبيه (HTTP request) إلى ملقم الويب تحتوي على التالي:

١/ Request Line The:

السطر الأول من كل طلبيه (http request) هي Request Line الذي يحتوي على ثلاث أنواع من المعلومات:

١. أمر HTTP وهو مايسمى بـ method .
٢. المسار من السيرفر إلى المصادر المطلوبة (صفحات الانترنت) المطلوبة من قبل العميل (المستعرض) .
٣. إصدارة ال HTTP .

إذن كمثال على ال Request Line انظر إلى السطر التالي: (ال method يخبر السيرفر كيف يتعامل مع الطلب).

GET /testpage.htm HTTP/1.1

هناك ثلاث أنواع شائعة من ال method والتي تظهر في الجدول التالي:

Method	وصفه
GET	عبارة عن طلب لمعلومات تستقر في نفس صفحة الانترنت، وهذا الmethod الذي يستخدم. وهو المستخدم بكثرة في صفحات الانترنت ويعتبر الرئيسي فيهم. المعلومات التي تطلب بواسطة هذا الأمر قد تكون معلومات قد تكون أي شيء من: صفحة الhtml أو php إلى: مخرج من سكربت (برنامج) بيرل أو جافا أو ملفات تنفيذيه أخرى. يمكنك إرسال بعض المعلومات المحددة إلى مستعرض الانترنت لديك عبر نموذج (Form) في الصفحة.
HEAD	مثل الGET.. باستثناء أنه يقوم بعملية طلب للـheader فقط من غير بيانات (data).
POST	هذا الأمر يقوم بإرسال البيانات إلى السيرفر كجزء من HTTP body. هذه البيانات تعالج بواسطة برنامج مخصص لمعالجتها (Perl or php) على السيرفر.

هنـاك أوامر عديدة أخرى مثل: (OPTION - CONNECT - TRACE - DELETE - PUT)..
ولكنها تستخدم بقلة، ويمكنك أن تجد شرحاً موفياً لها باللغة الانجليزية على الرابط التالي: http://www.rfc.net

٢/ Header HTTP:

البت الثاني من المعلومات هو الهيدر HTTP Header.. الذي يحتوي على تفاصيل أو وثائق عن العميل مثل نوع المتصفح (نتسكيب أو اكسبلورر) الذي قام بطلب الصفحة والوقت والتاريخ والإعدادات العامة.

الHTTP Header يحتوي على معلومات نستطيع تقسيمها إلى ثلاث فئات وهي:

١. عامة General / تحتوي على معلومات إما عن العميل أو السيرفر ولا تخصص إلى فرد أو مجموعة .
٢. شخصية Entity / تحتوي على معلومات عن البيانات التي أرسلت بين المتصفح والسيرفر .
٣. مطلوبة Request / تحتوي على بيانات عن إعدادات العميل والأنواع المختلفة المقبولة من البيانات .

وهذا مثال:

Accept: * / *

Accept language: Arabic-KSA.
Connection: Keep -Alive.
Host: www.arabbuielder.com
Referer:http://www.arabbuielder.com/index.php?something=132
Agent :lexploer (win98- User)

مثلما ترى ال HTTP Header عبارة عن أعداد يتكون من عدة سطور، كل سطر يحتوي على قيم معينة.

هناك عدة سطور تشكل ال HTTP header وأكثرها اختياري. يقوم الHTTP بالإخبار عن انتهاء معلومات ال header بترك سطر فارغ (وهذا يكون في الHTTP1.1).

٣/ The HTTP Body:

إذا تم استخدام الأمر POST في ال HTTP Request Line.. عندها يقوم ال HTTP بطلب المعلومات التي أرسلت في ال body إلى السيرفر.

ثانياً عملية الإجابة Response HTTP:

يرسل من السيرفر إلى المستعرض، ويحتوي على ثلاث أشياء:

١- The Response Line.
٢- HTTP Header.
٣- HTTP Body.

١/ The Response Line:

ال line Response يحتوي فقط على نوعين من المعلومات:
١- رقم إصدارة ال HTTP .
٢- شفرة أو كود ال http request التي تقوم بتحديد ما إذا كان ال request ناجحاً أم فاشل .

مثال:
HTTP/1.1 200 OK

في هذا المثال يقوم ال response line بإرجاع القيمة ٢٠٠ متبوعة بالكلمة OK. هذه تشكل وتشير إلى نجاح ال request ويكون ال response يحتوي على الصفحة المطلوبة والبيانات من السيرفر.

ومثال آخر هو الشفرة ٤٠٤.. وتظهر عندما تقوم بطلب صفحة ويفشل السيرفر في الحصول عليها.
هناك خمس فئات من الشفرات:

الفئة	وصفها
١٠٠ - ١٩٩	يتم إعطاء هذا الكود إذا كان الطلب (request) يتم معالجته حالياً.
٢٠٠ - ٢٩٩	يتم إعطاء هذا الكود إذا تم استقبال الطلب بنجاح.
٣٠٠ - ٣٩٩	يتم إعطاء هذا الكود إذا كانت البيانات قد تم تحويلها أو تحريكها من موضعها.
٤٠٠ - ٤٩٩	يتم إعطاء هذا الكود إذا الطلب فيه خطأ من قبل العميل (المستعرض).. غير كامل أو غير صحيح أو غير ممكن.
٥٠٠ - ٥٩٩	يتم إعطاء هذا الكود إذا كان الخطأ من قبل السيرفر. أي إذا كان الطلب صحيحاً وموجوداً لكن السيرفر فشل في معالجته وإخراجه.

٢/ HTTP Header:

ال header Response يعتبر مشابه لـ Request header الذي ناقشناه في الأعلى. وتنقسم المعلومات التي فيه أيضاً إلى ثلاث أنواع:

١. عامة General / معلومات عن ال client أو السيرفر ولا تخصص إلى واحد منهما.
٢. شخصية Entity / يحتوي على معلومات عن البيانات التي يتم إرسالها بين السيرفر والعميل .
٣. الإجابة Response / يحتوي معلومات عن السيرفر الذي قام بإرسال الرد وكيفيه تعامله ومعاجلته للرد (Response) .

كما قلنا سابقاً.. يتكون من عدة سطور ويتم وضع سطر فارغ للإعلام عن انتهاء الهيدر (Header):

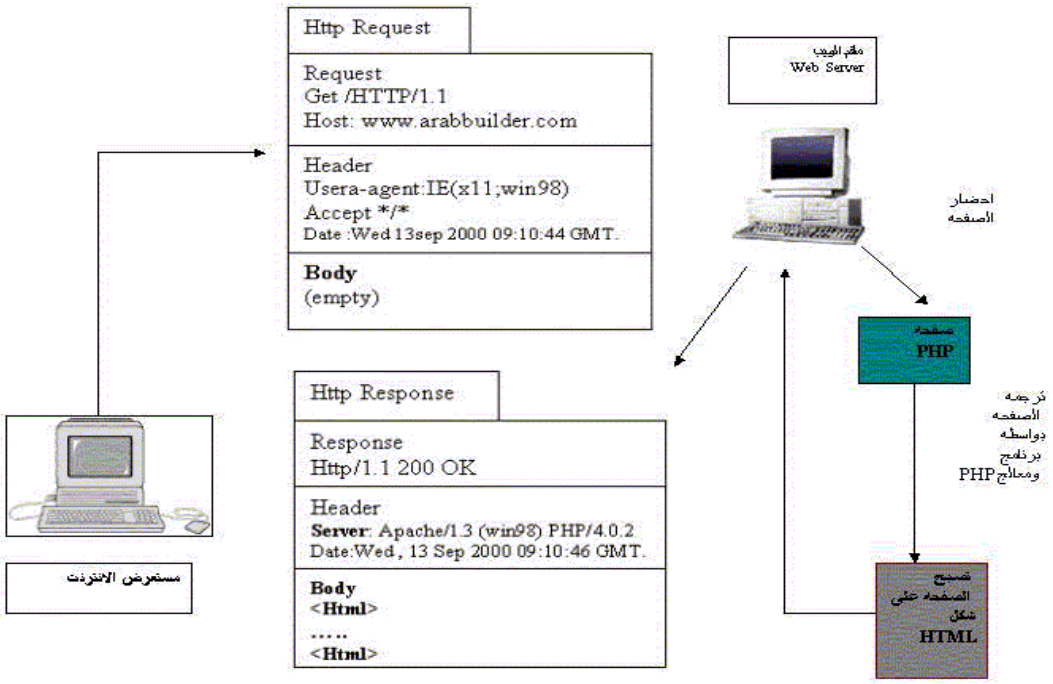
-The status HTTP/1.1 200 line OK
Date: Mon; 1st Nov 1999, 16:12:23 GMT -General header
-The response (Server : Apache/1.3.12 (Unix) (SUSE/Linux PHP/4.0.2
-Entity Header Last-modified: Fri, 29 Oct 1999, 12:08:03 GMT

السطر الأول ناقشناه، والسطر الثاني مفهوم من غير شرح، السطر الثالث يقوم بتحديد البرنامج تبع السيرفر ونوعه ونظام التشغيل القائم عليه، والسطر الأخير يقوم بتعريف آخر وقت تمّ فيه تعديل أو تجديد الصفحة.

* ملاحظة/ قد يحتوي الهيدر (Header) على أكثر من هذه المعلومات أو معلومات مختلفة وهذا يعتمد على نوع الشيء المطلوب من السيرفر.
إذا أردت معرفة معلومات أكثر عن هذه الأقسام.. تستطيع مراجعة المقالة رقم ٢٠٦٨ في الموقع التالي:
http://www.rfc.net .

٣/ The HTTP Body:

إذا تمت معالجة الطلب بنجاح.. فإن ال HTTP Response Body يحتوي على شفرة الHTML ويقوم مستعرض الانترنت بتفسيرها وتحويلها إلى الصفحة النهائية التي تراها.



صورة توضح عمليتى الطلب والإجابة ببروتوكول الـHTTP ومكونات كل عملية.

ثانياً: بروتوكولات طبقة النقل (المضيف إلى المضيف):

Transport Layer Protocols

أهم وظيفة لهذه الطبقة أن تحمى الطبقة العليا من عمليات الشبكة المعقدة. كأن هذه الطبقة تطلب من الطبقة العليا كل البيانات والارشادات وهي تقوم بعملية توصيل وتنظيم المعلومات. هناك بروتوكولان اثنان في هذه الطبقة، وهما:

١/ بروتوكول تحكم التوصيل: Transmission Control Protocol (TCP)

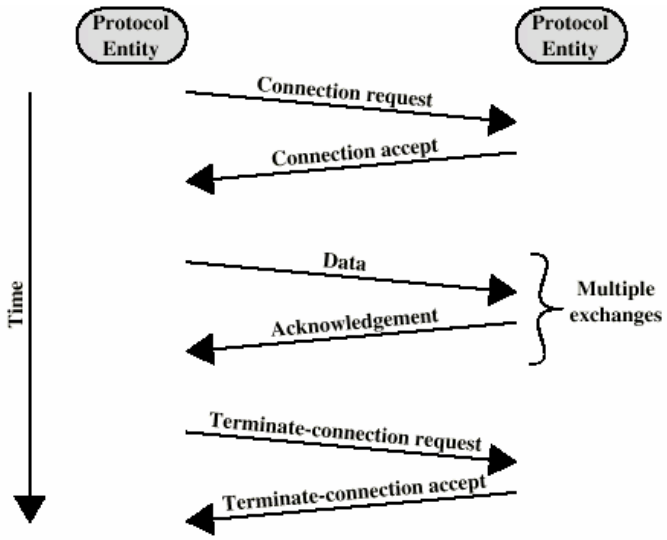
٢/ البروتوكول User Datagram Protocol (UDP)

أولا: بروتوكول تحكم التوصيل: Transmission Control Protocol / (TCP)

يقوم هذا البروتوكول بأخذ مجموعة كبيرة من البيانات من برنامج معين ومن ثم تكسيرها إلى أجزاء صغيرة وتُرقم هذه الأجزاء وترتبها. وعندا يتم ارسال هذه الأجزاء المرقمة،فإن TCP في الجهاز المرسل ينتظر رسالة تأكيد وصول من الـTCP في الجهاز المُستقبل، فإن لم تصل رسالة تأكيد وصول إلى TCP جهاز المرسل، فإن TCP يقوم بإعادة ارسال الأجزاء التي لم يأتي تأكيد بوصولها.

قبيل عملية بدأ الارسال، يقوم TCP الجهاز المرسل بارسال رسالة إلى TCP الجهاز المستقبل مستفسرا عن امكانية ارسال الرسالة الآن. فإن أتت الإجابة بالايجاب يقوم TCP الجهاز المرسل ببدأ عملية الارسال. وإن كانت الإجابة بلا، فإن TCP الجهاز المرسل ينتظر قليلا قبل أن يرسل رسالة استفسار مرة أخرى. وإن لم يأت الجواب على رسالة الاستفسار، فإن TCP الجهاز المرسل يقوم بإعادة ارسال رسالة الاستفسار.

وعندما تأتي رسالة الإيجاب، فإن TCP الجهاز المرسل يقوم بارسال الأجزاء المرقمة. ويتفقTCP الجهاز المرسل



مع TCP الجهاز المستقبل على كمية الأجزاء المرسلة قبل الحصول على رسالة تأكيد وصول آخرى من الجهاز المستقبل. وفي هذه الأثناء ومع بدأ الارسال فإن TCP المرسل يكون دائرة واقعية Virtual Circuit مع TCP المستقبل.

و يقوم هذا البروتوكول بتحديد كيف سيتم تكسير المعلومات إلى رزم وإرسالها عبر الإنترنت. يقوم TCP بتحديد طريقة تجزئة الرسائل أو المستندات لتجعلها بشكل ملفات أو رزم صغيرة Packets، بحيث تتحرك بسرعة خلال الشبكات في اتجاه مقصدها النهائي. يتكون كل باكيت من ١ إلى ١٥٠٠ "بت" بما فيها عنوان الكمبيوتر المرسل والكمبيوتر المستقبل. وتسافر تلك الرزم مستقلة عن بعضها البعض من كمبيوتر إلى آخر، بأي اتجاه من أجل تفادي العوائق، وكذلك بأي سرعة متوفرة .

كما ترى يا عزيزي القارئ، فإن هناك الكثير من الأمور التي يجب الإحاطة بها لارسال البيانات عن طريق TCP، مما يؤدي إلى بطء في عملية الارسال. ولكن الناحية الإيجابية هي الاعتمادية: فيمكن الاعتماد على TCP لارسال بيانات صحيحة وخالية من الخطأ. ولكن TCP قد صنع في السبعينات من القرن الماضي، عندما لم تكن طبقات التوصيل متطورة بالشكل اللازم، فكانت الكثير من البيانات تضيع أثناء الارسال أو يتم تحويرها. فاستدعت الحاجة انشاء بروتوكول ذو اعتمادية كبيرة. ولكن الآن ومع التطوير في بنية الطبقات وتحسين عمليات تصحيح الأخطاء، أصبحت اعتمادية TCP غير مهمة على النحو السابق، ولكن في هذا العصر السريع تطلب الأمر استحداث بروتوكول جديد يفي هذا الطلب من ناحية السرعة واعتمادية أقل وهي User Datagram Protocol

ثانياً : البروتوكول UDP... User Datagram Protocol

أما البرتوكول الثاني فهو UDP وهذا البرتوكول هو من نوع No connection-Based بمعنى الإتصال غير الموثق وهو لا ينشئ جلسة عمل بين الحواسيب أثناء الاتصال وهو لا يضمن وصول البيانات مثل ما ارسلت به وهو عكس TCP ولكن هذا البرتوكول له مميزات تجعل يستحب إستخدامه في بعض الحالات مثل عند إرسال بينات جماعية عامة وعند الحاجة إلى السرعة وسرعته من عدم حاجته إلى التحقق من دقه الإرسال ويستخدم في نقل الوسائط المتعدده مثل الصوت و الفديو لان الوسائط لا تحتاج إلى دقه الوصول ونستطيع أن نقول أن هذا البروتوكول ذو فاعلية كبيرة وسريع الأداء... ومن أهم الاسباب التي أدت إلى إنشاء البروتوكول UDP أن الإرسال عبر هذا البروتوكول لا يتطلب إلا القليل من الحمل و الوقت إذ أن رزمة UDP لا تحتوي على كل المعطيات التي ذكرت مع البروتوكول TCP لمراقبة الإرسال .. لذلك سمى بروتوكول الإتصال غير الموثق .

ثالثاً بروتوكولات طبقة الإنترنت
Internet Layer Protocols

أولاً : البروتوكول IP... Internet Protocol .

IPهي اختصار لـ Internet Protocol و تعني بروتوكول الانترنت. كما نعرف البروتوكول هو مجموعة من القواعد (القوانين) التي يجب اتباعها للوصول الى هدف معين. الهدف هنا هو تمكين الاجهزة المختلفة التي تعمل بطرق مختلفة و برامج مختلفة من تبادل المعلومات بصورة صحيحة و لتكوين ما نعرفه بالانترنت. اي ان الانترنت هي عبارة عن مجموعة كبيرة من الشبكات و كل شبكة هي عبارة عن مجموعة من اجهزة الكمبيوتر و ملحقاتها و اجهزة الاتصال التي تتبادل المعلومات و الخدمات فيما بينها باستخدام العديد من البروتوكولات المتفق عليها .

احد هذه البروتوكولات هو بروتوكول الانترنت او الايبي و مهمته تنظيم الاجهزة لتكوين الانترنت. من بين قواعد الايبي قواعد لتعريف كل جهاز كمبيوتر سواء كان خادم (Server)او ضيف (Host) او جهاز ملحق مثل الراوتر (Router)و غيرها بما يعرف بعنوان الايبي .(IP Address) ايا من هذه الاجهزة يجب ان يكون له رقم ايبي محدد ليتمكن من الاتصال بشبكة الانترنت و هو له بمثابة الاسم الذي يميزه عن غيره فلا يمكن لجهازين ان يكون لهما نفس الايبي في نفس الوقت على الشبكة.

يمكن تعريف IP address بأنه معرف رقمي يتم تعيينه لكل جهاز على الشبكة بحيث يصبح عنوانا خاصا له يسهل الوصول إليه و تحديد موقعه على الشبكة ويسمح له بالاتصال بغيره من الأجهزة.
يتكون IP address من ٣٢ bit و يكون مقسم الى أربع أقسام كل قسم عبارة عن byte أو octet و يتم كتابته بأحد الأساليب التالية:

١- باستخدام النظام العشري و يكون كل قسم مفصول عن الآخر بنقطة مثل : ١٧٢,١٦,٣٠,٥٦,

٢- باستخدام النظام الثنائي مثل: ١٠١٠١١٠٠,٠٠٠١٠٠٠٠,٠٠٠١١١١٠,٠٠١١١٠٠٠,

٣- باستخدام النظام الست عشري مثل: AC 10 1E 38 و يستخدم في سجل النظام Windows Registry.

وينقسم رقم IP ألى قسمين رقم للشبكة ورقم عنوان الحاسب، مثلا لنفترض وجود جهازين في الشبكة أحدهما له العنوان ١٩٢,١٦٨,١,٢ و الآخر لديه العنوان ١٩٢,١٦٨,١,٣ نلاحظ أنهما يشتركان في نفس عنوان الشبكة و هو ١٩٢,١٦٨,١ ، و لكن يكون لكل منهما عنوانه الخاص و يطلق عليه node address

يوجد ٥ فئات (Class) للآيبي. هيA,B,C,D,E
للتوضيح فقط لنرمز لأول قسم من الآيبي هو W والقسم الثاني هو X والقسم الثالث هو Y والقسم الرابع هو Z اذا يكون الآيبي على النحو التالي:
W.X.Y.Z

المدى الأول لعناوين الشبكة : Class A

يتميز هذا المدى من عناوين الشبكة وفقا لما قرره مصمموها بأن أول bit من أول byte من عنوان الشبكة المنتمي للمدى Class A لابد أن تكون قيمته صفر مما يعني أن عناوين المدى Class A يجب أن تتراوح بين ٠ و ١٢٧ ، لنفهم كيف حصلنا على هذين الرقمين للنظر سويا الى البايت الأول و الذي اتفقنا أن البت الأول منه يجب أن يكون ٠ هذا يعني أن العناوين في هذا البايت ستبدأ من :

٠٠٠٠٠٠٠٠

وتنتهي بالعنوان:

٠١١١١١١١

عند تحويل الرقمين الى النظام العشري نحصل على ما يلي:

٠٠٠٠٠٠٠٠ = ٠

٠١١١١١١١ = ١٢٧
و هكذا إذن ، إذا رأينا أي عنوان IP يبتدئ بأي رقم بين ٠ و ١٢٧ سنعرف أنه ينتمي الى المدى Class A.

المدى الثاني لعناوين الشبكة : Class B

عناوين هذا المدى تتميز بما قرره المصممين من أن أول bit من أول byte من عنوان الشبكة المنتمي للمدى Class B لابد أن تكون قيمته ١ أما البت الثاني فيجب أن تكون قيمته ٠ دائما، و بهذا حصلنا على مدى العناوين ابتداء من ١٠٠٠٠٠٠٠ = ١٢٨ و انتهاء ب ١٠١١١١١١ = ١٩١.

المدى الثالث لعناوين الشبكة : Class C

عناوين هذا المدى تتميز بما قرره المصممين من أن البت الأول و الثاني من البايت الأول يحملان القيمة ١ بينما يحمل البت الثالث القيمة ٠ دوما، و بهذا حصلنا على مدى العناوين ابتداء من ١١٠٠٠٠٠٠ = ١٩٢ و انتهاء ب ١١٠١١١١١ = ٢٢٣.

هناك بعض العناوين التي لا يستطيع مدير الشبكة منحها للأجهزة أبدا رغم أنها قد تنتمي الى مدى مسموح به كما يلي:

١- العنوان ٠,٠,٠,٠ و يستخدم من قبل موجهات routers التابعة لشركة Cisco للإشارة الى الوجهة الافتراضية default route عند توجيه حزم البيانات.

٢- العنوان ٢٥٥,٢٥٥,٢٥٥,٢٥٥ و يستخدم لبث أو إرسال البيانات الى جميع الأجهزة nodes على الشبكة الحالية.

٣- لا يمكن أن يكون الجزء من عنوان IP الخاص بالجهاز كله ٢٥٥ أو ٠ أي أنك لا تستطيع منح جهاز ما العنوان التالي على سبيل المثال : ١٢٨,٢,٢٥٥,٢٥٥ أو ١٢٨,٢,٠,٠ و مثال آخر:
١٩٢,١٦٨,١,٢٥٥ أو ١٩٢,١٦٨,١,٠، حيث يشير كل من ١٢٨,٢,٠,٠ و ١٩٢,١٦٨,١,٠ الى عنوان الشبكة

بينما يشير كل من ١٩٢,١٦٨,١,٢٥٥و ١٢٨,٢,٢٥٥,٢٥٥ الى العنوان المستخدم في البث لجميع أجهزة الشبكة.

٤- لا يمكن أن يكون الجزء من عنوان IP الخاص بالشبكة كله ٠ أو ٢٥٥ أي أنك لا تستطيع منح جهاز ما العنوان التالي: ٠,١,٥,٣ .

٥- العنوان ١٢٧,٠,٠,١ لا يمكن منحه لأي جهاز و هو يستخدم تلقائيا من قبل الجهاز لغرض اختبار اتصاله بأن يقول بإرسال حزمة من البيانات الى نفسه.

نعود من جديد لتقديم المزيد من التفاصيل حول عناوين كل من المدى A, B ، C.

عـنــاويــن الــمــــدى A:

في المدى Class A يتم تعيين البايت الأول لعنوان الشبكة بينما تتوفر البايتات الثلاثة الأخرى لعناوين الأجهزة على الشكل التالي:

Network.node.node.node ، على سبيل المثال فإن في عنوان IP التالي: ٤٩,٢٢,١٠٢,٧٠ يعتبر ٤٩ هو عنوان الشبكة بينما يعتبر ٢٢,١٠٢,٧٠ هو عنوان الجهاز. كل جهاز على هذه الشبكة لابد أن يكون لديه نفس عنوان الشبكة أي ٤٩.

بالنسبة للعناوين المتاحة للشبكة فقد ذكرنا أنها بين ٠ و ١٢٧ و لكننا ذكرنا من ضمن العناوين التي لا يمكن استخدامها كل من العنوان ٠ كعنوان للشبكة و العنوان ١٢٧ مما يعني أننا فعليا نستطيع استخدام العناوين من ١ الى ١٢٦ فقط لاستخدامها كعناوين للشبكة في Class A.

أما العناوين المتاحة لجزء الجهاز node من عنوان IP في Class A فهي تتكون من ٣ بايتات أو ٢٤ بت مما يعني أننا نستطيع الحصول على ٢ ^ ٢٤ عنوان مختلف أي أننا نستطيع في شبكة واحدة من النوع Class A أن نشبك عدد ١٦،٧٧٧،٢١٦ جهاز و نعطي كل جهاز عنوان مختلف و لكننا ذكرنا أنه لا يمكن لعنوان الجهاز أن يكون كله ٠ أو ٢٥٥ مما يعني أن العدد الحقيقي الأجهزة التي من الممكن شبكها هو ٢٤٨٢ – ٢ = ١٦,٧٧٧،٢١٤.

و تكون عناوين IP التي يمكن منحها للأجهزة هي كل العناوين بدءا من ١٠,٠,٠,١ و انتهاء ب ٠,٢٥٥,٢٥٥,٢٥٤.

عـنــاويــن الــمــدى B:

في المدى Class B يتم تعيين البايت الأول و الثاني لعنوان الشبكة بينما يتوفر البايتان الباقيان لعناوين الأجهزة على الشكل التالي:

Network.Network.node.node ، على سبيل المثال فإن في عنوان IP التالي: ١٧٢,١٦,٣٠,٥٦ يعتبر ١٧٢,١٦ هو عنوان الشبكة بينما يعتبر ٣٠,٥٦ هو عنوان الجهاز.

العدد الأقصى لعناوين الشبكات التي يمكن الحصول عليه في المدى B هو ١٤٨٢=١٦،٣٨٤ ، لأننا ذكرنا أنه يخصص بايتان لعنوان الشبكة أي ١٦ بت و لكننا ذكرنا أن المصممين نصوا على حجز البت الأول لتكون قيمته ١ و حجز البت الثاني لتكون قيمته ٠ مما يترك لنا ١٤ بت لاستخدامها بدءا من ١٢٨,٠ و انتهاء ب ١٩١,٢٥٥.

أما العناوين المتاحة لجزء الجهاز node من عنوان IP في Class B فهي تتكون من بايتان أو ١٦ بت و بالتالي فإن العدد الأقصى للعناوين التي يمكن استخدامها للأجهزة هو ١٦٨٢ – ٢ = ٦٥،٥٣٤ حيث استثنينا عنوانين (الكل ٠ و الكل ٢٥٥).

و تكون عناوين IP التي يمكن منحها للأجهزة هي كل العناوين بدءا من ١٧٢,١٦,٠,١ و انتهاء ب ١٧٢,١٦,٢٥٥,٢٥٤.

عـنــاويــن الــمــدى C:

في المدى Class C يتم تعيين البايتات الثلاثة الأولى لعنوان الشبكة بينما يتوفر البايت الأخير لعناوين الأجهزة على الشكل التالي:

Network.Network.Network.node ، على سبيل المثال فإن في عنوان IP التالي: ١٩٢,١٦٨,١٠٠,١٠٢ ، يعتبر ١٩٢,١٦٨,١٠٠ هو عنوان الشبكة ، بينما يعتبر ١٠٢ هو عنوان الجهاز.

العدد الأقصى لعناوين الشبكات التي يمكن الحصول عليه في المدى C هو ٢١٨٢=٢،٠٩٧،١٥٢ ، لأننا ذكرنا أنه يخصص ٣ بايتات لعنوان الشبكة أي ٢٤ بت و لكننا ذكرنا أن المصممين نصوا على حجز البتات الثلاثة الأولى لتكون ١١٠ مما يترك لنا ٢١ بت لاستخدامها بدءا من ١٩٢,٠,٠,٠ و انتهاء ب ٢٢٣,٢٥٥,٢٥٥.

أما العناوين المتاحة لجزء الجهاز node من عنوان IP في Class C فهي تتكون من بايت واحد أو ٨ بت و بالتالي فإن العدد الأقصى للعناوين التي يمكن استخدامها للأجهزة هو ٨٨٢ ــ ٢ = ٢٥٤ حيث استثنينا عنوانين (الكل ٠ و الكل ٢٥٥).

** أما عن المدى D و المدى E فهما خاصين بالابحاث و الإستخدامات العسكرية. **

ثانياً : البروتوكول ICMP... Internet Control Message Protocol

وهو مسؤول عن رسائل الاخطاء التي تتعلق بتامين وصول IP ويحتوي على رسائل من اشهرها التي تاتي مع الاداة Pingوهي رسالة Echo Request و Echo Reply .

ثالثاً : البروتوكول ARP... Address Resolution Protocol

يقوم هذا البروتوكول بعمل جدا مهم وهو وصف وإرشاد خدمة IP عن العنوان الفيزيايئ للعنوان المطلوب اذ يقوم IP عند إستلام طلب الإتصال بحاسب ما مثلا X يتوجه فورا إلى خدمة ARP ويسأله عن مكان هذا العنوان على الشبكة ثم يقوم البروتوكول ARP بالبحث عن العنوان في ذاكرته فإذا وجده قدم خريطة دقيقة للعنوان و إذا كان العنوان لحاسب

في شبكة بعيدة يقوم ARP بتوجيه IP إلى عنوان الموجه Router ثم يقوم هذا الموجه بتسليم الطلب ل ARP حتى يبحث عن العنوان الفيزيايئ لرقم ال IP .

كيف يعرف هذا البوتوكول العنوان الفيزيايئ للحواسيب ؟؟! يعرفه برقم كرت الشبكة إذ كل كرت يصنع من المصانع المختلفة يكون له رقم فريد لا يشبه رقم اخر فيحتفظ ARP بهذه الارقام في ذاكرته التي تشبه قاعدة البيانات بجميع الارقام الخاصة في محيط الشبكة ،،وهذا البروتوكول من أدوت الفحص التي تستخدم في مراقبة الشبكة وتحديد بعض المشاكل.

إنـــتـــهى بحـــمـــد الله ....