البروتوكولات

تنوية : قمت بجمع وترجمه بعض مما ورد في هذه المشاركة منذ فترة طويلة ، بعضها من مواقع عربية وأجنبية ، وبعضها من مراجع rfc المعتمدة , وقد توجد أخطاء كثيرة بالترجمة اتمنى راجيا ان يتم الإشارة إليها وتنقيحها..

3-1-بداية ما هو رقم: IP (IP Address)

-رقم , IP طوله ٣٢ بت ، ويستخدم لتعريف الجهاز في الشبكة ، وهو يشبه كثيراً رقم الهاتف ، فكل جهاز يدخل إلى الشبكة يكون له رقم منفرد لا يملكه جهاز آخر ، فلا يكون لجهازين في العالم كله الرقم نفسه في وقت واحد ، وإلا لما أمكنهما رؤية بعضهما وتبادل الاتصال فيما بينهما.

-ولا بد من الإشارة إلى أن رقم IP ينقسم إلى قسمين رقم لتحديد الشبكة ورقم لتحديد عنوان الحاسب على هذه الشبكة.

3-2-ما هو ال: DNS (Domain Name System)

-وهو عبارة عن نظام يستخدم في تحويل أرقام IP للحواسيب المضيفة على الشبكة إلى أسماء لتسهيل التعامل معها وبالعكس ، فبدلاً من حفظ أرقام IP طويلة ومعقدة للوصول إلى مضيف ما (إلى موقع على شبكة الإنترنت مثلاً) نقوم بكتابة أسماء هذه المواقع التي عادة ما تكون معبرة عن المحتوى ، مع العلم أن العمل الأصلي على الشبكة يتم كله باستخدام أرقام IP وخدمة الدومين تستخدم فقط للتسهيل على المستخدم .

-و ال DNS له عدد من النطاقات التي تعرف الفئة التي ينتمي إليها مثل : المنظمات التجارية , (.com) المنظمات غير الاقتصادية , (.org) الشبكات , (.net) المنظمات الحكومية غير العسكرية , (.gov) المنظمات العسكرية . (.mil)

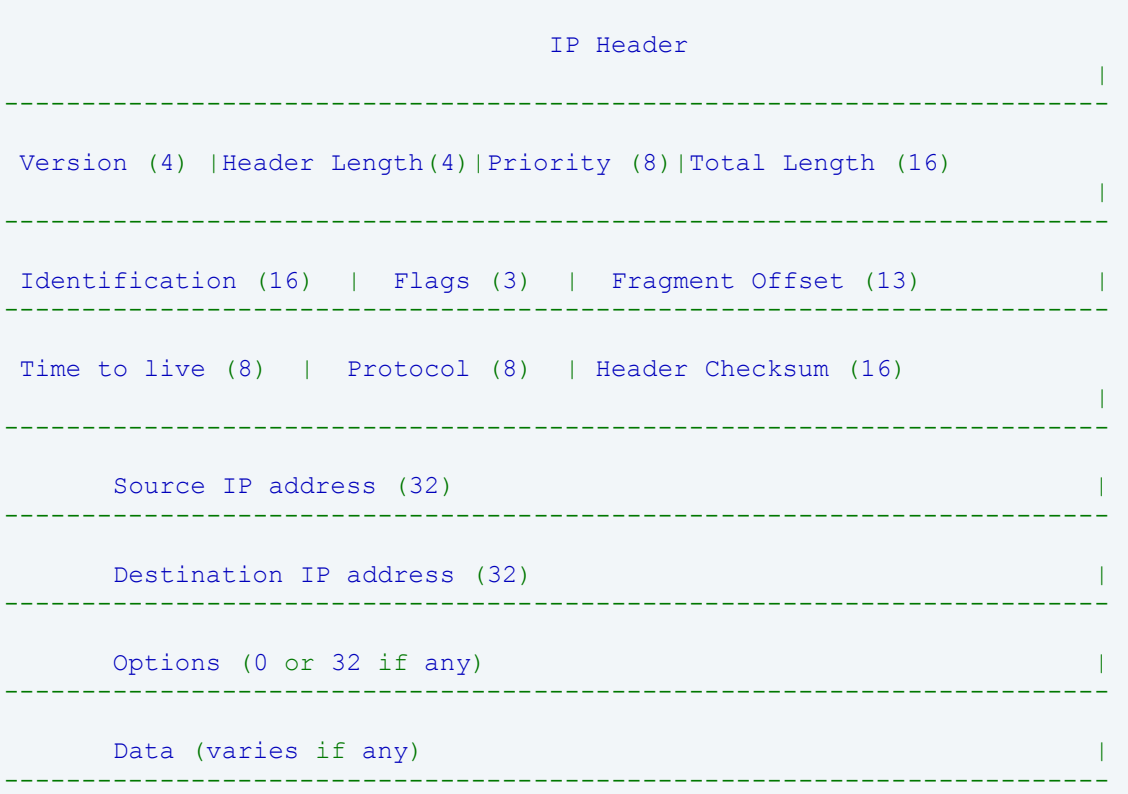
3-3-بروتوكول الإنترنت: IP (Internet Protocol)

-بروتوكول الإنترنت IP هو بروتوكول تعتمده جميع أجهزة الكمبيوتر المتصلة بالإنترنت ، وهو الذي يقوم بتجزئة الرسائل الإلكترونية إلى وحدات من البيانات (الحزم) ، كما إنه يتحكم بتوجيه البيانات (data routing) من المرسل إلى المستقبل.
-وينطوي بروتوكول الإنترنت IP تحت مجموعة بروتوكولات التحكم بالإرسال / بروتوكول الإنترنت TCP/IP (Transmission Control Protocol/Internet Protocol)و وهي مجموعة بروتوكولات طورتها وزارة الدفاع الأمريكية لإتاحة الاتصالات عبر الشبكات المختلفة الأنواع.
-ينظر بروتوكول الإنترنت IP إلى عنوان كل حزمة ، ثم باستخدام جدول يسمى جدول التوجيه يقرر من هي افضل محطة للرزمة التالية ، وكما قلنا للوصول إلى جهاز معين على الشبكة يلزمنا أمرين هما : على أي شبكة الجهاز موجود ؟ ، وما هو رقم التعريف للجهاز على الشبكة ؟ ، وهما كما ذكرنا مضمنان في رقم ال IP ,والذي يشكل العنوان الذي يتجه إليه بروتوكول. IP

-إذاً بروتوكول الإنترنت IP في الجهاز المرسل يأخذ البيانات من طبقة المضيف ومن ثم يحولها إلى مجموعة من الحزم (packets) ثم يرسلها , وبروتوكول الإنترنت IP في الجهاز المستقبل يقوم بإعادة جمع هذه الحزم وتحويلها إلى أجزاء البيانات الأصلية ، وكل حزمة من هذه الحزم تحوي عنوان بروتوكول الإنترنت IP للجهاز المرسل وللجهاز المستقبل.

-نظرة تفصيلية على بنية البروتوكول: IP

-يتألف البروتوكول IP من مجموعة من الأجزاء سنعبر عنها بالحقول التالية:



1-النسخة: Version
-و هي عبارة عن رقم بطول ٤ بت ، يحدد هذا الرقم صيغة (format) ترويسة بروتوكول الإنترنت ، أي رقم نسخة بروتوكول الإنترنت لكي يعرف المستقبل آلية التعامل معه وما هي أجزاءه وحقوله وطول كل جزء.
2-طول الترويسة: Header Length
-ويسمى , IHL (Internet Header Length) وهو بطول ٤ بت ويحدد طول ترويسة بروتوكول الإنترنت بكلمات ٣٢ بت ، وبالتالي فإنه يؤشر إلى بداية المعلومات.
3-نوع الخدمة: Type of service
-وهو بطول ٨ بت ويحدد نوع الخدمة المطلوبة ، حيث نوع الخدمة هو مجموعة من البارومترات التي توصف خيارات تزويد الخدمة في الشبكات التي تشكل الإنترنت فمثلاً يمكن أن تكون نقل معلومات تحكم إنترنت أو بيانات يرسلها المستخدمين أو معلومات توجيه ، وذلك يفيد في تحديد القيم الفعلية لمتغيرات النقل على الشبكات الفرعية ، حيث كل شبكة فرعية بما أنها تعرف نوع الخدمة المطلوبة فإنها تختار الطريقة الأكثر مناسبة لها لتوجيه ونقل البيانات عبرها.
4-الطول الكلي: Total length
-وهو بطول ١٦ بت ، ويحدد الطول الكلي للطرد ، أي طول الرزمة) الحزمة) بالإضافة إلى طول الترويسة.
5-تعريف بالهوية: Identification
-وهو بطول ١٦ بت و وهو عبارة عن قيمة محددة يرسلها المرسل للمساعدة في إعادة تجميع الطرود كما كانت ، فهي إذاً تستخدم لتمييز الطرود المختلفة عن بعضها البعض.
6-مؤشرات : Flags
-بطول ٣ بت و وهي عبارة عن مؤشرات تحكم متنوعة ، تستخدم من احل تقنية الاتصال ، فيمكن مثلاً أن تحدد فيما إذا كان الطرد المستقبل هو آخر طرد في حزمة البيانات المستقبلة أم لا .
7-إزاحة التجزئة: Frag Offset
-بطول ١٣ بت ، يقوم بعملية تجزئة أخرى إذا كان حجم الحزم المرسلة كبيراً مقارنة مع المسموح به في شبكة معينة.
8-الوقت المحدد للحياة: Time to live
-بطول ٨ بت ، كل رزمة (حزمة) تحوي عداد خاص يحدد الوقت المتبقي للحياة ، فإذا كانت الرزمة تسبح في

أثير الإنترنت لفترة طويلة وتم اجتياز الوقت المحدد للحياة دون أن تصل إلى مقصدها , فإن الرزمة توقف عملية الإرسال وتلغي نفسها. (self destruct)
-9بروتوكول Protocol
-بطول ٨ بت ، وهو يحدد بروتوكول المستوى التالي ، أي البروتوكول الذي سوف يستخدم في جزء البيانات من الطرد.
10- Header Checksum :
-بطول ١٦ بت , ويستخدم للتأكد من أن البيانات الموجودة في قسم الترويسة من الطرد قد تم نقلها بشكل صحيح ، فهو مخصص لتأكيد وصول البيانات بدون أخطاء . وهو عبارة عن عملية يتم إجرائها على البيانات وحساب نتيجتها ، وبعد إرسالها يتم إعادة حساب القيمة مرة أخرى ، فإذا تطابقت القيمتان يتم التأكد من سلامة النقل ، وعندما يفشل ال checksum في التحقق و ستكون البيانات تحوي أخطاء في النقل ، وعندها سيتم طرح الطرد المستقبل جانباً من قبل الوحدة التي اكتشفت الخطأ.
-إذاً بروتوكول الإنترنت IP لا يؤمن موثوقية في النقل لأنه عندما يكتشف خطأ ، يقوم بحذف الطرد الحاوي له دون محاولة التصحيح أو إعادة طلب البيانات مرة أخرى ، وبالتالي نحن نستطيع أن نضمن أن كل البيانات الواصلة بيانات صحيحة ، ولكن لا نستطيع أن نضمن أنها وصلت كاملة أو بالترتيب الصحيح.
-11عنوان ال IP الخاص بالمرسل: Source IP address
-وهو بطول ٣٢ بت.
-12عنوان ال IP الخاص بالمستقبل: Destination IP address
-وهو بطول ٣٢ بت أيضاً.
-13خيارات: Options
-وهو يمكن أن يأخذ الحجم ما بين ٠ حتى ٣٢ بت وقد لا يكون موجوداً ، وهذا الخيار أضيف من أجل وظائف التحكم الإضافية والنافعة في بعض الأحيان ، وهو غير ضروري من أجل معظم الاتصالات ، فهو يستعمل مثلاً من أجل أغراض الأمن والتوجيه وما شابه.
-14بيانات: Data
-وليس لها طول محدد وإنما تأخذ طول البيانات المرسلة ، وبالطبع هذا هو الجزء الأكثر أهمية ، وإيصال هذا الجزء هو هدف كل الأجزاء السابقة.

-3-4بروتوكول التحكم بالنقل: (TCP (Transmission Control Protocol

-يقدم بروتوكول TCP درجة عالية من موثوقية نقل البيانات , يقوم هذا البروتوكول بتجزئة مجموعة البيانات التي سيتم إرسالها إلى أجزاء صغيرة , ويتم ترقيم هذه الأجزاء وترتيبها بصورة مشابهة لعمل البروتوكول , IP وعندما يتم إرسال هذه الأجزاء المرقمة فإن البروتوكول TCP في الجهاز المرسل ينتظر رسالة تأكيد وصول من البروتوكول TCP في الجهاز المستقبل ، فإذا لم تصل رسالة تأكيد الوصول إلى TCP الجهاز المرسل ، فإنه يقوم بإعادة إرسال الأجزاء التي لم يتم تأكيد بوصولها.

-وقبيل بدأ عملية الإرسال ، يقوم TCP الجهاز المرسل بإرسال رسالة إلى TCP الجهاز المستقبل مستفسراً عن إمكانية إرسال الرسالة الآن ، وإن كانت الإجابة "لا , "فإن TCP المرسل ينتظر قليلاً قبل أن يرسل رسالة استفسار مرة أخرى ، وعندما تأتي رسالة الإيجاب فإنه يقوم بإرسال الأجزاء المرقمة كما ذكرنا.

-ويتفق TCP المرسل مع TCP المستقبل على كمية الأجزاء المرسلة قبل الحصول على رسالة تأكيد وصول أخرى من الجهاز المستقبل ، وفي هذه الأثناء ومع بدأ الإرسال فإن TCP المرسل يكوّن ما يسمى دائرة افتراضية (virtual circuit) مع TCP المستقبل.
-1البروتوكول TCP هو بروتوكول موثوق بدرجة عالية ، حيث يدعم TCP طرق لمعالجة الاتصال بحيث يضمن بشكل موثوق وصول الحزم إلى الهدف بشكل صحيح وبالترتيب الذي أرسلت به ، وفي حال فقدان إحدى الحزم فإن البروتوكول TCP يعاود الاتصال بالجهاز المرسل لكي يعيد إرسال الحزمة الضائعة مرة أخرى ، وبالتالي فإن هذا البروتوكول قد يسبب حملاً زائداً عند إرسال كمية كبيرة من البيانات.

-كما أن البروتوكول TCP هو بروتوكول نهاية لنهاية , أي أن المصدر سيكون جهاز واحد فقط ، والهدف أيضاً سيكون جهاز واحد . أي أن TCP موجه للاتصال بين نقطتين فقط ، وهو غير قادر على بث البيانات التي ينقلها بشكل مشاع لجميع الأجهزة الموجودة وفي وقت واحد ، بل عليه أن يعيد إرسال هذه البيانات من أجل كل جهاز على حدة ، وذلك لأن قسم الوجهة في بنية البروتوكول TCP لا يتسع إلا لوجهة واحدة فقط.

-بنية البروتوكول : TCP

-ويتألف من الحقول التالية:

```
                                                TCP Segment Format
 ---------------------------------------------------------------
          Source port (16)  |  Destination port (16)            |
 ---------------------------------------------------------------
                      Sequence number (32)                       |
 ---------------------------------------------------------------
                           Acknowledgment number (32)            |
 ---------------------------------------------------------------
    Header Length(4)| Reserved(6) |Code bits(6) |Window(16)      |
 ---------------------------------------------------------------
                         Checksum (16) | Urgent (16)            |
 ---------------------------------------------------------------
                           Options (0 or 32 if any)              |
 ---------------------------------------------------------------
                                Data (Varies)                    |
 ---------------------------------------------------------------
```

-1منفذ المصدر: Source Port
-بطول ١٦ بت ، وهو رقم المنفذ الذي يستخدمه المصدر في الإرسال.
-2منفذ المستقبل: Destination Port
-بطول ١٦ بت ، وهو رقم المنفذ الذي يستخدمه الجهاز الوجهة في الاستقبال.
-3رقم التسلسل: Sequence number
-يعطى لكل حزمة يتم نقلها رقم تسلس خاص بها لكي يتم التأكد من استقبالها بالترتيب الصحيح الذي أرسلت به ، وللتأكد من عدم وجود نسخة مضاعفة من البيانات ، كما إنه يساعد في اكتشاف البيانات المفقودة والناقصة.
-4رقم إقرار الاستلام: Acknowledgment number
-يعتمد البروتوكول TCP لجعل نقل البيانات موثوقاً على الرقمين السابقين ، رقم التسلسل ورقم إقرار الاستلام بالإضافة إلى. Checksum
-عندما يتم استقبال الحزمة بصورة صحيحة فإن هذا الحقل يحدد رقم تسلسل الحزمة التالية التي يسمح بإرسالها ، وإلا فإنه يبقي رقم الحزمة القديمة ، ويقوم بإعادة إرسالها حتى يتم التأكد من استقبالها بشكل صحيح.
-5طول الترويسة: Header Length
-بطول ٤ بت ، ويحدد طول ترويسة بروتوكول TCP بكلمات ٣٢ بت ، وبالتالي فإنه يؤشر إلى بداية المعلومات .
-6الحقل المحجوز: Reserved
-وهو حقل محجوز للاستخدامات المستقبلية وقيمته دوماً تساوي الصفر.
-7شفرة البتات: Code Bits
-خواص تحكم لبدأ ونهاية الدورة , session متعلقة بكيفية تنظيم TCP لنفسه في نقل البيانات.
-8نافذة: Window
-حجم نافذة البيانات التي يسمح للمصدر بإرسالها في وقت معين.
9- Checksum :
-وهو بطول ١٦ بت ، وكما في البروتوكول , IP فإنه يستخدم للتأكد من أن البيانات قد تم نقلها بشكل صحيح ، فهو مخصص لتأكيد وصول البيانات بدون أخطاء ، وهو كما ذكرنا سابقاً عبارة عن عملية يتم إجرائها على البيانات وحساب نتيجتها ، وبعد إرسالها يتم إعادة حساب القيمة مرة أخرى فإذا تطابقت القيمتان يتم التأكد

من سلامة النقل ، وعندما يفشل Checksum في التحقق ، فإن البيانات تحوي أخطاء في النقل ، وعندها سيتم إعادة طلب البيانات من جديد على خلاف البروتوكول IP الذي يقوم بطرحها جانباً في حال الفشل في التحقق.

-10مؤشر البيانات المستعجلة: Urgent Pointer

-يؤشر إلى نهاية البيانات المستعجلة ، أي إلى رقم التسلسل الخاص بأول حزمة غير مستعجلة بعد الحزم المستعجلة مباشرةً ، حيث تعطى الأولوية في القراءة والاستقبال لهذه الحزم.

-11خيارات: Options

-وهذا الحقل يمكن أن يأخذ الحجم من ٠ حتى ٣٢ بت وقد لا يكون موجوداً ، وممكن أن يحوي خيارات مختلفة ، فمثلاً هو الذي يحدد أعلى قيمة للجزء segment الذي يسمح باستقباله.

-12البيانات: Data

-وليس لها طول محدد ، وإنما تأخذ طول البيانات المرسلة ، وبالطبع هذا هو الجزء الأكثر أهمية ، وإيصال هذا الجزء هو هدف جميع الأجزاء السابقة.

-3-5مجموعة البروتوكول: TCP/IP

-الكلمة TCP/IP اختصار بروتوكول التحكم بالنقل / بروتوكول الإنترنت / (Transnion ControProtocol , (Internet protocolوالبروتوكول TCP/IP ليس مكون وحيد ، فهو ليس بروتوكول منفرد ولكنه يتضمن عدة بروتوكولات.

-لقد تم تطوير هذا البروتوكول من أجل الأربانت في البداية ، ولكن مع مرور الوقت وتوسع شبكة الإنترنت أصبح أحد أهم البروتوكولات المستخدمة هذه الأيام لجميع أنوع الشبكات ، ويعود ذلك إلى كون هذا البروتوكول فعال ومناسب للأسباب التالية:

-1ليس تابعاً أو مكتوباً من قبل شركة واحدة ، ولقد أقرت جمعية الإنترنت بكاملها استخدام هذا البروتوكول فهو ملك للجميع ولا يتم التحكم به من قبل مؤسسة أو جهة ما.

-2يسمح بالاتصال بين الأنظمة المختلفة.

-3الدخول إلى الإنترنت حيث يعتبر البروتوكول الرئيسي لشبكة الإنترنت.

-طبقات البروتوكول -: TCP/IP الطبقات هي عبارة عن مجموعة من البروتوكولات الموجودة في عدة مستويات ، كل طبقة تتكون من عدة بروتوكولات وتقوم بعمل محدد لخدمة الحواسيب في الشبكة وتمكينها من الاتصال عبرها , حيث أن كل طبقة تقوم بخدمة ما تقدمها للطبقة التي فوقها في حين تطلب الخدمة من الطبقة التي تحتها ، والبروتوكول TCP/IP مكون من أربع طبقات هي:

1- Application , 2- Transport , 3- Internet , 4- Network Interface .

-1يبدأ الترتيب في الطبقات من النهاية إلى البداية ، وتكون طبقة Network Interface هي أول طبقة تتعامل مع الشبكة ، إذ تتلخص مهمتها في معرفة البنية المستخدمة في الشبكة.

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

-3وطبقة Transport فهي المسؤولة عن وصول الحزم المرسلة بواسطة طبقة , Internet وتستخدم إما بروتوكول TCP أو. UDP

-4وتبقى طبقة Application هي الطبقة المسؤولة عن التأكد من أن الترميز المرسل عبر الشبكة يستخدم نفس الأبجدية ، فمعظم الحواسيب تستخدم الترميز , ASCII ولكن يوجد بعض الحواسيب التي تستخدم الترميز EBCDIC لأجهزة , IBM وأيضاً هذه الطبقة مسؤولة عن البرامج المستخدمة في التعامل عبر الشبكة مثل البريد الإلكتروني وبرامج قواعد البيانات.

-مكونات البروتوكول: TCP/IP

-1البروتوكول : TCP والذي تحدثنا عنه سابقاً.

-2البروتوكول: UDP (User Datagram Protocol)

-هذا البروتوكول من نوع , Noconnection-Based بمعنى الاتصال غير الموثق ، وهولا ينشئ جلسة عمل بين الحواسيب أثناء الاتصال ، وهو لا يضمن وصول البيانات على الحالة التي أرسلت بها ,وهو بذلك على خلاف البروتوكول , TCP ولكن هذا البروتوكول له ميزات تجعل من المستحب استخدامه في بعض الحالات مثل عندما نقوم بإرسال بيانات جماعية عامة و وعند الحاجة إلى السرعة ، وسرعته ناتجة من عدم حاجته إلى التحقق من دقة الإرسال ، ويستخدم في نقل الوسائط المتعددة مثل الصوت والفيديو لأن الوسائط لا تحتاج إلى دقة الوصول , ونستطيع أن نقول أن هذا البروتوكول ذو فاعلية كبيرة وسريع الأداء .

-ومن أهم الأسباب التي أدت إلى إنشاء البروتوكول UDP أن الإرسال عبر هذا البروتوكول لا يتطلب إلا القليل من الحمل والوقت ، إذ أن حزمة UDP لا تحتوي على كل المعطيات التي ذكرت مع بروتوكول TCP لمراقبة الإرسال ... لذلك سمي بروتوكول الاتصال غير الموثوق.

-3البرتوكول : IP وقد تحدثنا عنه سابقاً.
-4البروتوكول: ICMP (Internet Control Message protocol)
-وهو مسؤول عن رسائل الأخطاء التي تتعلق بتأمين وصول. IP
-5البروتوكول: ARP (Address Resolution protocol)
-يقوم هذا البروتوكول بعمل جداً مهم وهو وصف وإرشاد خدمة IP عن العنوان الفيزيائي للعنوان المطلوب ، إذ يقوم IP عند استلام طلب الاتصال بحاسب ما مثلاً X بالتوجه فوراً 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 ، وإذا 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 الفيزيائي لرقم ال , IP يعرف هذا البروتوكول العنوان الفيزيائي للحواسيب برقم كرت الشبكة ، إذ كل كرت بصنع في المصانع المختلفة يكون له رقم فريد لا يشبه رقم كرت آخر ، فيحتفظ ARP بهذه الأرقام في ذاكرته التي تشبه قاعدة البيانات بجميع الأرقام الخاصة في محيط الشبكة ، وهذا البروتوكول من أدوات الفحص التي تستخدم في مراقبة الشبكة وتحديد بعض المشاكل.

بروتوكول ARP
****
كما قلت في شرحي عن البروتوكلات اني ساشرح بشكل خاص عن كل بروتوكول والان سوف اشرح عن بروتوكولARP = protocol- Resolution Address
وهو لكي المعلومات تستطيع العبور بين محطتين في شبكة اتصال معينة، يجب فعل ذلك عن طريق عنوان ال IP للمحطة.
كيف يشتغل ؟
اذا مجطة تريد إرسال معلومات لمحطة ثانية (اخرى) في شبكة محلية ، في البداية هي تفحص جدول ال ARP الذي موجود في الذاكرة الموجود ، اذا عنوان ال IP المراد ليس موخود ، اليس ترسل طلبARP المحددة في عنوان "بث للكل."
في البداية محطة المراد UPDATE الجدول , عتسجل عندها عنوان ال . IP هذة العملية مهمة كثيراً لأن ان تكون هناك محطتان تبدا في نقل المعلومات في وثت قريب. الجواب التي ترسلة محطة الاصل (المراد(هي عنوان فيزيائي الخاص بها . والمحطة المرادة UPDATE جدولها . والان هي جاهزرة للإرسال إلى المحطة المرادة عتقرأ الطلب.

هذا شرح بسيط عن هذا البروتوكول بالقريب ساشرح اخرى.....

ماذا تعنى الpop3

هذا البروتوكول هو اختصار لكلمة(post office protocol)
و هنا نقول ان الكلمة هى pop فقط ولكن ال pop3 هو بمثابة اصدار اخر لهذه الخدمة
و هذا البروتوكول من بروتوكولات خدمة البريد الالكترونى ويعنى بهذا (non-web-**d) email account**

أى انه يعنى خدمة تحكم بالبريد الالكترونى بدون صفحة ويب
و لهذه الخدمة طريقتين فى التحكم الاولى هى pop والاخرى هى Smtpوهى اختصار لكلمة(send-mail-transfer protocol)

اما اللى هيكون موضوعنا الان فهو ال pop وكل شىء عنه

البعض سيقول لماذا انا اتعلم هذا البروتوكول ؟؟؟

1-أولا اقدر اقولك للأمان واعنى بالكلمة دى انك باستخدام هذا البروتوكولتستطيع تفادى شيئين وهما

"تستطيع انك تتفادى تفجير الايميل و اظن الكل يفهم ماذا اعنى بهذه الكلمة لأنى اقصد بها انك اذا فتحت فى يوم ايميلك ووجدت ٥٠٠ رسالة هتعمل ايه؟؟؟؟
اعتقد انه صعب جدا مسحهم بالرسالة وهنا نلاقى اهمية الpop

*اذا قررت انك تفتح ايميلك من اى مكان لو انك مش فى بيتك فانت هنا معرض لفتح ايميلك ورؤية اسرارك لأن بعض المتصفحات تقوم بتخزين بياناتك وممكن يفتحها احد بعدك

2-لماذا لا تتعلم من اجل التعلم وبس ؟؟؟

و للفكرة ان هذا البروتوكول سهل التعلم جدا:

الدخول على الايميل بال pop3

1-نحتاج للتل نت و مش هنغلب فيه لأنه موجود مع الويندوز و طريقة فتحه هى فتح start ثم runونكتب telnet وهو عامة بيكون على هذا المسارc:\windows\telnet

2-نحتاج للاتصال بالبريد الالكترونى وهنختار remote system من قائمة connect وبعدها نكتب فى خانة ال host name ملقم البريد الالكترونى بتاعنا وفى الغالب بيكون mail.yoursite.comو ده مع اغلب الايميلات

3-الاتصال بيكون عن طريق البورت ١١٠ وهو الخاص بهذا البروتوكول

4-أول لما ندخل هتجينا رسالة ترحيبية وبعدها هنحط اليوزر نيم والباس وورد وهتكون user: your user name
Pass: your password
وطريقة وضعهم بانك تكتب اولاuser your username
ستظهر لك رسالة وبعدها تضع الباس وورد كالتالىpass your password
مع التغيير فيهم طبعا

*بعدها بندخل على الايميل وبتجينا رسالة ومعها عدد الرسائل الموجودة فى صندوق البريد و اذا حبينا اننا نعرضهم فهنستخدم الامر ده list >====

"وهنا هيعرضلنا الرسايل الموجودة فى الصندوق و عدد الرسائل الجديدة

*لما نفتح رسالة هنفتحها بالامر ده retr# >====== ثم رقم الرسالة

*لو حبينا نلغى رسالة فهنلغيها بالامر ده #dele <===== ثم ايضا رقم الرسالة

*و نستخدم الامر quit للخروج

Dynamic Host Configuration Protocol)

أخواني الأعزاء، بإذن الله سأقوم هنا بشرح مختصر

لل DHCP-حيث سيشتمل الشرح على أفكار عامة دون التطرق للتفاصيل بشكل دقيق،

[color=#CC6600]ماهو ال DHCP-؟[/color]
==========

هو عبارة عن بروتوكول إعدادات المضيف الديناميكي (Dynamic Host Configuration Protocol).

http://absba7.absba.org/teamwork8/416924/1.jpg

ما المقصود بهذا ؟

المقصود بهذا هو أن هذا البروتكول هو المسؤول عن الخدمة التي تقوم بتعيين إعدادت الجهاز الضيف في الشبكة بشكل ديناميكي دون تدخل الأدمن.

خدمةDHCP ، ولكننا نسمع عن خادم DHCP ؟
نعم، هناك الخدمة وهناك الخادم، فيمكنك أن تقوم بإعداد سيرفر ليعمل كسيرفر رئيسي(يحتوي Active Directory في ويندوز ٢٠٠٠ أو ٢٠٠٣ (وتقوم بتفعيل هذه الخدمة عليه ويمكنك أن تجعل السيرفر ليعمل فقط كخادم DHCP أي أن يكون عضو في الدومين ولكنه عندها لا يحتوي على.Active Directory

سأفترض في باقي الحديث أننا نتكلم عنDHCP Server

http://absba7.absba.org/teamwork8/416924/6.gif

كيف يتم تجهيز الجهاز ليكونDHCP Server ؟
نقوم في الويندوز بتركيب خدمة ال DHCPوهذا هو، ولكن قبل أن يمون الجهاز حاهزا ليعمل كسيرفر يجب أن نقوم بإعطاءه السلطة (Authorization)لتوزيه ال IP's-عالعالم فيكون بذلك مخولا من ال Active Directory-لإعطاء ال.IP's-

أوكي، متى يحدث تعيين الإعدادت للأجهزة المضيفة، وكيف؟
عند بدء تشغيل الجهاز المضيف أو عند تشغيل بروتوكول ال TCP/IPفإن الجهاز يتصل باجهاز الرئيسي(سأشرح إنشاء الله كيفية الإتصال لاحقا) ويطلب منه ال IPفيقوم الخادم بإعطاء ال IP-وباقي الإعدادت للجهاز المضيف (الزبون.(

ما هي هذه الإعدادات؟

هناك نوعان من الإعدادت التي يقوم هذا:
النوع الأول: الإعدادت الإجبارية وهي ال IP-والSubnet Mask-
النوع الثاني: الإعددات الإختيارية وهي عنوان ال DNS server-و عنوان ال WINS server-وعنوان

المخرج الإفتراضي.**(Default gateway)**

http://absba7.absba.org/teamwork8/416924/2.png

كيفية طلب الإعدادات من السيرفر؟
عند بدء تشغيل الجهاز يقوم بإرسال رسالة طلب (Request) من السيرفر للحصول علىIP ، عندما يستقبل السيرفر هذه الرسالة فإنه يقوم بإرسال رسالة عرض (Offer) للجهاز يعرض عليه IP معين فيرسل له الجهاز رسالة تعلمه بانه قبل العرض (Accept) فيقوم السيرفر بدوره بإرسال رسالة إعلام بأنه قد سجل ال IP-له .(Aknowledgment)وتسمى هذه العملية بعملية التأجير.Lease

طيب بعد كل هاشغل، إذا كان السيرفر معطل، ماذا يحدث ؟
يتم تعيين IP من المدى{169.254.0.0 - 169.254.255.255}

http://absba7.absba.org/teamwork8/416924/3.gif

ماذا لو تغيرت الإعدادت في السيرفر بعد أن قام الزبون بأخذ الإعدادت؟
هناك عملية تدعى بعملية تجديد الإيجار (Lease Renewal) حيث يقوم الزبون بطلي تجديد للإعدادت كل فترة معينة وبهذا يكون up2date دائما (في الوضع الطبيعي.(

لماذا وضعت بين قوسين) في الوضع الطبيعي)، ما المقصود؟
لأنه يمكن لسبب ما(تم تعيين مدة الإيجار لوقت لا محدود مثلا) أن لا يقوم الزبون بطلب تجديد الإيجار بشكل أوتوماتيكي، وعندها يجب التجديد يدويا باستعمال الأمر:
ipconfig /renew
بالمناسبة: هناك فرق بين ipconfig/renew وهي طلب تجديد الإيجار و ipconfig/release وهي إطلاق سراح ال.IP-

هل تعني أن هذه الخدمة تغنينا عن تعيين العناوين بشكل يدوي؟
نظريا نعم ولكن هناك بعض الأجهزة التي يجب أن نعطيها IP بشكل يدوي حتى تعمل باقي الشبكة مثل السيرفر الرئيسي وال DHCP-و ال DNS-والراوترز...الخ.

ولكن ما هي عناوين ال IP-التي سيحصل عليها الزبائن؟
يجب أن نقوم بإعداد مدى من عناوين ال IP-التي نريد إعطاءها للأجهزة كأن يكون مثلا المدى:١٩٢,١٦٨,٥,٠ - ١٩٢,١٦٨,٥,٢٥٥ ومن ثم نقوم بإنشاء شئ يدعى scope ونضع في إعدادته هذه المدى، وبهذا فإن الزبون سيحصل على عنوان من ضمن هذا المدى ولكن قبل لكي يتم تنشيط هذا ال Scope-يجب أن نقوم بعمل Activation له.

http://absba7.absba.org/teamwork8/416924/4.bmp

ذكرت سابقا أنه يجب إعطاء بعض الأجهزة العناوين بشكل يدوي، ويجب أن تكون هذه العناوين من نفس المدى، ألن يحدث هذا تعارضا في تأجير العناوين؟
نعم هذا سيحدث تعارضا، ولذلك فإنه في إعدادت ال scopeيجب أن أقوم باستثناء مدى معين من العناوين وتسمى (Excluded adresses)بحيث لا يقوم السيرفر بتأجير هذه العناوين لأي من الأجهزة التي تطلب وأقوم انا يدويا بتعيين الأرقام التي أريدها من هذا المدى.

ما هو العنوان المحجوز(Reserved IP) ؟

هو عنوان أقوم بحجزه لجهاز معين دائما، وعند طلب هذا الجهاز من السيرفر IP فإن السيرفر يقوم بشكل دائم بتعيين هذا ال IP-لهذا الجهاز(Associate the IP with the MAC address).

http://absba7.absba.org/teamwork8/416924/5.jpg

Superscope
هو عبارة عن ٢ scope أو أكثر تم دمجهما ليكونا شبكة واحدة فمثلا يمكن أن ندمج الشبكتين 192.168.15.0 و الشبكة ١٩٢,١٦٨,٤,٠ فيكونا شبكة واحدة ، أي أنه يتم تعيين العناوين للأجهزة من أي من الشبكتين.