مجلة جامعة تشرين للدراسات والبحوث العلمية _ سلسلة العلوم الهندسية المجلد (29) العدد (3) 2007
Tishreen University Journal for Studies and Scientific Research- Engineering Sciences Series Vol. (29) No. (3) 2007

تأثير بروتوكول تحليل العناوين ARP في شبكات الإثرنت

الدكتور حسن عباس *
الدكتور هيثم الرضوان**
مسعود علي***

(تاريخ الإيداع 26 / 6 / 2007. قُبِل للنشر في 2007/9/6)

□ الملخّص □

في هذا البحث سنوضح مفهوم وماهية بروتوكول تحليل العناوين ARP وسنستعرض دراسة وتحليل سلوك هذا البروتوكول ARP في شبكات الاثرنت، موضحين تأثير هذا البروتوكول في الشبكات، والعوامل التي تؤدي إلى ازدياده بشكل كبير فوق الحدود الطبيعية، وانعكاساتها السلبية على الشبكة، مع تبيان تأثير الحركة الناتجة عن البث العام Broadcast Traffic على أداء الشبكة، وسوف نقارنها مع قياسات حصلنا عليها من شبكة الجامعة.

الكلمات المفتاحية: بروتوكول تحليل العناوين ARP، البث العام، جدول ARP، عنوان الـ MAC، الإطار، زمن التلاشي، دودة الانترنيت.

* أستاذ مساعد في قسم هندسة الاتصالات – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين – اللاذقية – سورية.
** أستاذ مساعد في قسم هندسة الاتصالات – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين – اللاذقية – سورية.
*** طالب دراسات عليا في قسم هندسة الاتصالات – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين – اللاذقية – سورية.

مجلة جامعة تشرين للدراسات والبحوث العلمية _ سلسلة العلوم الهندسية المجلد (29) العدد (3) 2007
Tishreen University Journal for Studies and Scientific Research- Engineering Sciences Series Vol. (29) No. (3) 2007

The Effects of Address Resolution Protocol (ARP) in Ethernet Networks

Dr. Hassan Abbas*

Dr. Haytham Al-Radwan**

Masoud Ali ***

(Received 26 / 6 / 2007. Accepted 6/9/2007)

□ ABSTRACT □

The study demonstrates the ARP (Address Resolution Protocol) working principals and the behavior and analyses ARP broadcast in Ethernet networks.

The study shows the causes and factors for excessive ARP broadcast requests above normal levels, as well as the effect of this broadcast on network performance. These are compared with theoretical and experimental results at the university network.

Key words: ARP (Address Resolution Protocol), broadcast, ARP table, MAC address, frame, Timeout, Internet worm.

*Associate professor, Department of Communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.

**Associate professor, Department of Communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.

***Master Student, Department of Communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.

مقدمة:

تعتبر شبكة الإثرنت من أكثر الشبكات المحلية نجاحاً والمستخدمة بشكل واسع في العديد من المجالات العلمية والإدارية والاقتصادية.

حيث يوجد عدد كبير من الشبكات المحلية والمتوسطة التي تعتمد كثيراً على الإثرنت، والسبب الهام لهذا الانتشار والاستخدام الواسع هو الطريقة البسيطة نسبياً في تشكيل واستخدام هذا النوع من الشبكات، كما أصبح تنفيذ الشبكات المحلية والمتوسطة ذات النطاق الواسع التي تعتمد على تقنية التبديل اعتمادا على عنوان MAC مسألة هامة يزداد الإقبال عليها.

إن الوظيفة الأساسية في الشبكة المحلية تكمن في استخلاص ومعرفة عنوان طبقة الربط MAC المرتبط بعنوان طبقة الشبكة IP، حيث يستخدم بروتوكول تحليل العناوينARP في شبكات الإثرنت في بداية الاتصال ليكتشف العنوان MAC ذو الـ 48 خانة للجهاز المراد الاتصال معه ويرتبط عنوان MAC مع العنوان IPv4 المعطى ذي الـ 32 خانة **[1]**. أي أن وظائف البروتوكول تتم ببث رسائل طلبات التحليل بثاً عاماً إلى جميع الأجهزة (الـ hosts) في الشبكة المحلية ويجاوب الجهاز الهدف فقط برسالة موجّهة إلى المصدر.

أهمية البحث وأهدافه:

تتجلى أهمية البحث في دراسة وتحليل سلوك بروتوكول الـ ARP– بروتوكول تحليل العناوين، حيث يقوم هذا البروتوكول بتحديد عنوان MAC للجهاز الهدف المعروف عنوان IP له من خلال عملية البث العام (Broadcast) في الشبكة، والذي بدوره يسبب في كثير من الأحيان مشاكلاً تحد من أداء الشبكة ويسيطر على أدائها. وسوف نعرض أهم أسباب ازدياد ARP عن المستوى العادي، وانعكاساتها على أداء الشبكة.

علما أننا سنقوم بتحليل بعض القياسات التي حصلنا عليها من شبكة الجامعة. وسنبين دور ARP في مجمل الحركة ضمن هذه الشبكة، مع اقتراح الحلول المناسبة.

طريقة البحث ومواده:

يتضمن هذا البحث عرضاً عاماً لمفهوم بروتوكول ARP، ومبدأ عمله وتأثيره على أداء الشبكة من خلال اعتماده على مبدأ البث العام، الذي يسبب في حالات ازدياده فوق الحدود الطبيعية إلى حجز معظم سعة الشبكة من أجل هذا البث، وسنبين ونحلل أهم أسباب هذا السلوك غير الطبيعي لـ ARP الذي يظهر في بعض الحالات على شكل قفزات مفاجئة في التحليل البياني، مع استعراض نتائج قياساتنا على شبكةالجامعة.

1. بروتوكول تحليل العناوين:

1-1. ماهية البروتوكول ARP

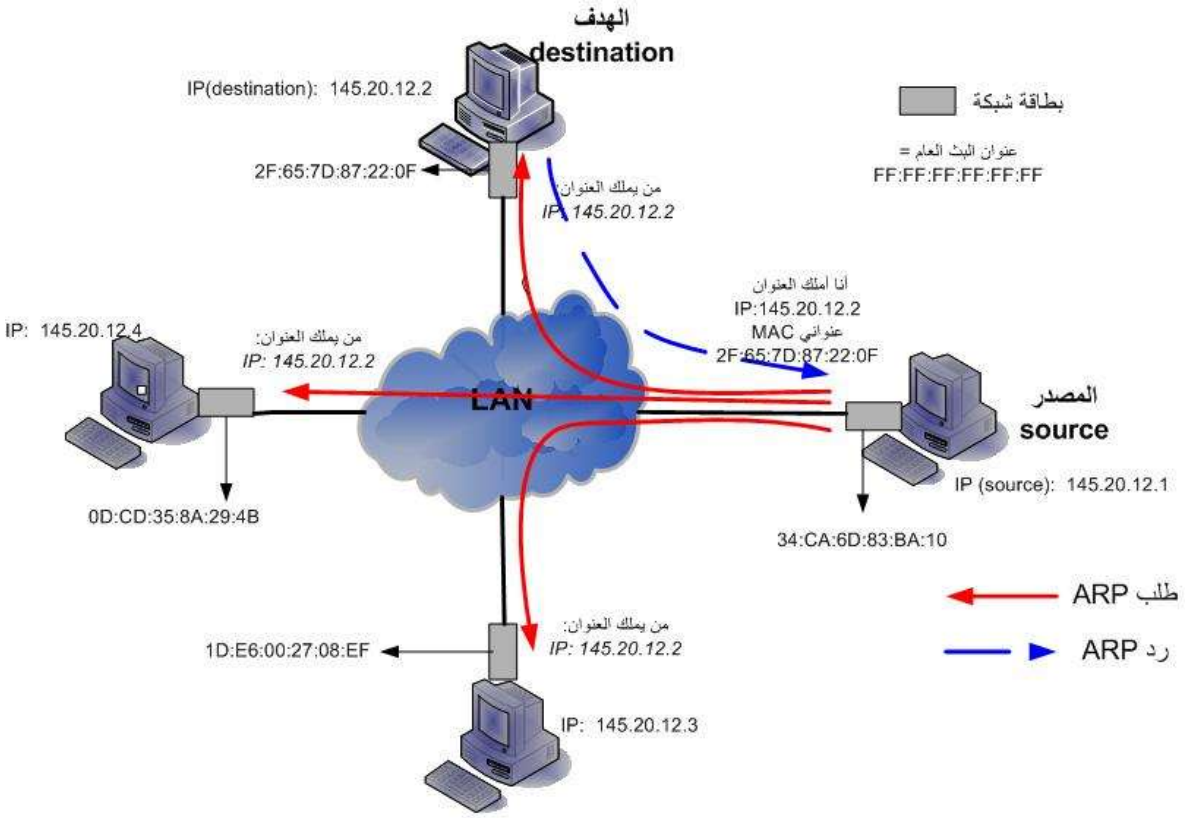
يحتاج أيُّ جهاز موجود على شبكة محلِّية كي يوصِّل رزمة IP بأمان إلى جهاز آخر أن يؤطِّر هذه الرزمة (أي يضعها ضمن إطار) ويرسلها إلى بطاقة الشبكة (NIC) الصحيحة للجهاز الهدف، ويستطيع أيُّ جهاز موجود على الشبكة بواسطة بروتوكول تحليل العناوين ARP أن يكتشف العنوان الفيزيائي MAC المرتبط مع عنوان IPv4 للجهاز

الآخر الموجود على الشبكة المحلية أو على شبكات أخرى مجاورة مرتبط معها، فعندما يحتاج الجهاز المصدر source مخطط عنونة للعنوان $IP_{destination}$ للجهاز الهدف destination، فإن هذا الجهاز ببساطة يبثُّ (بثاً عاماً) رسالة طلب (ARP request message) سائلاً جميع الأجهزة على الشبكة أنَّ على الجهاز الذي يملك عنوان $IP_{destination}$ أن يُخبر الـ IP_{source} كما هو موضح في الشكل (1-1).

تصِل هذه الرسالة إلى جميع الأجهزة على الشبكة المحلية بما فيها الجهاز الهدف destination، وعند استلامه للطلب فإنه سيرسل جواباً (unique reply) بأنَّ عنوان الـ $IP_{destination}$ موجود لديه وأنَّ عنوانه الفيزيائي هو $MAC_{destination}$، وهذا الرد هو بث أحادي بين جهازي الهدف والمصدر على خلاف الطلب الذي هو عبارة عن بث عام **[2]**.

وللتقليل قدر الإمكان من إرسال طلبات ARP، فإنَّ كل جهاز يحافظ على جدول بروتوكول تحليل عناوين (ARP table) حيث يتم تخزين مخطَّطات العنوان (address mapping) على شكل أزواج (IP_N, MAC_N) حيثN: أي جهاز موجود على الشبكة، وهذه العناوين تمَّ الحصول عليها من طلبات تحليل عناوين سابقة. قبل إرسال طلب ARP مُستهدفاً جهازاً ما (Node)، فإن الجهاز يتفحص عن العنوان IP_{Node} ضمن المدخلات السابقة في جدول ARP. ولمَّا كانت الأجهزة تُرسل عادةً دفقات من الرزم إلى أجهزة أخرى، فإنَّ ذاكرة التخزين (cache) تكفل بأن الجهاز(host) لا يكرِّر طلبات ARP لكل رزمة منفردة. ويتم إرسال طلبات تحليل العناوين ARP لعدة مرات محدَّدة قبل اعتبار أنَّ الجهاز الهدف غير موجود على الشبكة، هذا ويستغل الجهاز الهدف طلب ARP الموجه إليه من قبل المصدر ليخزِّن مخطط العنوان (IP_{source}, MAC_{source}) في جدولARP الخاص به. وبذلك لا تعود الأجهزة الهدف بحاجة لإرسال طلبات تحليل عنوان ARP فورية رداً على الطلبات الموجَّهة إليهم من المصادر **[2]**. وإنَّ المُدخلات التي هي عبارة عن أزواج (IP_N, MAC_N) إلى جدول ARP تتلاشى (تُحذَف) بعد فترة محددة من الزمن (timeout). ويتم عادة التأكد من تلاشي مدخلات ARP مباشرة باستخدام البَثِّ الأحادي unicast حيث يتم استخدام البث العام فقط في حالة عدم وجود استجابة لطلبات البث الأحادي. وإن المُدخَل يزول في حالة عدم تَلقِّي أية إجابة لطلب البث العام.

وهناك فرق بين جداول ARP وبين جداول التوجيه في الشبكات، إذ أن جداول ARP موجودة في كل أجهزة الشبكة devices سواء كانت أجهزة ربط أو أجهزة المستخدمين، فهي تحوي جداول ARP التي تحفظ ضمنها مخططات العنونة على شكل أزواج (IP, MAC). في حين أن جداول التوجيه توجد في الموجهات فقط والتي تستخدم إحدى خوارزميات التوجيه في تحديد أفضل المسارات من المصدر إلى الجهاز الهدف بالاعتماد على عدة بارامترات تتعلق بطبيعة الشبكة والخوارزمية المستخدمة.



مخطط يبين كيفية طلب طلبات ARP
وطريقة الرد على هذه الطلبات
الشكل (1-1)

1-2. ما هي الحاجة للبروتوكول ARP؟

على الرغم من أن كل جهاز له عنوان شبكة IP أو أكثر، ولكن هذه العناوين لا يمكن أن تستخدم بشكل فعلي في إرسال الرزم، لأن بطاقة الشبكة التي تعمل على طبقة الربط لا تستطيع أن تفهم عناوين الشبكة IP. في هذه الأيام معظم الأجهزة تتصل مع الشبكات المحلية عن طريق بطاقة الشبكة NIC والتي يمكنها أن تترجم العناوين MAC. فعند إرسال رزمة سنواجه عندئذ مشكلة كبيرة لأن طبقة الربط غير قادرة على تفسير عناوين الشبكة IP، وباستخدام بروتوكول ARP يمكن حل هذه المشكلة، بالإضافة لفوائد أخرى منها: مدير النظام سيكون مهتما فقط بعنوان الشبكة IP (32 bits)، وغير مكترث بعنوان MAC المعقد والمؤلف من 12 خانة بـ Hexa decimal أي 48 bits، لأن من خلال هذا البروتوكول يمكن الوصول إلى عنوان MAC بسهولة انطلاقا من عنوان IP.

1-3. بنية إطار ARP:

هناك الكثير من الصيغ المختلفة للإطارات في العديد من البروتوكولات، وإن بنية إطار ARP هي بسيطة جداً لتستخدم في أي نوع من الشبكات، كما أن التقييد الوحيد هو أن هذا البث غير مدعوم من قبل أجهزة الطبقات الأعلى مثل الموجه router. وأن بنية الإطار ARP **[3]** مبينة في الجدول (1-1) التالي:

الجدول (1-1) بنية الإطار ARP

0 8 15	16 31
Hardware Type	Protocol Type
HLEN / PLEN	Operation
Sender HA (octets 0-3)	
Sender HA (octets 4-5)	Sender IP (octets 0-1)
Sender IP (octets 2-3	Target HA (octets 0-1)
Target HA (octets 2-3)	
Target IP (octets 0-3)	

يحتوي إطار ARP الحقول التالية:

- نوع الأداة (Hardware Type): يُعرِّف نوع أداة الشبكة المستخدمة بالبداية مثل 0x0001 من أجل الإثرنت.
- نوع البروتوكول (Protocol Type): ويشير المدخل إلى هذا الحقل إلى البروتوكول الذي يستخدم عملية ARP مثل 0x0800 من أجل بروتوكول IP.
- HLEN: ويشير هذا الحقل إلى طول عنوان MAC مقدرا بـ octal، فالإثرنت تستخدم ست بايتات للعنونة.
- PLEN: هذا الحقل يوضح طول عنوان IP بـ octal أيضاً، فعلى سبيل المثال IPv4 يملك قيمة في حقل PLEN تساوي إلى 4 وفي IPv6 يملك قيمة 6.
- رمز العملية (operation): كل العمليات المعرَّفة يمكن استخدامها بوضع القيمة الموافقة في هذا الحقل، فمثلاً.

1. عند اختيار القيمة 1، يعني هذا رزمة طلب ARP
2. عند اختيار القيمة 2، يعني هذا رزمة رد ARP
3. عند اختيار القيمة 3، يعني هذا رزمة طلب RARP
4. عند اختيار القيمة 4، يعني هذا رزمة رد RARP

- العناوين (addresses): سيوضع في هذه الحقول كلا العنوانين (IP, MAC)، ويتم الحصول عليها من كلا الجهازين المصدر والهدف.

2. سلوك ARP في الشبكات:

للحصول على مفهوم واضح وللمزيد من التعمق عن سلوك ARP في الشبكات المحلية المتوسطة والكبيرة، سنوضح عمل وتأثير وسلوك ARP في الشبكات المحلية تحت ظروف العمل الطبيعية للشبكة، وسنعرض أيضا بعض الحالات الخاصة أي سلوك ARP في ظل بعض الظروف غير العادية وتحت تأثير مختلف الهجمات الفيروسية التي

يمكن أن تتعرض لها الشبكة وتؤثر على أدائها بالمجمل العام، وسوف نقارن هذه الدراسة التحليلية والتفسيرية مع تحليل لمجموعة من القياسات التي حصلنا عليها من شبكة الجامعة موضحين الجوانب الإيجابية والجوانب السلبية وكيفية تقليل هذه الآثار السلبية إلى الحدود الدنيا مع مراعاة ظروف شبكتنا المحلية من جهة التصميم والبنية التحتية والاستخدام.

إن طبيعة البث العام لطلبات ARP تشكل مجموعة من حركة ARP وهذه الحركة بالنسبة للحركة الإجمالية للشبكة غير جديرة بالاهتمام ومقبولة في الظروف الطبيعية لحركة البيانات في الشبكة ولكن في بعض الأحيان تصبح جديرة بالاهتمام لأنها تشغل معظم حركة الشبكة وتقلل من أدائها، حيث كنا قد وجدنا سابقا إن طلب ARP يكون على شكل بث عام ولكن رد الطلب يكون موجها إلى المصدر فقط أي بث أحادي (unicast)، ونتيجة لقلة أهمية دور ARP في حالة الرد بالنسبة لطلب ARP سوف نركز على طلبات البث العام ARP فقط.

3. توزع طلبات ARP:

إن أي جهاز يريد الدخول إلى الشبكة يريد التعرف على الأجهزة التي يرغب الاتصال معها سواء ضمن الشبكة المحلية أو خارجها (معرفة الـ IP, MAC) لكل من هذه الأجهزة عن طريق إرسال طلبات ARP في جميع أنحاء الشبكة، وكذلك يتم إرسال هذه الطلبات عندما يرغب أحد الأجهزة الاتصال بجهاز جديد. وضمن هذه الظروف نرى أن عدد طلبات ARP سيكون مقبولا ويتعلق بنشاط الشبكة.

ولكن الأمور لا تجري في كل الأوقات على هذا المنوال، فهناك حالات وظروف معينة تجعل سلوك ARP هذا شاذ وغير مقبول ويَستغِل جزء كبير من سعة الشبكة لصالحه على حساب حركية البيانات ضمن الشبكة، والسبب في زيادة طلبات ARP بشكل غير منطقي لبعض الفترات يعود إلى بعض الأجهزة التي تغمر الشبكة بطلبات ARP.
وهذا السلوك الشاذ لبعض الأجهزة يمكن أن يُفسَّر بعدة أشكال:

❖ الشكل الأول يعود إلى:

1) المخدِّمات التي تحتفظ بقائمة للأجهزة المتصلة معها في جدول ARP على شكل أزواج (IP, MAC) لكل جهاز متصل معها، وهذه الأجهزة تتصل مع المخدم بشكل دوري وقد يحصل بعض التأخير نتيجة تأثير الطبقات الأعلى أو نتيجة بقاء الجهاز بدون اتصال مع المخدم لفترة أكبر من زمن التلاشي (timeout)، ويعرف زمن تلاشي timeout لجدول ARP: بأنه الفترة الزمنية التي إذا لم يتم خلالها تواصل بين الجهازين المتصلين يتم حذف زوج (IP, MAC) المدخل سابقا ضمن الجدول ARP فاسحاً المجال لتخزين أزواج جديدة **[4]**.
2) ولدينا حالة ثانية وهي حالة اتصال الجهاز مع عدد من الأجهزة يزيد عددها على حجم جدول ARP عندها يبقى عدد من الأجهزة المتصلة غير موجودة في جدول ARP وبالتالي سيتم إرسال طلب ARP لهذه الأجهزة في كل مرة يتم إرسال رزمة إليها، وتستمر هذه العملية في التكرار لتلك الأجهزة غير المخزنة في الجدول ARP طالما أن جدول ARP لا يخزن أزواج (IP, MAC) لكامل الأجهزة المتصلة مع هذا الجهاز.

❖ الشكل الثاني:

إن سبب الازدياد الكبير في عدد طلبات ARP يتعلق بالأجهزة الماسحة للشبكة، التي تُحفِّز على إرسال طلبات ARP لكل العناوين الموجودة ضمن مجال عناوين هذه الشبكة، وتعود أسباب هذا المسح الشامل من قبل بعض الأجهزة لكامل الشبكة إلى:

1) وجود فيروسات وهي عبارة عن برمجيات من النوع الخطير، تدعى ديدان المسح (worms)، والتي تبحث عن أجهزة ضعيفة المقاومة تجاه الهجمات الفيروسية، وحتى زمن ليس بالبعيد لا توجد محاولات جادة للحد من تأثيرات ديدان المسح التي تؤثر على أداء شبكات الإثرنت.
2) عقد خارجية، مثال ذلك عندما تصدر عقدة خارجية طلب صدى ICMP للعناوين IP على الشبكة، وفي هذه الحالة فإن موجّه الشبكة هو البادئ بطلبات ARP.

من الخصائص الهامة لبث طلبات ARP لكل جهاز هو burstiness. فإذا عرّفنا معدل طلب ARP اللحظي الأعظمي لجهاز بأنه معكوس الزمن الأقصر الملاحظ بين طلبين متتاليين لذلك الجهاز، ومعدل طلب ARP الوسطي وهو العدد الكلي للطلبات مقسوما على الفترة الزمنية لهذه الطلبات، عندئذ يمكن تعريف burstiness بأنه نسبة معدل الطلب الأعظمي إلى معدل الطلب الوسطي.

في حالة العمل العادية للأجهزة، ليس من الطبيعي لأي جهاز أن يبث بشكل فعلي عددا أكبر بكثير من طلبات ARP بالنسبة للمعدل. ويمكن أن تحدث دفقات صغيرة عند إقلاع الأجهزة وعند تكرار الكشف عن العنوان.

4. مخطط الحركة لـ ARP:

إن طلبات ARP تكاد تكون موزعة بشكل متماثل بين جميع الأجهزة الموجودة على الشبكة وهذا ما يقودنا إلى السلوك الطبيعي لحركة ARP في بعض الأوقات في الشبكة، أما بالنسبة للدفقات الكبيرة لطلبات ARP في بعض الأوقات الأخرى فتعود إلى مجموعة صغيرة من الأجهزة المستهدفة بالحركة بشكل كبير من قبل مجموعة كبيرة من الأجهزة الأخرى، فالمخدمات والموجهات وبوابات العبور مستهدفة بالحركة أكثر من غيرها. وبشكل تقريبي كل جهاز موجود على الشبكة يحتاج لاتصال مع المخدم المحلي للشبكة ومع المخدمات غير المحلية الموجودة على الشبكات الأخرى وذلك عن طريق الموجهات وبوابات العبور ونتيجة لذلك ستكون هذه الأجهزة (المخدمات والموجهات وبوابات العبور) هدفا لقسم كبير من طلبات ARP. وكذلك تلاحظ بعض طلبات البث العام ARP للموجهات وبوابات العبور والتي تستهدف الأجهزة المحلية. ففي طور إقلاع بعض أجهزة الشبكة يتم بناء مخطط العنونة لها.

وبما أن الجهاز المستهدف بطلب ARP سوف يضيف زوج (IP, MAC) الخاص بالجهاز المصدر إلى جدول ARP الخاص به، ومن خلال الرد على هذا الطلب سيعلم الجهاز المصدر زوج (IP, MAC) للجهاز الهدف وبالتالي فإن طلب ARP الوحيد سيكون كافيا لتأسيس الاتصال بين جهازي الاتصال (المصدر والهدف)، وهذا يعني أن مدخلات ARP على كل من جدولي جهازي الاتصال ستحدث في نفس الوقت تقريبا، ولكن هذا الاستنتاج لا يتطابق مع كل من المخدمات والموجهات وبوابات العبور وذلك لعدة أسباب.

إن أحد أسباب العدد الكبير لطلبات البث العام ARP الصادرة عن المخدمات وبوابات العبور تعود لحقيقة أن جدول ARP على هذه الأجهزة غير كبير كفاية لاحتواء كامل مجموعة الأجهزة الفعالة على الشبكة، أي أن بعض

محتويات الجدول (بعض المدخلات) التي ما تزال تستخدم ستتم إزالتها من الجدول قبل أن يحين موعد إزالتها وذلك لإفساح المجال لمدخلات جديدة، وبعد إزالة هذه المدخلات سيتم إرسال طلبات بث ARP للعناوين التي تم حذفها حديثا حاذفة بدورها مدخلات بشكل سابق لأوانه وذلك عندما يكون جدول ARP ممتلئاً، في هذه الحالة ستنخفض فعالية جدول ARP، وسيزاد معدل طلبات ARP.

وسبب آخر لارتفاع معدل طلبات ARP الصادرة عن بوابة العبور مصدره خارجي، ويتمثل بمسح مجال العناوين المخصص للشبكة، فعندما تقوم أجهزة مصابة بديدان المسح موجودة على شبكة أولى بعملية مسح لشبكة ثانية، فإن رزم المسح سوف تدخل الشبكة الثانية من خلال بوابة العبور، عندها تحتاج هذه البوابة لمخطط العنونة الذي يحدد عنوان الـ MAC المقابل لكل من عناوين IP للشبكة الثانية، وهذا ما يدفع البوابة لتفحص جدول ARP الموجود لديها فإذا لم يكن هناك مدخلات مطابقة عندها فالبوابة تبث طلبات ARP بثاً عاماً. ولما كان الجهاز الذي يقوم بعملية المسح والموجود على الشبكة الأولى لا يعرف عناوين IP للأجهزة الموجودة على الشبكة الثانية، سيرسل عندئذ العديد من الرزم والتي تستهدف عناوين غير محدودة، وكل من هذه الرزم سيولد طلب بث ARP من قبل بوابة العبور التي تصل الشبكتين في حال عدم وجود زوج (IP, MAC) مطابق في جدول ARP لهذه البوابة.

بالإضافة إلى ذلك، بعض أنظمة التشغيل تعتمد تقنية زمن التلاشي timeout، وهكذا فهي تتأكد من صحة زمن التلاشي للمدخلات بدلا من إزالتها مباشرة وهذا يتم بشكل طلب ARP موجه من المصدر إلى الهدف مباشرة، فإذا لم يجاوب الهدف، عندها يتم بث طلب ARP إلى جميع الأجهزة، مع احتمال اكتشاف مخطط عنونة جديد خاص بعنوان الهدفIP.

ويمكن القول مما سبق: إن معظم الأجهزة لا تتصل مباشرة مع بعضها البعض في أغلب الأحيان، إذ أن معظم الاتصالات المنشأة من جهاز ما تكون متجهة إلى المخدمات المحلية الخاصة بالشبكة أو إلى المخدمات الموجودة على شبكات خارجية.

5. تأثير الأجهزة المصابة بالفيروسات والسيئة التشكيل:

تصاب بعض أجهزة الشبكة أحيانا بفيروس يدعى دودة مسح الانترنيت، وهذه الدودة بالذات تمسح جميع الشبكات الفرعية المحلية بحثا عن أجهزة ضعيفة وقابلة للإصابة وبترتيب تسلسلي، وذلك قبل إجراء مسح الأجهزة الضعيفة في الشبكات المجاورة. وبعض الديدان الأخرى ربما تستخدم مسحاً عشوائياً انتقائياً، أي أن العدوى تنتقل من الأجهزة المصابة إلى السليمة عند اتصال السليمة بتلك المصابة، وعدم وجود برمجيات حماية لهذه الأجهزة السليمة.

تجري الأجهزة المصابة بالدودة بثا عاما بطلبات ARP من خلال عملية السبر الشاملة، فتقوم الدودة لتسريع انتشارها بالبحث قدر الإمكان عن أجهزة كضحايا محتملين وبأقصر زمن، وهذا ينتج ازدياداً مفاجئاً في معدل طلبات ARP على الأجهزة المصابة، وازدياداً في انشغال المبدلات في معالجة هذه الإطارات، الأمر الذي يقلل من أداء الشبكة من ناحية معالجة البيانات وانخفاض سعة الشبكة الخاصة للبيانات بسبب استغلاله من قبل طلبات ARP. وللحصول على تصور عن كيفية تأثير الدودة على أداء شبكات الاثرنت المحلية، فمن المفيد الحصول على معرفة كيفية انتشار هذه الدودة، وسنبين فيما يلي كيفية حساب هذا الانتشار وتقدمه **[5]**.

فالمعادلة التالية تبين انتشار ديدان المسح:

$$m_i = \sum_{j=0}^{i} n_j$$

$$s_i + 1 = \sum_{k=i-\frac{T}{s}}^{i} n_k$$

$$n_i + 1 = [N - m_i][1 - (1 - \frac{1}{T})^{rs_i+1}$$

حيث

N: يمثل العدد الإجمالي لعدد الأجهزة الضعيفة القابلة للإصابة.

T: حجم مجال العناوين من الأجهزة المستهدفة للسبر والتي تختار بشكل عشوائي.

r: معدل المسح.

n_i, s_i, m_i: تمثل عدد الأجهزة المصابة، عدد طلبات مسح الدودة، وعدد الإصابات الجديدة في الفترة الزمنية الضيقة i (time slot) على التعاقب.

ومما تقدم نرى أنه كلما زاد عدد الأجهزة القابلة للإصابة بالدودة زاد معدل الإصابة ومعدل طلبات ARP.

وبسبب ازدياد عدد طلبات ARP الذي يؤدي بدوره إلى ازدياد عدد الإطارات التي تعبر المبدلات مسببا بطئاً في أداء المبدل وبالتالي انخفاض في أداء الشبكة، إذ إن حجم الإطار الأصغري لطلبات ARP في شبكة الاثرنيت هو 64 byte. وكلما احتاج الأمر للبث العام على هذه الشبكة ومن أجل مبدل بـ n port (منفذ) عليه أن يكرر الطلب بـ (n-1) مرة في مخارجه. ومعظم المبدلات تستخدم المسار البطيء لتوجيه البث، فعلى CPU المبدل أن ينسخ الإطار إلى جميع منافذ الخرج. وهذا يؤدي إلى تخفيض أداء معظم المبدلات بشكل كبير وملحوظ.

ففي شبكة تحوي m من الأجهزة المصابة، وكل منها يبث بمعدل r requests/second وبالتالي فإن عد الطلبات الصادرة عن مبدل بـ n منفذ تساوي إلى R:

$$R = m \times (n-1) \times r$$

فعلى سبيل المثال من أجل 30 جهاز مصاب، وكل منها يبث 40 طلباً في الثانية ومن أجل مبدل بـ 12 منفذاً عندئذ يكون عدد طلبات ARP الصادرة عن المبدل هي R:

R = 30 * 50 * 11 = 13200 requests/second.

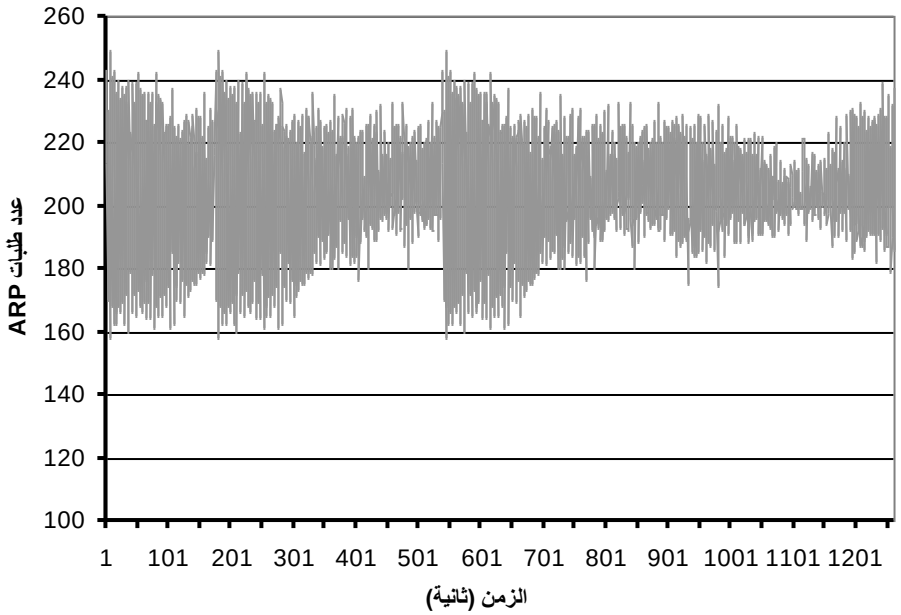
ويمكن تحديد الأجهزة المصابة من خلال مراقبة حركة طلبات ARP الصادرة عن مختلف الأجهزة، فأي ارتفاع كبير مفاجئ في طلبات ARP الصادر عن أي من الأجهزة يدل على إصابة هذا الجهاز بدودة الانترنيت، وهكذا تتميز هذه

الأجهزة المصابة عن الأجهزة غير المصابة. ويمكن أيضا تحديد الأجهزة المصابة من خلال برامج خاصة مضادة للفيروسات الشبكية.
ويعتبر القضاء على الدودة خاصاً بأمن الشبكات وخارجاً عن نطاق هذا البحث.

6. القياسات العملية:

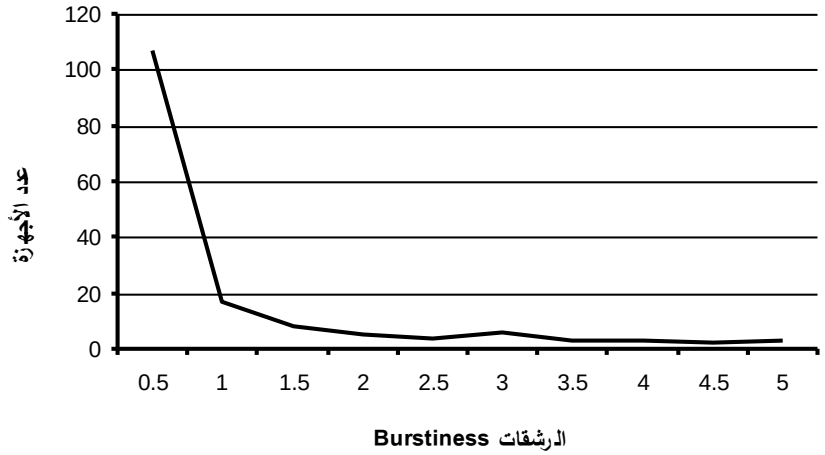
أجرينا مجموعة من القياسات على شبكة الجامعة، وشبكة الجامعة هذه عبارة عن شبكة LAN، تعمل على مستوى الطبقة الثانية Data Link Layer أي أنها تعمل على مستوى Switch، وهذه الشبكة تغطي الجامعة بالكامل بكافة كلياتها وأقسامها العلمية والإدارية، ومقسمة إلى قطاعات ترتبط فيما بينها عن طريق مبدلات الطبقة الثانية. وتمت هذه القياسات لفترة متواصلة من الزمن وأخذنا عددا كبيرا من الإطارات، وفي الملحق في نهاية المقالة عَيِّنات من هذه القياسات في فترات وفي لحظات مختلفة من زمن القياس الكلي في الملحق A، وذلك باستخدام برمجيات مايكروسوفت 2003 مع العلم أنه توجد العديد من البرمجيات التي تقوم بهذا، وذلك لتسجيل الحركة على مخدم الشبكة.

من خلال القياسات التي أجريناها على شبكة الجامعة وبعد تحليل القياسات الناتجة وجدنا أنه في الشكل (6–1) الذي يبين عدد طلبات ARP التي تبثها الأجهزة خلال كل ثانية وكما نرى من خلال الشكل أنه لدينا قفزات في عدد الطلبات الذي يعود إلى السلوك الشاذ لبعض الأجهزة،



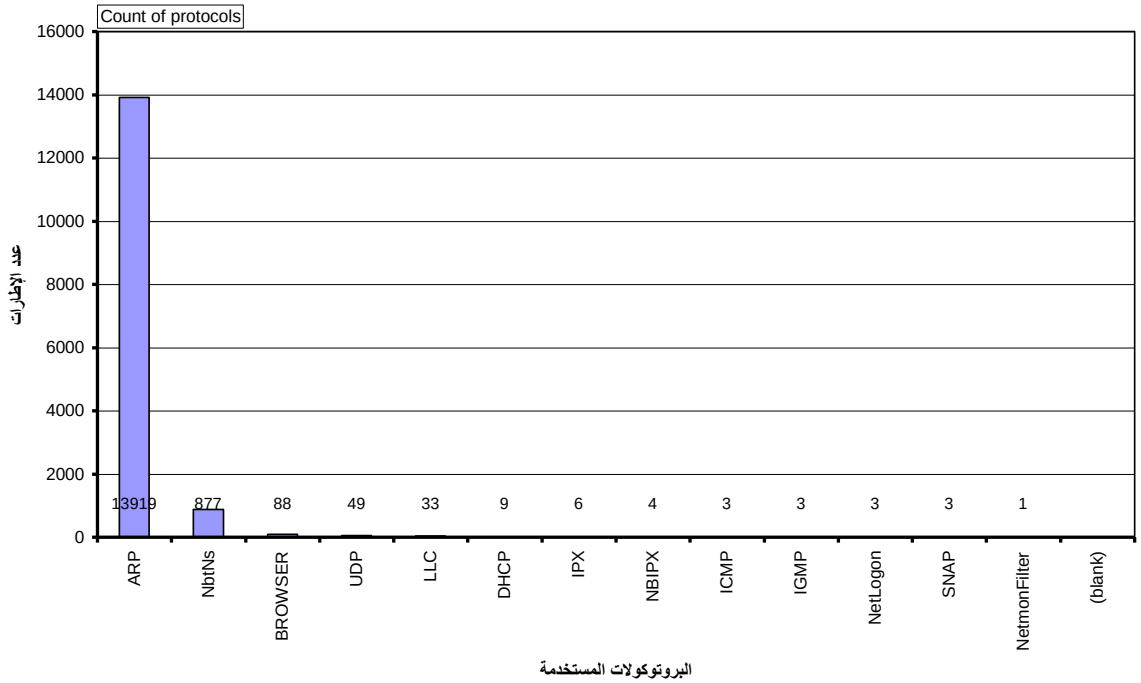
الشكل (6-1) عدد طلبات ARP التي تبثها الأجهزة في كل ثانية

أما الشكل (6–2) الذي يبين عدد الأجهزة مع معدل Burstiness الموافقة لها، ومن خلال هذا الشكل نلاحظ أن الأجهزة التي لها Burstiness صغير يكون عددها كبيراً، أما الأجهزة التي يكون Burstiness لها كبيراً فعددها صغير وهذا ما يتوافق مع ما شُرِح أعلاه من أن عدداً صغيراً من الأجهزة هي التي تبث طلبات ARP بشكل كبير.



الشكل (6-2) العلاقة بين عدد الاجهزة وعدد Burstiness

الشكل (6-3) الذي يبين عدد الإطارات الخاصة بكل نوع من البروتوكولات خلال فترة زمنية معينة، بالاعتماد على الجدول (6-1). وقد وجدنا في الفترة التي تم أخذ القياسات فيها أن طلبات ARP هو المسيطر على أداء الشبكة.



الشكل (6-3) عدد الإطارات الخاصة بكل بروتوكول

الجدول (6 -1) يبين عدد الإطارات الخاصة بكل بروتوكول

Protocol Name	Total
ARP	13919
NbtNs	877
BROWSER	88
UDP	49
LLC	33

DHCP	9
IPX	6
NBIPX	4
ICMP	3
IGMP	3
NetLogon	3
SNAP	3
NetmonFilter	1
(blank)	
Grand Total	14998

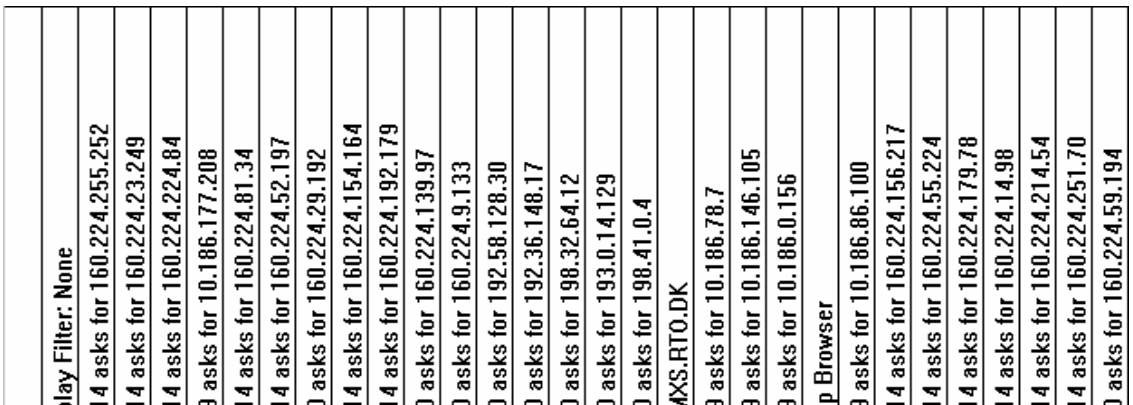
7. المقترحات:

لقد بينت القياسات العملية التي أجريناها على شبكة الجامعة في أوقات مختلفة أن الشبكة تعاني كثيرا من التأثير السلبي لبث طلبات ARP على أداء الشبكة حيث إن هذه الطلبات تتم بمعدلات أكبر بكثيرمن المعدلات الطبيعية، فيتم استهلاك معظم سعة الشبكة من قبل هذه الطلبات التي هي على شكل بث عام وذلك كله على حساب حركة البيانات في الشبكة وبالتالي على حساب أداء الشبكة، وبنتيجة تأثيرها السلبي يجب التقليل قدر الإمكان منها وذلك عن طريق تغييرات جوهرية في الشبكة من خلال:

1. إعادة تشكيل الشبكة بحيث يتم تجزئتها إلى أجزاء مختلفة لحصر طلبات ARP قدر الإمكان بحيث يتم إدخال Hardware و Software جديدين يعملان على الطبقة الثالثة Router or layer 3 switch.
2. التقليل قدر الإمكان من الانقطاعات في الشبكة والتي تنتج من خلال:
Hardware, Software and power faults لتجنب إعادة إرسال طلبات ARP بين الأجهزة المتصلة بعد كل انقطاع في الشبكة.
3. اختيار مخدمات وRouters لها مقدرات معالجة وتخزين كبيرة.
4. تحديد الأجهزة المصابة بدودة الانترنيت على الشبكة وعزلها وتنظيفها من هذه الدودة وبقية الفيروسات المسببة لارتفاع معدلات طلبات ARP.
5. استخدام الـ Domain Controllers.

جدول القياسات على شبكة الجامعة

الملحق (A)



Frame	Time	ConvID	Source	Dest	Protocol	Description
60001	272.586914	{ARP:28726}	160.224.25.14	160.224.158.199	ARP	ARP: Request, 160.224.25.14 asks for 160.224.158.199
60002	272.596679	{ARP:28274}	160.224.25.175	160.224.25.217	ARP	ARP: Request, 160.224.25.175 asks for 160.224.25.217
60003	272.597656	{ARP:28727}	160.224.25.14	160.224.23.190	ARP	ARP: Request, 160.224.25.14 asks for 160.224.23.190
60004	272.599609	{ARP:28728}	160.224.25.14	160.224.49.185	ARP	ARP: Request, 160.224.25.14 asks for 160.224.49.185
60005	272.605468	{ARP:28729}	10.186.44.99	10.186.97.165	ARP	ARP: Request, 10.186.44.99 asks for 10.186.97.165
60006	272.624023	{ARP:28730}	10.186.44.99	10.186.175.128	ARP	ARP: Request, 10.186.44.99 asks for 10.186.175.128
60007	272.637695	{ARP:28731}	10.186.44.99	10.186.67.216	ARP	ARP: Request, 10.186.44.99 asks for 10.186.67.216
60008	272.637695	{ARP:28732}	10.186.44.99	10.186.120.189	ARP	ARP: Request, 10.186.44.99 asks for 10.186.120.189
60009	272.638672	{ARP:28733}	10.186.44.99	10.186.46.205	ARP	ARP: Request, 10.186.44.99 asks for 10.186.46.205
60010	272.638672	{ARP:28734}	10.186.44.99	10.186.140.203	ARP	ARP: Request, 10.186.44.99 asks for 10.186.140.203
60011	272.652343	{ARP:28423}	160.224.25.14	160.224.49.168	ARP	ARP: Request, 160.224.25.14 asks for 160.224.49.168
60012	272.652343	{ARP:28409}	160.224.25.14	160.224.92.81	ARP	ARP: Request, 160.224.25.14 asks for 160.224.92.81
60013	272.652343	{ARP:28426}	160.224.25.14	160.224.210.68	ARP	ARP: Request, 160.224.25.14 asks for 160.224.210.68
60014	272.65625	{ARP:28411}	10.186.11.20	160.224.181.160	ARP	ARP: Request, 10.186.11.20 asks for 160.224.181.160
60015	272.65625	{ARP:28412}	10.186.11.20	160.224.138.45	ARP	ARP: Request, 10.186.11.20 asks for 160.224.138.45
60016	272.65625	{ARP:28413}	10.186.11.20	160.224.138.120	ARP	ARP: Request, 10.186.11.20 asks for 160.224.138.120
60017	272.65625	{ARP:28414}	10.186.11.20	160.224.199.227	ARP	ARP: Request, 10.186.11.20 asks for 160.224.199.227
60018	272.65625	{ARP:28415}	10.186.11.20	160.224.125.11	ARP	ARP: Request, 10.186.11.20 asks for 160.224.125.11
60019	272.65625	{ARP:28416}	10.186.11.20	160.224.67.248	ARP	ARP: Request, 10.186.11.20 asks for 160.224.67.248
60020	272.65625	{ARP:28417}	10.186.11.20	160.224.133.252	ARP	ARP: Request, 10.186.11.20 asks for 160.224.133.252
60021	272.65625	{ARP:28419}	10.186.11.20	160.224.9.39	ARP	ARP: Request, 10.186.11.20 asks for 160.224.9.39
60022	272.65625	{ARP:28410}	10.186.44.99	10.186.57.23	ARP	ARP: Request, 10.186.44.99 asks for 10.186.57.23
60023	272.65625	{ARP:28420}	10.186.11.20	160.224.236.216	ARP	ARP: Request, 10.186.11.20 asks for 160.224.236.216
60024	272.65625	{ARP:28418}	10.186.44.99	10.186.199.133	ARP	ARP: Request, 10.186.44.99 asks for 10.186.199.133
60025	272.65625	{ARP:26406}	10.186.11.20	160.224.122.6	ARP	ARP: Request, 10.186.11.20 asks for 160.224.122.6
60026	272.65625	{ARP:28424}	10.186.44.99	10.186.57.43	ARP	ARP: Request, 10.186.44.99 asks for 10.186.57.43
60027	272.65625	{ARP:28421}	10.186.11.20	160.224.95.170	ARP	ARP: Request, 10.186.11.20 asks for 160.224.95.170
60028	272.65625	{ARP:28422}	10.186.11.20	160.224.30.41	ARP	ARP: Request, 10.186.11.20 asks for 160.224.30.41
60029	272.722656	{ARP:28735}	10.186.44.99	10.186.232.28	ARP	ARP: Request, 10.186.44.99 asks for 10.186.232.28
60030	272.722656	{ARP:28736}	160.224.25.14	160.224.45.114	ARP	ARP: Request, 160.224.25.14 asks for 160.224.45.114

Frame	Time	ConvID	Source	Dest	Protocol N	Description
120001	548.347656	{ARP:56822}	10.186.11.20	160.224.207.103	ARP	ARP: Request, 10.186.11.20 asks for 160.224.207.103
120002	548.347656	{ARP:56823}	10.186.11.20	160.224.105.202	ARP	ARP: Request, 10.186.11.20 asks for 160.224.105.202
120003	548.347656	{ARP:56824}	10.186.11.20	160.224.92.42	ARP	ARP: Request, 10.186.11.20 asks for 160.224.92.42
120004	548.347656	{ARP:56825}	10.186.11.20	160.224.37.48	ARP	ARP: Request, 10.186.11.20 asks for 160.224.37.48
120005	548.347656	{ARP:56827}	10.186.11.20	160.224.62.164	ARP	ARP: Request, 10.186.11.20 asks for 160.224.62.164
120006	548.347656	{ARP:56828}	10.186.11.20	160.224.97.120	ARP	ARP: Request, 10.186.11.20 asks for 160.224.97.120
120007	548.347656	{ARP:56829}	10.186.11.20	160.224.234.219	ARP	ARP: Request, 10.186.11.20 asks for 160.224.234.219
120008	548.347656	{ARP:56830}	10.186.11.20	160.224.13.131	ARP	ARP: Request, 10.186.11.20 asks for 160.224.13.131
120009	548.347656	{ARP:56831}	10.186.11.20	160.224.52.227	ARP	ARP: Request, 10.186.11.20 asks for 160.224.52.227
120010	548.353515	{ARP:56821}	10.186.44.99	10.186.140.25	ARP	ARP: Request, 10.186.44.99 asks for 10.186.140.25
120011	548.353515	{ARP:56826}	10.186.44.99	10.186.103.71	ARP	ARP: Request, 10.186.44.99 asks for 10.186.103.71
120012	548.365234	{ARP:57194}	10.186.44.99	10.186.27.97	ARP	ARP: Request, 10.186.44.99 asks for 10.186.27.97
120013	548.371093	{ARP:57195}	10.186.44.99	10.186.191.58	ARP	ARP: Request, 10.186.44.99 asks for 10.186.191.58
120014	548.37207	{ARP:57196}	10.186.44.99	10.186.133.183	ARP	ARP: Request, 10.186.44.99 asks for 10.186.133.183
120015	548.375976	{ARP:57197}	10.186.44.99	10.186.116.130	ARP	ARP: Request, 10.186.44.99 asks for 10.186.116.130
120016	548.384765	{ARP:57198}	10.186.44.99	10.186.195.6	ARP	ARP: Request, 10.186.44.99 asks for 10.186.195.6
120017	548.388672	{ARP:57199}	10.186.44.99	10.186.93.77	ARP	ARP: Request, 10.186.44.99 asks for 10.186.93.77
120018	548.390625	{ARP:57200}	10.186.44.99	10.186.48.225	ARP	ARP: Request, 10.186.44.99 asks for 10.186.48.225
120019	548.40332	{ARP:57201}	160.224.25.14	160.224.50.223	ARP	ARP: Request, 160.224.25.14 asks for 160.224.50.223
120020	548.425781	{ARP:57202}	10.186.44.99	10.186.76.208	ARP	ARP: Request, 10.186.44.99 asks for 10.186.76.208
120021	548.427734	{ARP:57203}	10.186.44.99	10.186.44.4	ARP	ARP: Request, 10.186.44.99 asks for 10.186.44.4
120022	548.447265	{ARP:56832}	10.186.11.20	160.224.59.14	ARP	ARP: Request, 10.186.11.20 asks for 160.224.59.14
120023	548.447265	{ARP:56833}	10.186.11.20	160.224.189.195	ARP	ARP: Request, 10.186.11.20 asks for 160.224.189.195
120024	548.447265	{ARP:56834}	10.186.11.20	160.224.231.97	ARP	ARP: Request, 10.186.11.20 asks for 160.224.231.97
120025	548.447265	{ARP:56836}	10.186.11.20	160.224.181.56	ARP	ARP: Request, 10.186.11.20 asks for 160.224.181.56
120026	548.447265	{ARP:56837}	10.186.11.20	160.224.105.112	ARP	ARP: Request, 10.186.11.20 asks for 160.224.105.112
120027	548.447265	{ARP:56838}	10.186.11.20	160.224.69.203	ARP	ARP: Request, 10.186.11.20 asks for 160.224.69.203
120028	548.447265	{ARP:56839}	10.186.11.20	160.224.155.170	ARP	ARP: Request, 10.186.11.20 asks for 160.224.155.170
120029	548.447265	{ARP:56840}	10.186.11.20	160.224.97.201	ARP	ARP: Request, 10.186.11.20 asks for 160.224.97.201
120030	548.447265	{ARP:56841}	10.186.11.20	160.224.141.63	ARP	ARP: Request, 10.186.11.20 asks for 160.224.141.63

المختصرات:

ARP	Address Resolution Protocol
MAC	Media Access Control
IP	Internet Protocol
IPv4	Internet Protocol version 4
LAN	Local Area Network
NIC	Network Interface Card
HA	Hardware Address
RARP	Reverse Address Resolution Protocol.
ICMP	Internet Control Message Protocol
UDP	User Datagram Protocol
TCP	Transmission Control Protocol

المراجع:

1. TANENBAUM, A. S. *Computer Networks*, Fourth Edition, Prentice Hall PTR, Upper Saddle River, New Jersey 07458, 2003, 891.
2. GROTH, D.; LAMMLE, T.; TEDDER, W. *Network+ Study Guide*, Deluxe Edition, Sybex, 2003, 578.
3. RAMADAS SHANMUGAM, R.; PADMINI, S. *Special Edition Using TCP/IP*, Second Edition, Que Publishing, Indianapolis, Indiana 46290, 2002, 510.
4. SLOAN, J. D. *Network Troubleshooting Tools*, O'Reilly, August 2001, 364.
5. WEAVER, N.; PAXON, V.; STANIFORD, S and CUNNINGHAM, R. *A Taxonomy of Computer Worms*, Washington DC, USA, October 2003, 8.