الأمن في IPv6

عبدالمحسن الدعفس
423103099

مقدمة:

IP هو بروتوكول شبكة الإتصال التي يجب أن تستخدمها كل الأجهزة المتصلة بالإنترنت للإتصال مع بعضها البعض. وهو بمثابة عنوان البريد إذ لا يمكن إرسال خطاب إلى أي شخص مالم تكن تعرف عنوان الشارع والمدينة والدولة والرقم البريدي لهذا الفرد. بالطريقة ذاتها فإن أي حاسب متصل بالإنترنت في أي وقت يكون له عنوان IP فريد.

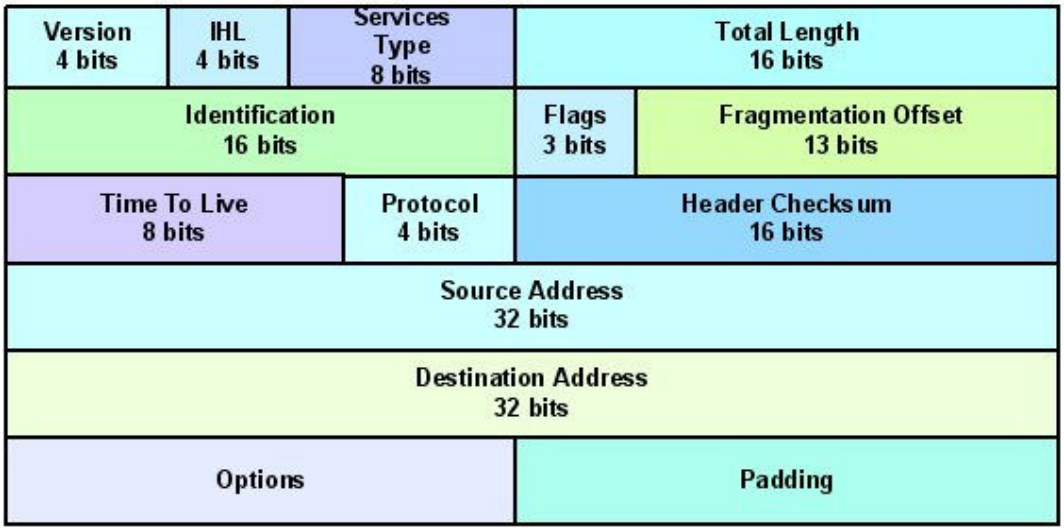
يتم تخصيص عناوين ال IP للحاسبات بطريقتين: ثابتة ومتغيرة. عناوين ال IP الثابتة تخصص للمزودات أو الخوادم لذا تكون ثابتة يمكن للجميع الوصول إليها ، أما المتغيرة فتكون لأجهزة العميل أو بعنى آخر الأجهزة التي لا تحتاج لأن تكون متصلة كل الوقت. ويتم تخصيص عنوان متغير لها من قبل مزود خدمة الإنترنت "الذي له عنوان ثابت" بواسطة بروتوكول Dynamic Host Configuration Protocol (DHCP).

نستخدم حاليا بوتوكول IP النسخة الرابعة بشكل أساسي ويستطيع أن يوفر لنا 4,294,967,296 عنوان فريد، العديد منها محجوز لأهداف خاصة مثل الشبكات الخاصة (حوالي 18 مليون عنوان) وهذا يقلل من العناوين المتاحة لعناوين الإنترنت العامة لذا فالقدرة الإستيعابية ستكون محدودة في المدى البعيد.

ساعدت هذه المحدودية في ولادة IP النسخة السادسة والذي يرمز له ب IPv6 وهو حاليا في مراحل التطوير الأولى ويعتبر حاليا المنافس الوحيد لاستبدال IPv4. لايمكن في بعض الأحيان مراقبة شخص بواسطة عنوان الإنترنت الذي يستخدمه لأنه بإمكانه تزييف العنوان بحيث يبدوا من دولة أخرى.

قبل أن نبدأ باسعراض IPv6 أود أن أنوه إلى أن جميع أرقام النسخ الفردية تكون تجريبية والأرقام الزوجية هي التي تستخدم.

المعيار الجديد لبروتوكول الإنترنت هو IPv6 الغير منتشر حاليا ويبلغ طوله 128 بت. نظريا تبلغ العناوين الفريدة 2^{128} أو حوالي 3.403×10^{38} عنوان. يمثل الشكل التالي رزمة IPv6 :



طريقة استخدام العناوين في IPv6 :

يتكون العنوان من ثمان خانات يتم فصل كل خانة وأخرى بنقطتين رأسيتين ':' تحتوي كل خانة على أربعة أرقام ستعشرية "من 0 إلى 9 ومن A إلى F" ويمكن تجاهل الأصفار القيادية وإذا كان هنالك سلسلة كلها أصفار فيمكن تجاهل كتابتها، يوضح لنا هذا المثال طريقة كتابة العنوان:

1080:0000:0000:0000:0000:0034:0000:417A
1080:0:0:0:0:34:0:417A
1080::34:0:417A

جميع هذه العناوين تمثل عنوان واحد لكن طريقة الكتابة مختلفة.

الأمن في IPv6:

يجب أن ندرك أن IPv6 ليس فقط مجرد زيادة في عدد العناوين بل هناك الكثير من التطويرات مثل دعمه الأساسي ل IPSec (عبارة عن معيار لحماية رزم الIP بواسطة التشفير والتحقق من الهوية) . أيضا تطوير أداء التوجيه باستخدام بنية سهلة لترويسة الرزم "Packets header". ولا ننسى أن حجم الرزمة الواحدة في IPv4 محدود ب 64 kb لكن مع IPv6 نستطيع كسر هذة المحدودية وهذا ما يعرف ب Jumbograms وهذا من شأنه زيادة أداء الشبكات. يستطيع مضيفوا IPv6 (IPv6 hosts) ضبط الإعدادات تلقائيا عند الإتصال بشبكة IPv6 موجهة 'stateless address autoconfiguration'.

أيضاً فقد تم فصل التحقق من الهوية Authorization من التشفير Encryption وذلك ليتم التحقق من الهوية في الحالات التي لاتسمح بالتشفير أو يكون التشفير فيها مكلفاً.

للإستفادة من تقنية IPSec بكفاءة أكثر تم استحداث إطار عمل لإدارة المفتاح أو ما يسمى " Key Management Framework" للحصول على اتصال آمن من نقطة البداية في أحد الطرفين إلى نقطة النهاية. ولذا نجد أن IPv4 يدعم هذة الخاصية بدون Key Management Framework الذي يقوم بها IPv6.

الجدير بالذكر أن IPv6 يستخدم تقنية IPSec بشكل مستقل لذا نحتاج إلى مفتاح عام Public Key لاستخدامه في نطاق واسع ووظيفته الرئيسية هي التحقق من هوية المصدر بواسطة هذا المفتاح مع مفتاح المظيف Host أو مقدم الخدمة Server في الإنترنت. لكن المشكلة تكمن في أنه لايوجد معيار مقبول للمفتاح العام Public Key ولا يمكن وضع مفتاح واحد لجميع من في الشبكة فهذا غير مقبول عمليا ولا يوافق فلسفة الإنترنت. والبديل لهذه الطريقة للتحقق من من الهوية بدون طرف ثالث هو استخدام ما يسمى بالعناوين المولدة بشكل تخطيطي Cryptographically Generated Addresses "CGAs" وهي تقدم لنا خدمة أمنية تحت مستوى المفتاح العام Strong Public Key Authorization وأعلى من نظريات التوجيه Routing methods . والفكرة من هذه الطريقة هي تكوين آخر 64 بت من عنوان ال IP بواجهه تعريفية عن طريق حساب قيمة ال Hash لهذه البتات وجعلها مفتاح تعريفي للعنوان. ويتم توقيع البيانات مع المفتاح الخاص به Private Key ويتم إرسال المفتاح العام Public key مع البيانات الموقعة ثم يقوم المستقبل بحساب قيمة ال Hash للمفتاح العام Public Key ويقارن هذه القيمة مع قيمة ال Hash في عنوان ال IP للمرسل ويتم كل هذا قبل بداية إرسال البيانات. وهذا من شأنه منع أي شيء من إرسال بيانات بواسطة عنوان IP آخر والجدير بالذكر أنه لا يمكن استخدام ال CGAs إلا مع IPv6 .

من السهل عمل مسح شامل على شبكة IPv4 . كل ما عليك هو معرفة عنوان الشبكة والقيام بمسح شامل على المضيفين المتوفرين لديها. بعض الأدوات مثل nmap يستطيع أي شخص من خلالها القيام بعمل تقرير شامل عن أجهزة الشبكة ونظم التشغيل والخدمات المتوفرة والبروكسيات ومعرفة المنافذ التي يمكن الدخول من خلالها إلى الشبكة أو الخدمات الحساسة التي يمكن المهاجمة من خلالها. وخير مثال ما قامتا به الدودتان Slammer و Blaster اللتان استطاعتا التكاثر عن طريق عمل مسح على الشبكة بحثا عن ثغرات معينة تستطيع من خلالها الولوج إلى جهاز الضحية. والسبب في سهولة المسح على عناوين IPv4 هو قلة عدد العناوين المتوفرة تحت نطاق شبكة معينة. لكن نجد أن هذا مستحيل عمله مع IPv6 لأن عدد العناوين كبيره جداً تجعل مثل هذه الأدوات في ورطة كبيرة مع هذا العدد الهائل من العناوين وكيفيةالبحث عن عنوان حي من بينها.

يوضح الجدول التالي مقارنة بين IPv4 و IPv6 من الناحية الأمنية:

الخدمة	IPv4	IPv6
إلغاء التجزئة Fragmentation	ممكن تجزئة الموجه والنهاية الطرفية end node	ممكن تجزئة النهاية الطرفية end node فقط
التوجيه المصدري Source routing	ممكن تعطيله	يتطلب توجيه عناوين النقالات mobile
إعادة التوجيه باستخدام ICMP	لا يتم توجيه ip icmp	لا يتم توجيه IPv6
العنونة النتكررة Duplicate addressing	لا يوجد	حاليا لا يوجد
الحماية	الطبقة الثالثة	الطبقة الثانية والثالثة
التحقق من الهوية تكامل البيانات السرية	IPSec	الطلب من IPSec

التحديات:

هناك بعض المشاكل التي تواجه فريق التطوير وما زالت الحلول المطروحة مبدئية وقيد الدراسة ومن أهم هذه المشاكل هي الواجهة التعريفية التي تستخدم للعناوين العامة Public Key. فعند إرسال البيانات بطريقة سرية بدون استخدام Tunnel mode سيكون عنوان ال IPv6 ظاهراً للمرسل والمستقبل على حد سواء. وهذا ما يجعل المتنصتون على الشبكة قادرون على ملاحظة الجلسة "Session". وإذا كانت الأجهزة متحركة فيمكن تتبع حركتها أيضاً. وهذا يعتبر مشكلة أمنية خطيرة خاصة مع الشبكات اللاسلكية وأجهزة النقال، والحل المقترح لهذه المشكلة هو استخدام رقم عشوائي مزيف يتغير مع الوقت ويكون في الواجهة التعريفية Interface Identity.

المصادر:

http://www.microsoft.com/technet/community/columns/cableguy/cg1005.mspx#ERB

http://www.stindustries.net/IPv6/whitepapers/IPv6_Security.pdf#search='security%20in%20ipv6'

http://www.6journal.org/archive/00000160/01/SEINIT_up6-2Ladid.pdf

http://users.adelphia.net/~snyderbunch/ipv6-security.htm

http://www.microsoft.com/technet/itsolutions/network/ipv6/ipv6sec.mspx

http://en.wikipedia.org/wiki/IP_address

http://en.wikipedia.org/wiki/IPv6

كتاب الإتصال عالي السرعة بالإنترنت