ITRAINONLINE MMTK

التشبيك المتقدّم – كراسة المتدرّب

إعداد: ألبيرتو إسكوديرو باسكال / <aep@it46.se> +46 IT>
النسخة العربية: أنس طويلة، www.tawileh.net/anas

1.....ITRAINONLINE MMTK
1. عن هذا المستند.....2
1.1. معلومات حفظ الملكية الفكرية.....2
2.1. المتطلّبات المسبقة.....2
2.1. درجة الصعوبة.....2
2. مقدّمة.....2
3. نموذج OSI.....2
4. التحكّم بالوصول إلى الناقل Media Access Control 3
1.4. بروتوكولات التحكّم بالوصول إلى الناقل Access Control Protocols.....4
1.41.. الوصول المتعدد عبر تحسّس الناقل (Carrier Sense Multiple Access (CSMA
وكشف التصادم Collision Detection (CD).....4
2.4. العنونة الفيزيائيّة MAC Addressing.....7
3.4. تشفير وصلة البيانات Data Link Encryption.....8
5. مستوى الشبكة Network Layer (IP) 8
1.5. العنونة Addressing.....9
1.51.. الشبكات الفرعيّة وقناع الشبكة Subnetting and Netmask.....9
2.5. التحكّم بالأخطاء Error Control.....10
3.5. التوجيه Routing.....11
4.5. ترجمة عناوين الشبكة Network Address Translation (NAT).....11
4.51.. التقنيع SNAT.....12
4.52.. ترجمة عناوين الوجهة DNAT.....12
5.5. أقنية بروتوكول الإنترنت IP Tunnelling.....13
5. مستوى النقل Transport Layer 14
1.6. بروتوكول التحكّم بالنقل Transmission Control Protocol (TCP).....15
2.6. بروتوكول بيانات المستخدم User Data Protocol (UDP).....15
3.6. الجدران الناريّة ضمن الطبقة الثالثة Layer 3 Firewalls.....17
7. مستوى التطبيقات Application Layer 18
1.7. الجدران الناريّة ضمن مستوى التطبيقات Application Firewalls.....19
8. الخلاصة.....20

1.عن هذا المستند

تشكل هذه المواد التدريبية جزءاً من حزمة تدريب الوسائط المتعددة Multimedia Training Kit (MMTK). توفر هذه الحزمة مجموعةً متكاملةً من المواد التدريبية والموارد الداعمة للإعلام الإجتماعي، مراكز الوسائط المتعددة للمجتمعات، مراكز الولوج البعيد وغيرها من المبادرات باستخدام تقنيات المعلومات والإتصالات لتدعيم المجتمعات ودعم نشاطات التنمية.

1.1 معلومات حفظ الملكية الفكرية

لقد تم إصدار هذه الوحدة ضمن إتفاقية الترخيص Creative Commons Attribution-NonCommercial-ShareAlike 2.5 السويد. للحصول على المزيد من المعلومات عن كيفية استخدام هذه المواد يرجى الإطلاع على نص حماية الملكية الفكرية المضمن مع هذه الوحدة أو راجع http://creativecommons.org/licenses/by-nc-sa/2.5/se/

2.1 المتطلّبات المسبقة

لاستيعاب هذه الوحدة على الشكل الأمثل يتوجّب عليك الإلمام بمبادئ بروتوكول الإنترنت IP والمتطلّبات الأساسيّة للإتصال بالإنترنت، كما ينبغي أن تكون على درايةٍ ببعض المفاهيم الأساسيّة مثل عنونة الإنترنت ومبادئ التوجيه.

2.1 .درجة الصعوبة

درجة صعوبة هذه الوحدة: متقدّم.

2. مقدّمة

تستعرض هذه الوحدة كدسة Stack بروتوكولات الإنترنت / OSI مع التركيز على الجوانب المتعلّقة بتركيب الشبكات اللاسلكية. تلخّص الوحدة تأثيرات كل طبقةٍ على الأداء الكلّي لشبكة الإتصالات اللاسلكية.

تهدف هذه الوحدة إلى توفير شرحٍ لكيفيّة تأثير كلٍّ من الطبقات المختلفة (المكونات) من نموذج OSI على الطبقات الأخرى بالإضافة إلى العناصر الأساسيّة التي ينبغي أخذها بعين الإعتبار عند تخطيط الشبكات اللاسلكية. سنستخدم نموذج OSI كنموذجٍ مرجعيٍّ للمساعدة في استيعاب التفاعل بين هذه المكونات.

تشير الأيقونة الحمراء في أي موقعٍ من هذه الوحدة إلى أنّ هذه الفقرة تتعلّق خصيصاً بالشبكات اللاسلكية وليس بالشبكات بشكلٍ عامٍ.

3.نموذج OSI

نموذج OSI (Open Systems Interconnection) المعياري (والذي أعدّته منظمة المعايير الدولية International Standards Organisation) هو توصيفٌ نظريٌّ لتصميم بروتوكولات شبكات الحواسب

(والإتصالات). يفصل هذا النموذج وظائف الإتصال إلى سبع طبقاتٍ مختلفةٍ يمكنها العمل بشكلٍ مستقلٍّ عن بعضها البعض.

يتبع تصميم البروتوكولات التي تتبع هيكليّة نموذج OSI مبادئ "الكدسة Stack". تستخدم كلّ طبقةٍ من طبقات البروتوكول خدمات الطبقة التي تقع أسفلها مباشرةً فقط وتقدّم خدماتها للطبقة التي تعلوها مباشرةً فقط. يمكن تطبيق "كدسة" البروتوكولات ضمن البرمجيّات، التجهيزات أو ضمن خليطٍ من كليهما.

عمليّاً، لا يتّبع نموذج OSI بدقّةٍ في الكثير من البروتوكولات المعروفة. على سبيل المثال، تتبع الإنترنت حزمة بروتوكولاتٍ ذات أربع طبقات تتألّف من طبقة الوصول إلى الناقل (طبقة الوصلة)، طبقة الشبكة (بروتوكول الإنترنت IP)، طبقة النقل (TCP/UDP) وطبقة التطبيقات.

الطبقة	OSI	TCP/IP
7	التطبيقات Application	التطبيقات Application
6	التقديم Presentation	
5	الجلسة Session	النقل (TCP Transport)
4	النقل Transport	
3	الشبكة Network	الشبكة (IP Network)
2	وصلة البيانات Data Link	التحكّم بالوصول إلى الناقل Media Access Control
1	الفيزيائيّة Physical	

جدول 1: نموذج OSI المعياري في مقابل مجموعة بروتوكولات TCP/IP

تتعلّق معايير الشبكات اللاسلكية عادةً بالطبقتين الأولى والثانية من كدسة بروتوكولات OSI للحفاظ على حزمة بروتوكولات الإنترنت IP دون تغيير. يتم نقل حزم بروتوكول الإنترنت IP عبر بروتوكولاتٍ خاصّةٍ بالشبكة اللاسلكية في الطبقة الفيزيائيّة وطبقة وصلة البيانات.

تتعامل معايير الشبكات اللاسلكية (IEEE 802.11, IEEE 802.16, Bluetooth, IrDA وغيرها) مع الطبقة الفيزيائيّة وطبقة الوصلة فقط، وقد صممما أساساً لنقل أيّ نوعٍ من البيانات وبروتوكول الإنترنت IP هو نوعٌ واحدٌ فقط من هذه البيانات. تصمم معايير الشبكة اللاسلكية خارج فريق عمل هندسة الإنترنت (Internet Engineering Task Force (IETF.

يعتبر المعهد الدولي لمهندسي الكهرباء والإلكترون أحد أبرز جهات وضع المعايير للشبكات اللاسلكية http://standards.ieee.org/wireless

4. التحكّم بالوصول إلى الناقل Media Access Control

تتضمّن طبقة التحكّم بالوصول إلى الناقل (Media Access Control (MAC في نموذج TCP/IP الطبقة الفيزيائيّة من نموذج OSI والتي تتعلّق بغالبيّة الجوانب الفيزيائيّة للإتصال (تقنيات الترميز، ترميز البتّات،

الوصول الفيزيائي إلى الناقل إلخ) وطبقة الوصلة المسؤولة عن العنونة وتوصيل الحزم من حاسبٍ (مضيفٍ) إلى آخر عبر قناة نقلٍ مشتركة.

يمكننا القول بأنّ الطبقة الفيزيائيّة مسؤولةٌ عن تحويل الإشارات الكهرطيسيّة الفيزيائيّة إلى بتّات Bits في حين تعتبر طبقة الوصلة مسؤولةً عن تجميع هذه البتّات على شكل حزم بيانات Data Packets.

من البروتوكولات الشائعة للطبقة الفيزيائيّة RS-232, V. 35, 10BaseT, ISDN إلخ.
من البروتوكولات الشائعة لطبقة الوصلة بروتوكول الإيثرنت ATM، PPP، IEEE 802.3 إلخ.

تتعلّق معايير الشبكات اللاسلكية مثل IEEE 802.11 (WLAN) بالطبقة الفيزيائيّة وطبقة الوصلة في نموذج OSI المعياري.

تستخدم عائلة بروتوكولات IEEE 802.11 عدداً من بروتوكولات الطبقة الفيزيائيّة المختلفة والتي تعتمد على مفاهيم الطيف الموزّع Spread Spectrum (FHSS، DSSS و OFDM).

يحدد المعيار الأساسي IEEE 802.11-1997 طبقةً واحدةً للتحكّم بالوصول إلى الناقل MAC وثلاثة مواصفاتٍ للطبقة الفيزيائيّة. يقدّم المعيار توصيفين للطبقة الفيزيائيّة للإرسال الراديوي اللاسلكي (والعامل ضمن حزمة الترددات 2400 – 2483.5 ميغاهرتز (FHSS و DSSS) وتوصيفاً واحداً للإرسال بالأشعة تحت الحمراء Infrared.

للمزيد من المعلومات راجع http://grouper.ieee.org/groups/802/11/main.html

1.4 بروتوكولات التحكّم بالوصول إلى الناقل Access Control Protocols

1.41. الوصول المتعدد عبر تحسّس الناقل Carrier Sense Multiple Access (CSMA) (كشف التصادم Collision Detection (CD)

من أكثر آليّات التحكّم بالوصول الفيزيائي إلى الناقل شهرةً حيث تقوم مجموعةٌ من الحواسب بالوصول إلى ناقلٍ مشتركٍ الإيثرنت Ethernet. يستخدم بروتوكول الإيثرنت أو IEEE 802.3 بروتوكولاً للتحكم بالوصول يعرف بإسم الوصول المتعدد عبر تحسّس الناقل Carrier Sense Multiple Access (CSMA) وهو نسخةٌ مطورةٌ من تقنية معالجة التعارض تدعى ALOHA.

عندما تملك نقطةٌ ما بياناتٍ تريد إرسالها ستقوم بدايةً بالإستماع إلى الناقل لمعرفة ما إذا كانت أيّة نقطةٍ أخرى تقوم بالإرسال في تلك اللحظة (عبر الإستماع إلى القناة المشتركة). إذا لم تكتشف النقطة وجود أي إرسالٍ ضمن الناقل ستبدأ عندها بإرسال البيانات. من الممكن جداً أن يبدأ إرسال البيانات من نقطتين مختلفتين في آنٍ واحدٍ حيث يمكن لكليهما اكتشاف عدم وجود أيّ إرسالٍ على الناقل. عند قيام عدّة نقاط

بإرسال البيانات في آنٍ واحدٍ سينتج عن ذلك تصادمٌ يؤدّي إلى إتلاف البيانات. سيتم كشف هذا التصادم من قبل المستقبل نتيجة عدم تطابق بيانات التحقق من سلامة البيانات CRC مع البيانات المستقبلة. سيقوم المستقبل عندها بإهمال البيانات التالفة.

يستخدم المرسل عنصراً آخر من بروتوكول الإيثرنت تدعى كشف التصادم (Collision Detection (CD لكشف تصادم حزم البيانات. تقوم النقاط المرسلة للبيانات بمراقبة الناقل المشترك باستمرار (يمكنها الإستماع إلى البيانات الموجودة ضمن الناقل أثناء الإرسال). إذا تم الكشف عن تصادمٍ ما (عند سماع المرسل لبياناتٍ تختلف عن تلك التي قام بإرسالها) ستتوقّف النقطة عن الإرسال وسترسل رقماً لتعريف الإزدحام Jam Sequence لإعلام النقاط المستقبلة بحدوث التصادم وبضرورة إهمال الحزم المستقبلة.

ستقوم جميع النقاط بعد كشف التصادم بإعادة إرسال البيانات مجدداً. لتجنّب التصادم مجدداً عند إعادة الإرسال يستخدم بروتوكول الإيثرنت فترة تراجعٍ عشوائيّةً (تعتمد على معاملٍ عشوائيٍّ وعلى عدد محاولات إعادة الإرسال السابقة) لحساب فترة الإنتظار قبل معاودة الإرسال. يحاول بروتوكول الإنترنت تقليص إحتمالات "إعادة التصادم" بعد كشف تصادمٍ ما.

(IEEE 802.11 (WLAN

تدعى طبقة التحكّم بالوصول إلى الناقل في معيار IEEE 802.11 (WLAN) بـــ CSMA/CA وهي تشبه إلى حدٍ كبيرٍ بروتوكول الإيثرنت كونها تستخدم آليّة CSMA لمشاركة الناقل مع النقاط اللاسلكية الأخرى إلا أنّها تفتقد آليّة كشف التصادم Collision Detection (CD). لا يمكن للمرسل كشف التصادم نظراً لتعذّر الإستماع إلى البيانات أثناء الإرسال. يعمل معيار IEEE 802.11 عبر الإرسال / الإستقبال الأحادي Half Duplex باستخدام تقنيّة TDD. لذلك لا يمكن استخدام آليّة كشف التصادم بنفس أسلوب بروتوكول الإيثرنت في الإرسال اللاسلكي لمعايير IEEE 802.11.

بما أنّ باستطاعة النقاط في الشبكة اللاسلكية كشف عدم وجود إشارةٍ على الناقل لكنّها عاجزةٌ عن كشف التصادمات على هذا الناقل لذلك ينبغي أن تقوم نقاط الولوج بإرسال إشعارٍ لتأكيد نجاح الإرسال. تزيد هذه الآليّة من الحمل الزائد على الشبكة وتقلل من سعة نقل البيانات الفعليّة.

تحدث نتيجة هذه المحدوديّة في شبكات IEEE 802.11 الواصلة من نقطةٍ إلى عدّة نقاطٍ مشكلةٌ معروفةٌ تدعى مشكلة "النقطة الخفيّة Hidden Node". في إعدادات الشبكات الواصلة من نقطةٍ إلى عدّة نقاط تتخاطل مجموعةٌ من النقاط مع نقطةٍ مشتركةٍ تدعى "نقطة الولوج Access Point". تنتج "النقطة الخفيّة Hidden Node" بسبب عدم تمكّن جميع النقاط من الإستماع لبعضها البعض ضمن الشبكة اللاسلكية مما يؤدّي إلى عدم إمكانيّة تجنّب التصادمات باستخدام آليّة CSMA فقط. لحل (أو لتخفيف) هذه المشكلة تحتوي طبقة الوصول إلى الناقل MAC من معيار IEEE 802.11 آليّةً تدعى تجنّب التصادم Collision Avoidance (CA)). يجب أن تقوم نقطة الإرسال عند استخدام تجنّب التصادم CA بإرسال حزمة جاهزيّة الإرسال Ready to Send (RTS) إلى نقطة الولوج وانتظار حزمة جاهزيّة الإستقبال Clear to Send (CTS) قبل بدء الإرسال.

على الرغم من تعذّر سماع حزمة RTS من قبل جميع نقاط الشبكة الأخرى إلا أنّها قادرةٌ على سماع الرد CTS المرسل من قبل نقطة الولوج إلى نقطةٍ معيّنةٍ. هكذا تستطيع نقاط الشبكة تجنّب إرسال البيانات خلال الفترة الزمنيّة المخصصة من قبل نقطة الولوج لنقطةٍ معيّنةٍ ضمن الشبكة.

لا تعمل آليّة RTS/CTS بشكلٍ فعّالٍ عندما تزداد المسافة بين نقاط الشبكة أو بين نقاط الشبكة ونقطة الولوج ولا بدّ حينها من البحث عن بدائل أخرى.

(IEEE 802.16 (WMAN

لقد أخذ تصميم المعيار IEEE 802.16 بالحسبان بعض المشاكل الموجودة ضمن سابقه IEEE 802.11 لذلك فهو يوفّر حلاً لمشكلة "النقطة الخفيّة Hidden Node" للوصلات اللاسلكية التي تربط نقطةً بعدّة نقاط PtMP. علينا أن نتذكّر هنا بأنّ المعيار IEEE 802.11 لم يكن مصمماً بالأساس ليعمل ضمن البيئات الخارجيّة. يستخدم معيار IEEE 802.16 مزيجاً من تقنيّات TDMA و DAMA لمعالجة المشاكل التي مازال نظيره IEEE 802.11 يناضل لحلّها حتى يومنا هذا.

يتوجّب علينا في هذا السياق التأكّيد على ضرورة التصميم الجيّد للشبكة ولبنيّة نقل البيانات ضمن الشبكة اللاسلكية لتجاوز محدوديّة آليّات التحكّم بالوصول إلى الناقل MAC في المعيار IEEE 802.11. لقد أظهرت التجارب الآثار السلبيّة لإضافة الكثير من النقاط إلى شبكةٍ لاسلكيةٍ دون أخذ اعتبارات تصميم الشبكة ونقل البيانات ضمنها بالحسبان.

2.4.العنونة الفيزيائيّة MAC Addressing

يستخدم العنوان الفيزيائي MAC ضمن طبقة الوصلة كآليّةٍ لتحديد وعنونة البيانات المرسلة إلى مضيفٍ معيّنٍ ضمن ناقلٍ مشترك. يتألّف هذا العنوان من تسلسلٍ فريدٍ يحتوي على 48 بتّاً (12 رقماً ست عشريّاً) مرتبط ببطاقةٍ شبكةٍ لاسلكيةٍ محددةٍ (أو جهاز).

تحتوي ترويسة حزم البيانات المرسلة عبر ناقلٍ مشتركٍ عناوين حواسب المصدر والوجهة لهذه البيانات. يتم استخدام عنوانٍ خاصٍّ عند إرسال الحزم إلى جميع الحواسب (بث Broadcast) يدعى عنوان البث وهو يعادل في شبكات الإيثرنت العنوان ff:ff:ff:ff:ff:ff (جميع البتّات الـــ 48 تساوي 1).

تقوم بطاقة الشبكة عادةً بتمرير حزم البيانات التي توافق العنوان الفيزيائي MAC للحاسب فقط إلى نظام التشغيل.

يكون العنوان الفيزيائي عادةً مثبّتاً ضمن التجهيزات عندما يقوم المنتج بشحنها.

إستخدام العناوين الفيزيائيّة للتحقق من الهويّة

لقد شاع استخدام العناوين الفيزيائيّة MAC لبطاقات الشبكة اللاسلكية في الكثير من شبكات مزودي خدمات الإنترنت اللاسلكية WISP كآليّةٍ لإتاحة أو منع الوصول إلى الشبكة. يعتمد هذا الإجراء على افتراض أنّ العناوين الفيزيائيّة تأتي "مثبّتةً" ضمن التجهيزات، مما يجعلها غير قابلةٍ للتعديل من قبل المستخدم العادي. لكن الحقيقية تخالف هذا الإفتراض ويمكن عمليّاً تغيير العنوان الفيزيائي MAC لمعظم بطاقات الشبكة اللاسلكيّة بسهولة.

لا يمكن اعتبار آليات التحقق من الهويّة بالإعتماد على العناوين الفيزيائيّة خياراً آمناً.

3.4.تشفير وصلةالبيانات Data Link Encryption

تشفير وصلة البيانات هو عمليّة تأمين البيانات ضمن مستوى الوصلة أثناء انتقالها بين نقطتين متصلتين بنفس الوصلة الفيزيائيّة (كما يمكن أن يتصلا بوصلتين فيزيائيتين مستقلتين عبر استخدام مكرر كوصلات الأقمار الصناعيّة). يقوم هذا التشفير بحماية جميع البروتوكولات وبيانات التطبيقات المنتقلة عبر الوصلة الفيزيائيّة من أعين المتطفلين.

يتطلب التشفير مشاركة مفتاحٍ أو سرٍ معيّن بين الأطراف المتصلة ببعضها البعض بالإضافة إلى الإتفاق على خوارزميّة تشفيرٍ مشتركة. عندما لا يقع المرسل والمستقبل ضمن نفس الناقل ينبغي فك تشفير البيانات وإعادة تشفيرها عند كلّ نقطة تبديلٍ للناقل على طول مسار البيانات.

يستخدم التشفير على مستوى الوصلة عادةٍ عندما لا يوجد تشفيرٌ على مستويات أعلى ضمن الشبكة.

التشفير على مستوى الوصلة في شبكات IEEE 802.11

تعتبر أكثر خوارزميّات التشفير على مستوى الوصلة شهرةً في شبكات IEEE 802.11 خوارزميّة الخصوصيّة المكافئة للشبكة السلكية (Wired Equivalent Privacy (WEP. لقد أثبتت التجارب أنّ هذه الخوارزميّة غير آمنة مما أدّى إلى اقتراح عدّة بدائل أقرّت كمعيار أسمي الوصول المحمي إلى الشبكة اللاسلكية (WiFi Protected Access (WAP. سيتضمّن المعيار الجديد للشبكات اللاسلكية IEEE 802.11i إصداراً مطوراً من WPA يدعى WPA2.

لا يوفّر التشفير على مستوى الوصلة أمن البيانات من البداية إلى النهاية خارج الوصلة الفيزيائيّة ويتوجّب اعتباره دائماً مجرّد إجراءٍ أمنيٍّ إضافيٍّ عند تصميم الشبكة اللاسلكية.

يتطلّب تشفير الوصلة مزيداً من موارد التجهيزات ضمن نقاط الولوج بالإضافة إلى تصميم آليّاتٍ آمنةٍ لإدارة وتوزيع مفاتيح التشفير.

5.مستوى الشبكة Network Layer (IP)

يستخدم بروتوكول الإنترنت Internet Protocol لإرسال البيانات عبر شبكةٍ تعمل بتبديد الحزم Packet-Switched, يطلق على البيانات المرسلة عبر شبكة برتوكول الإنترنت IP إسم الحزم Packets. يوفّر بروتوكول الإنترنت IP خدمةً غير موثوقةٍ Unreliable (الجهد الأقصى) لنقل البيانات دون ضمان وصولها. قد تصل حزم البيانات معطوبةً، مكررةً، دون ترتيبٍ أو قد يتم إهمالها بالكامل من قبل أحد النقاط على المسار.

يعتبر عنوان المصدر والوجهة للأطراف المتواصلة أحد أهم عناصر بروتوكول الإنترنت IP. لا تستخدم هذه المعلومات (العناوين) لإرسال الحزم أو تحديد النقاط وحسب، بل تستخدم أيضاً في التطبيقات عالية المستوى مثل الجدران الناريّة Firewalls.

1.5.العنونة Addressing

يعدّ الإصدار الرابع من بروتوكول الإنترنت IPv4 أكثر أشكال بروتوكول الإنترنت إستخداماً. يستخدم هذا الإصدار حقلاً للعنوان طوله 32 بت. أما الجيل التالي من بروتوكول الإنترنت فسيعتمد عناوين بطول 128 بتّاً للوجهة والمصدر لتجذّب مشكلة نفاذ عناوين الإنترنت IPv4 المتاحة.

1.51.الشبكات الفرعّيةوقناع الشبكة Subnetting and Netmask

تستخدم الشبكات الفرعيّة Subnet بشكلٍ عامٍّ للتحكّم / تقسيم البيانات المنتقلة عبر الشبكة. يمكن بفضل الشبكات الفرعيّة أن يشير حقلٌ واحدٌ في جدول التوجيه إلى شبكةٍ فرعيّةٍ كاملةٍ أو إلى كل مضيف ضمنها على حدة، مما يعني أنّه من الممكن إستخدام مسار توجيهٍ واحد عبر الإنترنت في حين تستخدم مسارات توجيهٍ أكثر تحديداً ضمن نطاق الشبكة الفرعيّة فقط.

قناع الشبكة Netmask هو رقمٌ بطول 32 بت يحدد الشبكة الموافقة لعنوان إنترنت IP معيّن. يقسم قناع الشبكة إلى قسمين: قسم الشبكة وقسم المضيف حيث تشير البتات ذات القيمة 1 إلى الشبكة والبتّات ذات القيمة 0 إلى المضيف.

10.0.0.0/255.0.0.0	شبكة من الفئة A
10.1.0.0/255.255.0.0	255 شبكة من الفئة B
10.1.1.0/255.255.255.0	255 شبكة من الفئة C
10.1.1.128/255.255.255.128	نصف الفئة 127) C عنوان)
10.1.1.64/255.255.255.192	63 عنوان مضيف
10.1.1.8/255.255.255.248	7 عناوين مضيف

جدول 2: الشبكات الفرعيّة ضمن شبكة من الفئة A

يتم إجراء عملية AND المنطقيّة على عنوان الإنترنت IP وقناع الشبكة الموافق للحصول على عنوان الشبكة.

لا بدّ من الإنتباه إلى القيود المفروضة على عنوان الشبكة الفرعيّة. تحجز عناوين المضيف المؤلّفة جميعها من أصفار أو واحدات لتعريف عنوان الشبكة المحليّة وعنوان البث Broadcast. تنطبق هذه القاعدة أيضاً على الشبكات الفرعيّة، مما يعني أنّه لا يمكن استخدام قناعٍ للشبكة يتألّف من واحدات فقط.

يمكن استخدام المعادلة التالية لحساب عدد الشبكات الفرعيّة والأجهزة التي يتيحها قناع شبكةٍ ما:

عدد الشبكات الفرعيّة = $2^n - 2$ حيث n هو عدد البتّات في قناع الشبكة
عدد الأجهزة في الشبكة الفرعيّة = $2^m - 2$ حيث m هو عدد البتّات في الشبكة المضيفة

العدد الإجمالي للأجهزة = $(2^n - 2)(2^m - 2)$

عنونة الشبكات الفرعيّة في الشبكات اللاسلكية

لا يقوم مزودوا خدمات الإنترنت اللاسلكية عادةً بعنونة شبكاتهم الفرعيّة بشكلٍ صحيح. من السهل القيام بتركيب شبكةٍ فرعيّةٍ واحدةٍ كبيرةٍ لا تتطلب اتخاذ أيّة قراراتٍ لتوجيه الحزم، إلا أنّ هذه إدارة وكشف أعطال هذه الشبكة تزداد تعقيداً مع ازدياد حجم الشبكة.

إنّ عنونة الشبكة اللاسلكية وتصميم بنية التوجيه بشكلٍ جيّدٍ سيحد من حركة بيانات البث Broadcast غير الضروريّة ويمكّن الشبكة من التوسّع بشكلٍ أفضل.

تجنّب قدر الإمكان استخدام شبكةٍ فرعيّةٍ واحدةٍ كبيرةٍ. ننصحك بتصميم شبكاتك الفرعيّة على ألا تتجاوز أيّ منها 32–64 مضيفاً.

2.5. التحكّم بالأخطاء Error Control

يتم التحكّم بالأخطاء عبر مجموعة من رسائل التحكّم ضمن مستوى بروتوكول الإنترنت IP تدعى بروتوكول رسائل التحكّم بالإنترنت (Internet Control Message Protocol (ICMP. لا يقوم هذا البروتوكول بالتحكّم بالأخطاء بشكلٍ كاملٍ بل يقوم فقط بإعلام المرسل عن الخطأ عند حدوثه.

تعتبر العمليّات التالية من أهم استخدامات بروتوكول ICMP:

- الإعلام عن المشاكل التي قد تؤدّي إلى تعذّر إيصال حزم البيانات (مثل مشاكل "**لا يمكن الإتصال بالوجهة** Destination Unreachable").
- كشف أعطال الشبكة باستخدام رسائل الطلب والرد (مثل رسائل "Echo Request" و "Echo Reply" والمستخدمة من قبل الأداة Ping).

تحتوي رسالة الخطأ في بروتوكول ICMP دائماً على ترويسة بروتوكول الإنترنت IP بأكملها (بما فيها الخيارات) للحزمة الفاشلة بالإضافة إلى البايتات الثمانية الأولى من حقل البيانات ضمن هذه الحزمة. يمكن حينها ربط الخطأ مع بروتوكولٍ معيّنٍ ومهمّةٍ معيّنةٍ (من خلال رقم البوابة ضمن ترويسة TCP أو UDP والتي تشكّل البايتات الثمانية الأولى من حقل البيانات في حزم بروتوكول الإنترنت IP).

مراقبة بروتوكول ICMP في الشبكات اللاسلكية

تتيح لك مراقبة حركة بروتوكول ICMP ضمن شبكتك اللاسلكية بالإضافة إلى تحديد مشاكل الإتصال ضمن الشبكة اكتشاف وجود بعض الفيروسات وأحصنة طروادة. تقوم غالبية الفيروسات وأحصنة طروادة بالمسح التلقائي للشبكة، وبالتالي فإنّ وجود حجمٍ كبيرٍ من رسائل "**لا يمكن الإتصال بالوجهة Destination Unreachable**" قد يشير إلى وجود نشاط للفيروسات ضمن الشبكة.

3.5.التوجيه Routing

تدعى عمليّة توجيه حزمة بياناتٍ من المصدر إلى الوجهة *بالتوجيه*. يتم اتخاذ *قرار توجيهٍ* في كل حاسبٍ يقع بين المصدر والوجهة لتحديد النقطة التالية الأمثل باتجاه الوجهة. يتم حفظ قرار التوجيه ضمن *جدول التوجيه*.

تستخدم جميع خوارزميّات التوجيه أحد عنواني الإنترنت IP للوجهة أو المصدر. يتم تحديد مسار البيانات في الحالة الأولى باستخدام عنوان وجهة حزم البيانات (وهو الأسلوب الأكثر شيوعاً) في حين تعتمد الحالة الثانية على عنوان المصدر فقط لتحديد المسار إلى الوجهة. هناك خيارٌ ثالثٌ يدعى "التوجيه المسيّس Policy-Based Routing) حيث تعتمد قرارات التوجيه على مصادر أخرى للمعلومات (مثل العناوين الفيزيائيّة MAC، نوع الخدمة، الضغط على الشبكة وغيرها).

إستخدام عنوان الإنترنت IP للمصدر في اتخاذ قرارات التوجيه

يعتبر استخدام عنوان الإنترنت IP للمصدر في اتخاذ قرارات التوجيه آليّةً ملائمةً لتوزيع الحمل Load Balancing في الشبكات اللاسلكية. يمكننا باستخدام موجّهٍ قادرٍ على اتخاذ القرارات بناءً على عنوان مصدر الحزم تطبيق مستوياتٍ مختلفةٍ من جودة الخدمة Quality of Service للحواسب المختلفة، كما يمكننا أيضاً توجيه مستخدمين مختلفين للشبكة اللاسلكية إلى موجّهاتٍ طرفيّةٍ Border Routers مختلفة.

لا يتطلّب استخدام التوجيه المسيّس بناءٍ على عنوان المصدر Source IP على سبيل المثال تغيير عنونة الشبكة اللاسلكية لتوصيل مستخدمٍ معيّنٍ إلى بوابةٍ خارجيّةٍ مختلفةٍ عن تلك المستخدمة من قبل الآخرين.

4.5.ترجمة عناوين الشبكة Network Address Translation (NAT)

يعتمد مبدأ ترجمة عناوين الشبكة NAT على قدرة الموجّه على "إعادة كتابة" عنوان الوجهة أو المصدر لحزم بروتوكول الإنترنت IP. لقد انتشرت ترجمة عناوين الشبكة NAT على نطاقٍ واسعٍ لأنّها تتيح لجهازٍ واحدٍ يملك عنوان إنترنت عام Public IP أن يقوم بتمثيل مجموعةٍ من الحواسب ضمن شبكةٍ خاصّةٍ.

لا تقتصر أهميّة ترجمة عناوين الشبكة NAT على تجاوز مشاكل شح عناوين الإنترنت الحقيقيّة Public IP Addresses بل تكمن أيضاً في اعتمادها كآليّةٍ لتطبيق مهام الشبكة التالية:

1.الجدار الناري Firewall / المنطقة منزوعة السلاح DMZ.

2.توزيع حمل حركة البيانات Traffic Load Balance (مثال: مجموعة من مخدّمات الوب المتماثلة خلف خدمة NAT لتوزيع طلبات الوصول إلى مواقع الإنترنت).
3.توزيع حمل معالجة البيانات Computing Load Balancing (مثال: مجموعة من قواعد البيانات المتماثلة لتوزيع حمل معالجة طلبات الوصول إلى البيانات).

سنركّز في هذه الفقرة على كيفيّة استخدام ترجمة عناوين الإنترنت NAT لتحسين أمن الشبكة. لقد قمنا بغية التوضيح بتقسيم ترجمة عناوين الإنترنت إلى وظيفتين أساسيتين: التعامل مع عناوين المصدر SNAT والتعامل مع عناوين الوجهة DNAT.

4.51..التقنيع SNAT

يمكّن تقنيع عناوين الإنترنت IP Masquerading (أو ترجمة عناوين المصدر SNAT) الحواسب ذات عناوين الإنترنت الخاصّة من الإتصال بحواسب تقع خارج شبكتها عبر تمكين جهازٍ واحدٍ من العمل بالنيابة عنها. يعتبر تقنيع عناوين الإنترنت شكلاً بسيطاً ومحدوداً من أشكال الجدران الناريّة. لا يسمح التقنيع لحاسبٍ ما **ببدء** الإتصال بحاسبٍ يقع ضمن الشبكة الخاصّة.

يقوم التقنيع Masquerading بإعادة كتابة عنوان المصدر لحزم البيانات أثناء مرورها عبر الموجّه بحيث يستقبل الحاسب الوجهة هذه الحزم وكأنّها صادرةٌ عن الموجّه نفسه. يقوم الموجّه أيضاً عندما يجيب مستقبل البيانات بإعادة كتابة عنوان الوجهة ليتطابق مع عنوان المرسل الأساسي.

يوفّر التقنيع مستوى إضافيّاً من الأمن للشبكة عبر القيام بدور الجدار الناري، لكنه يقوم أيضاً بالحد من قدرة الحواسب الواقعة داخل الشبكة من توفير الخدمات للمستخدمين خارجها.

ملاحظة: لتوخي الدقّة، لا يكافئ التقنيع Masquerade ترجمة عناوين المصدر SNAT تماماً، ذلك لأنّ التقنيع يلغي جميع الوصلات السابقة عند توقّف منفذ الشبكة عن العمل أو عند تغيير عنوان الإنترنت IP لهذا المنفذ.

4.52..ترجمة عناوين الوجهة DNAT

تستخدم ترجمة عناوين الوجهة Destination Network Address Translation – DNAT عادةً لإتاحة خدمةٍ متوفّرةٍ ضمن الشبكة الداخليّة (ذات عنوان إنترنت خاص Private IP Address) للمستخدمين خارج هذه الشبكة عبر إعادة كتابة عنوان الوجهة لحزم البيانات.

يمكن استخدام ترجمة عناوين الوجهة DNAT لتوجيه حزم البيانات ضمن المنطقة منزوعة السلاح Demilitarized Zone (DMZ)، وهي جزء الشبكة المخصص لاستضافة الخدمات المتاحة للعموم. تتوضع المنطقة منزوعة السلاح DMZ عادةً ضمن شبكةٍ فرعيّةٍ مختلفةٍ معزولةٍ عن البيانات المنقولة ضمن الشبكة.

يمكننا باستخدام ترجمة عناوين الوجهة DNAT إعادة توجيه (map) حزم البيانات الواردة إلى عنوان إنترنت عام Public IP Address وباتجاه رقم بوابةٍ معيّنٍ إلى عنوان الإنترنت ورقم البوابة الخاصين بالمنطقة منزوعة السلاح.

تطويع حركة البيانات في الشبكات اللاسلكية

يمكن استخدام ترجمة عناوين الشبكة (الوجهة أو المصدر SNAT / DNAT) لتطويع حركة البيانات في الشبكات اللاسلكية. يمكننا التحكّم بكيفيّة توجيه البيانات وبالخدمات المتاحة لمستخدمي الشبكة اللاسلكية دون أيّ تغييرٍ في إعدادات حواسبهم.

مثال:

يمكننا تطبيق ترجمة عناوين الشبكة NAT لإعادة توجيه طلبات الوصول إلى الإنترنت إلى مخدّمٍ وكيلٍ Proxy Server. يمكننا أكثر من ذلك توجيه أجزاءٍ مختلفةٍ من الشبكة إلى مخدّماتٍ وكيلةٍ مختلفةٍ يتصّل كلٌّ منها بمزودٍ مختلفٍ لخدمات الإنترنت.

يمكن استخدام ترجمة عناوين الإنترنت أيضاً لإعادة توجيه المستخدمين إلى بوابةٍ مقيّدةٍ Captive Portal حيث يتوجّب عليهم التسجيل أو إدخال بيانات حسابهم على الشبكة اللاسلكية.

5.5. أقنية بروتوكول الإنترنت IP Tunnelling

تستخدم أقنية بروتوكول الإنترنت IP Tunnelling لنقل حزم بروتوكول الإنترنت ضمن حزمٍ أخرى لإتاحة إعادة توجيه الحزم المرسلة إلى عنوان إنترنت IP معيّنٍ إلى شبكةٍ أخرى أولاً. يتم القيام بذلك عبر تغليف حزم بروتوكول الإنترنت Encapsulation. يعرف هذا الإجراء عندما يتم القيام بهذا التغليف داخل حزمٍ مشفّرةٍ بإسم الأقنية الآمنة Secure Tunnelling أو الشبكة الخاصّة الإفتراضيّة VPN.

تتطلّب أقنية بروتوكول الإنترنت IP Tunnelling أن تكون نهايات القناة قابلةً للتوجيه دون أن يعترضها جدارٌ ناريٌّ Firewall أو خدمات ترجمة عناوين الشبكة NAT.

لا توفّر أقنية بروتوكول الإنترنت IP Tunnelling أيّة حمايةٍ إضافيّةٍ للبيانات ما لم تكن الحزم المغلّفة (الحزم المنتقلة ضمن القناة) مشفّرةً. يعتبر استخدام بروتوكول التشفير IPSEC أكثر أساليب بناء أقنية بروتوكول الإنترنت الآمنة شيوعاً.

يمكن لبروتوكول التشفير IPSEC ضمان ثلاثة أنواعٍ من الحماية على مستوى بروتوكول الإنترنت:

1. **السريّة Confidentiality** (حماية البيانات)
2. **التحقق من الهويّة Authentication** (التأكّد من هويّة مرسل الرسالة)
3. **الكمال Integrity** (عدم تحريف البيانات)

يحتوي IPSEC على ثلاثة بروتوكولاتٍ أساسيّةٍ لتأمين هذه الخصائص الأمنيّة:

ترويسة التحقق من الهويّة Authentication Header (AH): مجموعٌ خاص مشّفر Crypto Checksum لحزمة بروتوكول الإنترنت IP بأكملها. يمكن التأكّد من أنّ حزمة البيانات المستقبلة قد أرسلت من قبل المرسل المفترض وبأنها لم تتعرّض للتحريف خلال نقلها عبر تفحّص قيمة هذا المجموع.

حمل التشفير المغلّف Encapsulation Security Payload (ESP): تشفيرٌ قويٌّ لحمل البيانات. يضمن وصول حزمة البيانات غير المشّفرة بشكلٍ صحيحٍ حماية محتويات هذه الحزمة. يتم تشفير الحزم باستخدام سرٍ مشتركٍ بين الأطراف المتصلة.

تبادل مفاتيح الإنترنت Internet Key Exchange (IKE): يوفّر أساليباً للتفاوض حول مفاتيح التشفير وتبادلها.

بروتوكول IPSEC في الشبكات اللاسلكية

يتطلّب بروتوكول IPSEC توفّر إمكانيّة التوجيه في جميع الأطراف المتصلة ضمن الشبكة اللاسلكية. إذا أردت تطبيق بروتوكول IPSEC تجنّب استخدام ترجمة عناوين الشبكة NAT واستخدم الجدران الناريّة Firewalls الكاملة عوضاً عنها.

يؤدّي تغليف حزم بروتوكول الإنترنت أيضاً إلى زيادة الحمل الزائد ضمن هذه الحزم، لذلك ننصحك باستخدام IPSEC جنباً إلى جنب مع تقنيّات الضغط للحفاظ على أداء الشبكة.

يحتاج بروتوكول IPSEC إلى تصميمٍ جيّدٍ لإدارة مفاتيح التشفير. يعتبر استخدام مفاتيح التشفير المتماثلة الأسلوب الأمثل لتوزيع مفاتيح التشفير في الحالات التي يكون عدد الأطراف التي ستتصل ببعضها البعض محدوداً. إلا أنّه في هذه الحالة لا يمكن ضمان أمن المعلومات بشكلٍ تام.

يمكنك إذا أردت بناء الشبكات الخاصّة الإفتراضيّة VPNs ضمن شبكتك اللاسلكية أن تستخدم الشبكات الخاصّة الإفتراضيّة على مستوى التطبيقات Application Layer VPNs. تستخدم هذه الشبكات عادةً أقنية UDP بالإضافة إلى بروتوكول SSL للتشفير.

للحصول على مزيدٍ من المعلومات عن الشبكات الخاصّة الإفتراضيّة على مستوى التطبيقات راجع الموقع التالي على شبكة الإنترنت:

http://www.openvpn.org

5.مستوى النقل Transport Layer

يدعم مستوى النقل Transport Layer نقل حزم بروتوكول الإنترنت IP بين العمليّات (الخدمات Services) باستخدام البوابات Ports (أرقام). بوابة TCP هي وصلةٌ إفتراضيّةٌ تقوم بربط سيلٍ من البيانات مع عمليةٍ معيّنةٍ Process.

1.6. بروتوكول التحكّم بالنقل Transmission Control Protocol (TCP)

بروتوكول التحكّم بالنقل Transmission Control Protocol (TCP) هو بروتوكول لنقل المعلومات مبني على الوصلة Connection-Oriented يوفّر النقل الموثوق للبيانات بين عمليتين Processes. يضمن هذا البروتوكول وثوقية نقل البيانات عبر تطبيق آليّات التحكّم بسيل البيانات Flow Control وتصحيح الأخطاء وتصحيح الأخطاء Error Correction.

يتم التحكّم بسيل البيانات بين المرسل والمستقبل باستخدام النوافذ متغيرة الحجم Sliding Windows، قواعد تغيير حجم النافذة Window Size Adjustment Heuristics وخوارزميّات تجنّب الإزدحام Congestion Avoidance Algorithms. تضمن هذه الآليّات الثلاث التوزيع العادل لموارد الناقل المشترك على جميع جلسات الإتصال Sessions الفعّالة.

تتألّف آليّة تصحيح (أو التحكّم) الخطأ في بروتوكول TCP من رسائل تأكيد الإستلام Acknowledgement المرسلة لكل حزمة تم استلامها بنجاح، كما تتحكّم هذه الآليّة بإعادة إرسال حزم البيانات في حين لم يتم استلامها بشكلٍ صحيح.

يلائم بروتوكول TCP التطبيقات التي تحتاج إلى نقل البيانات بشكلٍ موثوق (مثل SMTP، FTP، HTTP وغيرها).

2.6. بروتوكول بيانات المستخدم User Data Protocol (UDP)

يوفّر بروتوكول بيانات المستخدم User Data Protocol (UDP) (وهو أحد بروتوكولات طبقة النقل Transport Layer) خدمة نقل البيانات بالجهد الأقصى Best Effort. لا يمكن الوثوق بهذه الخدمة لأنّها لا توفّر الحماية من النسخ المتعددة لحزم البيانات أو ضياع هذه الحزم. لا يحتوي بروتوكول UDP على أيّة آليّاتٍ للتحكّم بسيل البيانات أو تصحيح الأخطاء. يعتبر المجموع الخاص لحمل البيانات Checksum الأسلوب الوحيد المستخدم في بروتوكول UDP للتحقق من سلامة البيانات المنقولة. يقوم المستقبل لدى اكتشافه لحزمة بياناتٍ تالفةٍ بإهمال هذه الحزمة دون أن يحاول أن يطلب من المرسل إعادة إرسالها.

يلائم بروتوكول UDP تطبيقات الزمن الحقيقي Real Time Applications (RTA) حيث تعتبر سرعة نقل البيانات أكثر أهميّةً من وثوقية خدمة النقل.

الخصائص	UDP	TCP
جودة الخدمة QoS	الجهد الأقصى، غير موثوقة	خدمة موثوقة

الوصلة	لا يعتمد على الوصلة Connection-less	يعتمد على الوصلة Connection-Oriented
تأكيد الإستلام	غير موجود	يتم تأكيد إستلام جميع البيانات
إعادة الإرسال	غير موجود	تتم إعادة إرسال البيانات المفقودة تلقائيّاً
التحكّم بسيل البيانات	غير موجود	النوافذ متغيرة الحجم Sliding Windows، تعديل حجم النافذة، تجنّب الإزدحام
الحمل الإضافي	منخفض جدّاً	منخفض لكنّه أكبر من بروتوكول UDP
سرعة الإرسال	مرتفعة جدّاً	مرتفعة لكنّها أقل من بروتوكول UDP
ملائم لـــ:	1.عندما تكون سرعة نقل البيانات أكثر أولويةً من الوثوقيّة 2.نقل حزم البيانات الصغيرة 3.عند استخدام البث Broadcast أو الإرسال لعدة أطراف Multicast	غالبيّة البروتوكولات

جدول 3: مقارنة بين خصائص بروتوكولي TCP و UDP

الفروقات بين بروتوكولي TCP و IEEE 802.11 MAC

من الجدير بالذكر أنّ بروتوكول TCP لا يعمل بالشكل الأمثل ضمن الشبكات اللاسلكية IEEE 802.11 وقد أجريت عدّة أبحاثٍ لتحسين أدائه.

1. يضمن بروتوكول IEEE 802.11b MAC والمعروف أيضاً بإسم أسلوب الوصول إلى القناة CSMA/CA إحتماليّةً متساويةً طويلة المدى للوصول إلى القناة لجميع المستخدمين، مما يعني أنه في حال كون سرعة نقل البيانات لأحد المستخدمين بطيئةً قد يؤدّي ذلك إلى التأثير سلباً على المستخدمين ذوي السرعات المرتفعة.
2. يفترض بروتوكول TCP أن ضياع الحزم ناتجٌ عن الإزدحام ضمن الشبكة. لا يستطيع هذا البروتوكول التمييز بين **التلف و الإزدحام**، مما يؤدّي إلى تخفيض حجم النافذة دون مبرر وينتج بالتالي سرعةً منخفضةً لنقل البيانات وتأخيراً طويلاً.

تبلغ السرعة القصوى التي يمكن تحقيقها عمليّاً في الشبكات اللاسلكية 802.11b نتيجة الحمل الإضافي لبروتوكول CSMA/CA حوالي 5.9 ميغابت في الثانية (للوصلات بين نقطتين PtP) عبر بروتوكول TCP و 7.1 ميغابت في الثانية عبر بروتوكول UDP.

ننصحك بشدّة أن تقوم بتصميم الشبكة اللاسلكية لتكون "متناظرةً قدر الإمكان". حاول ترتيب النقاط بحيث تستمع لبعضها البعض وبحيث تستخدم قدرات إرسالٍ فعّالةٍ متماثلةٍ.

قم بتشغيل بعض آليّات تشذيب سيل البيانات ضمن الموجّهات الطرفية. تتيح هذه الآليّات إمكانيّة التحكّم بالإزدحام ضمن البروتوكول TCP وتساعد على توزيع موارد عرض الحزمة بشكلٍ عادلٍ. للمزيد من المعلومات راجع: http://www.ieee-infocom.org/2003/papers/21_01.PDF

3.6. الجدران الناريّة ضمن الطبقة الثالثة Layer 3 Firewalls

يتم استخدام الجدران الناريّة ضمن طبقة النقل للتحكّم بحركة البيانات ضمن الشبكة عبر إغلاق منافذ بروتوكولي TCP أو UDP. بما أنّ غالبيّة التطبيقات تستخدم بواباتٍ "معروفة Well known ports" أثناء الإتصال لذلك يمكن استخدام تصفية حزم البيانات Packet Filtering مثلاً لإيقاف تطبيقات بروتوكول نقل الملفّات FTP (البوابة 20) أو Telnet (البوابة 23) أو بروتوكول نقل الرسائل البسيط SMTP (البوابة 25).

هناك استراتيجيتين مختلفتين لاستخدام الجدران الناريّة ضمن طبقة بروتوكول TCP: إمّا أن يتم إغلاق جميع البوابات وفتح البوابات التي ستحتاجها فقط أو أن يتم فتح جميع البوابات ومن ثمّ إغلاق البوابات التي قد تشكّل تهديداً لأمن الشبكة فقط. يعتبر الخيار الأكثر محدوديّةً والذي يعتمد على إغلاق جميع البوابات غير الضروريّة الحل الأكثر أمناً.

تستخدم الجدران الناريّة مزيجاً من ثلاثة أساليب أساسيّة:

- إيقاف حركة البيانات الصادرة من النوع X
- إيقاف حركة البيانات الواردة من النوع Y
- إعادة توجيه البيانات من النوع Z

تعني إعادة توجيه البيانات بأنّ الجدار الناري سيقوم بتمرير جميع الوصلات الواردة إلى بوابةٍ معيّنةٍ إلى حاسبٍ آخر وبوابةٍ أخرى ضمن الشبكة. تؤدّي إعادة توجيه البيانات إلى فتح ثغرةٍ في الجدار الناري لأدّك ستسمح لحزم البيانات الواردة بدخول الشبكة. الغايات الأساسيّة لإعادة توجيه البوابات هي:

- لتوفير خدمةٍ خارجيّةٍ من حاسبٍ يقع ضمن الشبكة المحميّة بالجدار الناري
- لتوفير نفس الخدمة المتوفّرة ضمن حاسبٍ يقع ضمن الشبكة المحميّة بالجدار الناري عبر عدّة منافذ بهدف توزيع حمل البيانات Load Balancing

تصميم الجدران الناريّة

تعتبر الجدران الناريّة عنصراً أساسيّاً في الشبكات اللاسلكية، فهي قادرةٌ على منع البرمجيّات الضارّة من دخول الشبكات اللاسلكية وتساعدنا على اختيار الخدمات التي نرغب بإتاحتها لمستخدمي الشبكة. يجب النظر إلى الشبكة اللاسلكية على أنّها مصدرٌ "محدودٌ" وبالتالي يتطلّب تحديد أولويات الخدمات المقدّمة.

ينبغي أن يحتوي التصميم الجيّد للشبكة اللاسلكيّة على جدارٍ ناريٍّ، تشذيب سيل البيانات والمراقبة. يتم كشف غالبيّة الأعطال في الشبكات اللاسلكية عبر (1) كشف، (2) تفحّص و(3) إزالة البرمجيّات الضارّة التي تستهلك موارد الشبكة.

يمكننا على سبيل المثال في حال أردنا استخدام برمجيّات الند للند Peer-to-Peer تخصيص مجموعةٍ محددةٍ من موارد عرض الحزمة لهذه البرمجيّات.

7.مستوى التطبيقات Application Layer

تتجلّى المهمّة الأساسيّة لمستوى التطبيقات في ضمان توفّر الإتصال الفعّال مع البرمجيّات التطبيقيّة الأخرى ضمن الشبكة. ينبغي عليك التمييز بين مستوى التطبيقات والتطبيقات ذاتها، فمستوى التطبيقات هو مجرّد مستوى لتوفير الخدمة يقدّم الخدمات التالية:

1. تحديد الطرف الآخر للإتصال والتأكّد من جاهزيته
2. التحقق من الهويّة (الرسالة، المرسل، المستقبل)
3. تحديد الموارد المطلوبة للإتصال
4. ضمان إتفاق المرسل والمستقبل على إجراءات تصحيح الأخطاء، كمال البيانات والسريّة

5.تحديد البروتوكول وقواعد ترتيب البيانات على مستوى التطبيقات

من أكثر بروتوكولات مستوى التطبيقات استخداماً هذه الأيام بروتوكول النقل التشعبي الآمن HTTPS، بروتوكول نقل الرسائل البسيط SMTP، بروتوكول البريد الإلكتروني IMAP/POP3، بروتوكول نقل الملفّات FTP، بروتوكولات الإتصالات الفوريّة Messengering Protocols وبروتوكولات الزمن الحقيقي RTP.

1.7. الجدران الناريّة ضمن مستوى التطبيقات Application Firewalls

تعمل الجدران الناريّة التي قمنا بدراستها حتى الآن ضمن طبقتي الشبكة والنقل. يمكن باستخدام هذه الجدران الناريّة:

- منع أو السماح بتمرير البيانات الواردة من عنوان إنترنت IP محدد
- منع أو السماح بتمرير البيانات الصادرة إلى عنوان إنترنت IP محدد
- منع أو السماح بتمرير البيانات الواردة أو الصادرة عبر بوابة TCP أو UDP محددة

لا تستطيع هذه الجدران النارية تفحّص محتوى البيانات ضمن الحزم وبالتالي منع تمرير هذه الحزم بناءً على محتوياتها. لتحقيق هذا الهدف يتوجّب عليك القيام بتصفية البيانات على مستوى التطبيقات.

مصفاة مستوى التطبيقات Application Layer Filter (ALF)

تقوم مصفاة مستوى التطبيقات ALF بكشف المعلومات غير الطبيعية ضمن ترويسة الرسالة والبيانات الموجودة ضمنها. يمكن إعداد هذه المصفاة للبحث عن عباراتٍ معيّنةٍ ضمن البيانات لمنع تمرير الرسالة بناءٍ على هذه المعلومات. تمكّن هذه الخصائص مصفاة مستوى التطبيقات ALF من تجنّب ما يلي:

- إغراق الذاكرة المؤقتة Buffer Overflow لبروتوكولات POP3، SMTP و DNS.
- هجمات مخدّمات الوب المعتمدة على المعلومات المضمّنة في ترويسة أو طلبات بروتوكول HTTP.
- البرمجيّات الضارّة المخفية ضمن أقنية SSL.
- منع تمرير بيانات التطبيقات التي تعتمد على بروتوكول HTTP (مثل الرسائل الفوريّة Messengering).
- منع المستخدمين الداخليين من نشر المعلومات الحساسة.

يمكن لمصفاة مستوى التطبيقات ALF أيضاً أن تقوم بمنع تمرير بعض الأوامر المحددة ضمن بروتوكولات مستوى التطبيقات. يمكن على سبيل المثال منع أمر GET في بروتوكول النقل التشعبي HTTP في حين يسمح بتمرير الأمر POST.

تتجلى مساوئ مصفاة مستوى التطبيقات ALF الأساسيّة في تأثيرها السلبي على الأداء نتيجة تفحّص جميع البيانات المارّة عبر الشبكة. كما أنّ استخدام هذه المصفاة يعني إمكانيّة تحليل البيانات الشخصيّة في الزمن الحقيقي مما يجعلها موضع تساؤلٍ فيما يتعلّق بأخلاقيّات هذا الإستخدام.

تتطلّب هذه الميزة تجهيزاتٍ أكثر قدرةً من تلك المستخدمة في الجدران الناريّة التقليديّة والتي تعتمد على تصفية حزم البيانات مما يؤثّر بالتالي على كلفة هذه الخدمة.

من المخاطر الناجمة عن التعقيد الناتج عن استخدام مصفاة مستوى التطبيقات ضمن الشبكة إمكانيّة الإعداد الخاطئ لهذه المصفاة مما قد يتسبب في منع تمرير البيانات بشكلٍ خاطئٍ أيضاً.

مصفاة مستوى التطبيقات Application Layer Filter

تعتبر البرمجيّات المضادة للفيروسات Anti-Virus والبرمجيّات المضادة للرسائل التجاريّة المرسلة عشوائيّاً Anti-Spam إحدى التطبيقات المشتقّة من مصفاة مستوى التطبيقات ALF. بإمكان الأنظمة المضادة للفيروسات أو الرسائل التجاريّة المرسلة عشوائيّاً أن تتفحّص محتويات البرنامج ومنع تمرير أو وضع علامةٍ على ملحقات البريد الإلكتروني المشبوهة.

يتوجّب عليك عند تصميم الشبكات اللاسلكية أن تفكّر بتركيب مصافي مستوى التطبيقات هذه. تشكّل الرسائل التجاريّة المرسلة عشوائياً SPAM حاليّاً حوالي 30–50% من مجمل حركة بروتوكول نقل الرسائل البسيط SMTP. يمكنك باستخدام برمجيّات كشف هذه الرسائل وتدريب المستخدمين على تشغيل بروتوكول IMAP في برمجيّات قراءة البريد الإلكتروني أن تتجنّب تمرير الرسائل المرسلة عشوائيّاً عبر وصلاتك اللاسلكية.

من مصافي مستوى التطبيقات الأخرى التي قد ترغب باستخدامها مخدّم الوكيل Web Proxy Server. يستخدم هذا المخدّم للإحتفاظ المؤقت بالبيانات التي تتكرر زيارتها باستمرار ضمن ذاكرة القراءة فقط RAM بالإضافة إلى حفظ نتائج طلبات ترجمة عناوين النطاق DNS.

8. الخلاصة

من أهم ميزات نموذج OSI المعياري ونموذج الإنترنت أنّها يضمنان إمكانيّة عمل كل طبقةٍ من البروتوكولات بشكلٍ مستقلٍ عن الطبقات الأخرى، مما يعطي مرونةً في تغيير الطبقة الفيزيائيّة المستخدمة ونقل التطبيقات من الشبكة السلكية إلى الشبكة اللاسلكية. تتيح لنا هذه النماذج أيضاً توصيف التفاعلات بين طبقات (مكونات) شبكة الإتصالات بشكلٍ أفضل.

يعتمد توفير جودة الخدمة الأمثل لمستخدمي الشبكة اللاسلكية على الإعداد الحكيم **لجميع طبقات البروتوكولات** والتصميم الجيّد لبنية الشبكة. يتوجّب عليك أثناء تصميم الشبكات اللاسلكية ألا تقلل من أهميّة الآليّات المتوفّرة ضمن مستويات الشبكة، النقل والتطبيقات في تحسين أداء هذه الشبكات.

تتطلّب مهمة زيادة البيانات المفيدة في حزم البيانات Useful Bits إلى الحد الأقصى استيعاب أثر كل مستوى من المستويات على الأداء الكلّي للشبكة.

يمكن تلخيص الأمور الأربع الرئيسية التي ينبغي عليك تذكرها من هذه الوحدة بما يلي:

1. من السهل جداً بناء الشبكات اللاسلكية البدائيّة، إلا أنّ بناء الشبكات اللاسلكية ذات الأداء الجيّد ليس بالأمر السهل على الإطلاق.
2. تعتبر زيادة البيانات المفيدة المنقولة ضمن حزم البيانات في كل مستوى إلى الحد الأقصى (أي تقليل الحمل الإضافي Overhead) عاملاً أساسيّاً في تصميم أيّ شبكة.
3. لن تستطيع تحديد المواقع التي يمكن تحسينها إلا بقياس أداء الشبكة.
4. يتطلّب بناء الشبكات اللاسلكية الجيّدة في الحالات المعقّدة كثيراً من الخبرة، لكن ذلك لا ينبغي أن يثنيك عن المحاولة. إنضم إلى منتديات الحوار على الإنترنت وشارك تجاربك مع الآخرين.