التشبيك المتقدم

إعداد: Alberto Escudero Pascual
النسخة العربية أنس طويلة

الأهداف

- إستيعاب جوانب التشبيك "التي قدتؤثر على الأداءالكلي للشبكة اللاسلكية
- إستيعاب التفاعلات بين IEEE 802.11)الطبقة الفيزيائية / الوصلة(مع TCP) طبقةالنقل(
- التمكن من تحسين أداء الشبكة

المحتويات

- منهجية الوحدة
- **OSI** في مقابل الإنترنت **(TCP/IP)**
- الطبقة الفيزيائية **MAC /**
  - مستوى الوصول إلى الناقل **Media Access Layer**، التحكم بالأخطاء، العناوين الفيزيائية **MAC** والتشفير
- طبقة الشبكة
  - عناوين الإنترنت **IP Addressing**، التحكم بالأخطاء **Error Control**، التوجيه **Routing**، ترجمة عناوين الشبكة **NAT**، أقنية بروتوكول الإنترنت **IP Tunnelling ،IPSec**
- طبقة النقل
  - **UDP ،TCP**، الجدران النارية في الطبقة الثالثة
- طبقة التطبيقات
  - الوكيل **Proxy**، الجدران النارية **Firewalls**

المنهجية

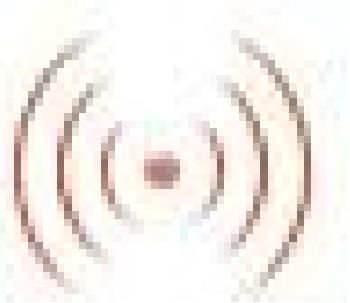
- الإنتقال ضمن "كدسة" البروتوكولات
- من الأسفل باتجاه الإعلى
- ركز على "المفاهيم" لا على خصوصيات التركيب
- حدد العوامل "الأساسية" التي يجب الإنتباه إليها عند تصميم الشبكة

المنهجية

هذه الوحدة ليست:

- سحراً
- بديلاً عن أسابيع عدة من التدريب على التشبيك
- تدريباً على كيفية تطبيق كل من العوامل "الأساسية" التي يجب أخذها بعين الإعتبار

الشبكات اللاسلكية



OSI في مقابل TCP/IP

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

التحكم بالوصول إلى الناقل

- الطبقة الفيزيائية
  - تقنيات الترميز، ترميز البتات، الوصول الفيزيائي إلى الناقل المشترك
  - RS-232, V. 35, 10BaseT, ISDN
- طبقة الوصلة
  - العنونة وتوصيل الحزم من حاسب (مضيف) إلى آخر عبر قناة نقل مشتركة
  - Ethernet (IEEE 802.3) , PPP , ATM

مستوى الوصول إلى الناقل

- IEEE 802.11 (WLAN)
- الطبقة الفيزيائيّة وطبقة الوصلة
- بروتوكولات الطبقة الفيزيائية
- IrDA
- Spread Spectrum
- FHSS, DSSS, OFDM

بروتوكولات التحكم بالأخطاء

- CSMA/CD
- Aloha, Ethernet
- CSMA/CD وCSMA/CA
- IEEE 802.11 (WLAN)
- TDD, CSMA/CA (RTS/CTS)
- IEEE 802.16 (WMAN)
- TDMA, DAMA

العنونة الفيزيائية MAC Addressing

- تسلسل فريديحتوي على 48 بتاً
- مثبت ضمن التجهيزات ولكن يمكن تغييره بسهولة

- إستخدام العناوين الفيزيائية للتحقق من الهوية
- غير آمن

تشفير وصلة البيانات

- تأمين البيانات ضمن مستوى الوصلة أثناء انتقالها بين نقطتين متصلتين بنفس الوصلة الفيزيائية
- خوارزمية تشفير وسر مشترك
- تتطلب وجود حواسب وسيطة مأمونة الجانب

- WEP (أمن ضعيف)
- WPA, WPA2
- لا يوفر تأمين البيانات من البداية إلى النهاية

OSI في مقابل TCP/IP

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

مستوى الشبكة (IP)

- عنوان الإنترنت IP
- التوجيه، تحديد المضيف، الجدار الناري
- الشبكات الفرعية
- قناع الشبكة، الفئات

- الشبكات الفرعية هامة جداً
- كشف الأعطال
- محاول ألا تتجاوز 32-64 حاسب في كل شبكة فرعية

التحكم بالأخطاء في بروتوكول الإنترنت IP

- ICMP
- الإعلام بالمشاكل التي تمنع توصيل البيانات (لا يمكن الإتصال بالوجهة Destination Unreachable)
- كشف أعطال الشبكات (تعليمة Ping)

- حركة كبيرة لرسائل ICMP؟
- الفيروسات وأحصنة طروادة

التوجيه Routing

- التوجيه إعتماداً على الوجهة أو المصدر
- التوجيه المسيس

- عنوان الإنترنت IP للمصدر لإتخاذ قرار التوجيه
- توزيع الحمل

ترجمة عناوين الشبكة NAT

- شح عناوين الإنترنت IP العامة
- الجدران النارية / المنطقة منزوعة السلاح DMZ
- توزيع حمل البيانات
- توزيع حمل المعالجة

التقنيع SNAT

- إعادة كتابة عنوان المصدر
  - يعمل الموجّه بالنيابة عن الآخرين
- جدار ناري بسيط
- يحد من إمكانية إتصال الحواسب الموجودة ضمن الشبكة بالخدمات الخارجية

ترجمة عناوين الوجهة DNAT

- إتاحة خدمة متوفرة ضمن الشبكة الداخلية للمستخدمين خارج هذه الشبكة
- إعادة كتابة عنوان الوجهة لحزم البيانات

- توفر الخدمات
- يؤثر على توجيه حزم البيانات
- إعادة توجيه طلبات الوصول إلى الإنترنت
- عمليات تسجيل الدخول

IP Tunnelling أقنية بروتوكول الإنترنت

- نقل حزم بروتوكول الإنترنت ضمن حزم أخرى
- تتطلب أن تكون نهايات القناة قابلة للتوجيه
- لا توفر أية حماية إضافية للبيانات ما لم تكن الحزم المغلفة (الحزم المنتقلة ضمن القناة) مشفرة

IP Tunnelling أقنيةبروتوكولالإنترنت

- يعرف تضمين حزمالبيانات في حزم مشفرة بإسم:
  - الأقنية الآمنة أوالشبكات الخاصة الإفتراضية VPN
- يعتبر بروتوكول التشفير IPSEC أكثرأساليب بناء أقنيةبروتوكول الإنترنت الآمنة شيوعاً

IPSec

- يضمن أمن البيانات على مستوى بروتوكول الإنترنت IP
- يوفر الحماية التالية:
  - السرية Confidentiality
  - التحقق من الهوية Authentication
  - الكمال Integrity
- ثلاثة بروتوكولات أساسية:
  - AH, ESP, IKE

IPSec

- جدران نارية كاملة عوضاً عن استخدام NAT
- إستخدم IPSec معتقنيات الضغط

فكر باستخدام الشبكات الخاصة الإفتراضية العاملة ضمن مستوى التطبيقات

- راجع www.openvpn.org

OSI في مقابل TCP/IP

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

مستوى النقل

- نقل حزم بروتوكول الإنترنت IP بين العمليات (الخدمات Services) باستخدام البوابات Ports
- البوابة هي وصلة إفتراضية تقوم بربط سيل من البيانات مع عملية معينة Process

بروتوكول TCP

- مبني على الوصلة Connection-Oriented
- نقل موثوق للبيانات
  - رسائل تأكيد الإستلام Acknowledgements
- التحكم بسيل البيانات Flow Control
  - النوافذ متغيرة الحجم Sliding Windows
  - حجم النافذة Window Size
  - تجنب الإزدحام Congestion Avoidance

TCP في مقابل UDP

الخصائص	UDP	TCP
جودة الخدمة QoS	الجهد الأقصى، غير موثوقة	خدمة موثوقة
تأسيس الوصلة	لا	نعم
تأكيد الإستلام	لا	نعم
إعادة الإرسال	لا	نعم
التحكّم بسيل البيانات	لا	النوافذ متغيرة الحجم، تعديل حجم النافذة، تجنّب الإزدحام
الحمل الإضافي	منخفض جداً	منخفض لكنّه أكبر من بروتوكول UDP
ملائم لـــ:	أولوية لسرعة نقل البيانات، حزم البيانات الصغيرة، البث Broadcast أو الإرسال لعدة أطراف Multicast	غالبيّة البروتوكولات

TCP و IEEE 802.11 MAC

- لا يعمل بروتوكول TCP بالشكل الأمثل ضمن الشبكات اللاسلكية IEEE 802.11
- الحالة الأولى: الكثير من النقاط ذات سرعة منخفضة لنقل البيانات
- الحالة الثانية: حزم البيانات التالفة ضمن الشبكة اللاسلكية

الجدران الناريةضمن الطبقة الثالثة

- إيقاف حركةالبيانات الصادرةمن النوع X
- إيقاف حركةالبيانات الواردةمن النوع Y
- إعادة توجيهالبيانات من النوع Z
  - لتوفير خدمة خارجيةمنحاسب يقع ضمن الشبكة المحميةبالجدار الناري
  - لتوفيرنفس الخدمة المتوفرةضمنحاسب يقع ضمن الشبكة المحميةبالجدار الناري عبر عدة منافذبهدف توزيع حملالبيانات Load Balancing

تصميم الجدران النارية

- أساسي في الشبكات اللاسلكية
- تشذيب سيل البيانات والمراقبة
- كشف، منع وإزالة البرمجيات الضارة التي تستهلك موارد الشبكة

OSI في مقابل TCP/IP

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

مستوى التطبيقات

- تحديدالطرف الآخر للإتصال والتأكدمن جاهزيته للإتصال
- التحقق من الهوية) الرسالة، المرسل،المستقبل(
- تحديد الموارد المطلوبةللإتصال
- ضمان إتفاق المرسل والمستقبل على إجراءات تصحيح الأخطاء،كمال البيانات والسرية
- تحديدالبروتوكول وقواعدترتيب البيانات على مستوى التطبيقات

الجدران النارية ضمن مستوى التطبيقات

تمنع:

- إغراق الذاكرة المؤقتة Buffer Overflow ببروتوكولات POP3، SMTP و DNS
- هجمات مخدمات الوب المعتمدة على المعلومات المضمنة في ترويسة أو طلبات بروتوكول HTTP
- البرمجيات الضارة المخفية ضمن أقنية SSL
- منع تمرير بيانات التطبيقات التي تعتمد على بروتوكول HTTP (مثل الرسائل الفورية Messengering)
- منع المستخدمين الداخليين من نشر المعلومات الحساسة

الجدران النارية ضمن مستوى التطبيقات

المساوئ:

- التأثير السلبي على الأداء
  - الكلفة المرتفعة
  - الإعداد الخاطئ

الجدران النارية ضمن مستوى التطبيقات

- البرمجيات المضادة للفيروسات Anti-Virus والبرمجيات المضادة للرسائل التجارية المرسلة عشوائياً Anti-Spam
  - منع تمرير أو وضع علامة على المحتويات المشبوهة
- تشكل الرسائل التجارية المرسلة عشوائياً SPAM حالياً حوالي 30-50% من مجمل حركة بروتوكول نقل الرسائل البسيط SMTP
- مخدم الوكيل Web Proxy Server
- الإحتفاظ المؤقت بالبيانات التي تتكرر زيارتها باستمرار ضمن ذاكرة القراءة فقط RAM
- حفظ نتائج طلبات ترجمة عناوين النطاق DNS

التشبيك المتقدم في الشبكات اللاسلكية يعني

- الإعداد الحكيم لجميع طبقات البروتوكولات
- التصميم الجيد لبنية الشبكة
- الهدف:
  - زيادة البيانات المفيدة في حزم البيانات Useful Bits إلى الحد الأقصى

الخلاصة

- من السهل جداً بناء الشبكات اللاسلكية البدائية
- بناء الشبكات اللاسلكية ذات الأداء الجيد ليس بالأمر السهل على الإطلاق
- القياس ثم القياس ثم القياس!
- لا تتوقف عن المحاولة! شارك تجاربك مع الآخرين.

سؤال للمناقشة

كيف يمكننا تحسين أداء شبكة لاسلكية تستخدم لنقل الصوت عبر بروتوكول الإنترنت VoIP؟

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