Soluciones Wireless

para el turismo

WiFi (Wireless-Sin cables):

- El cliente sin WiFi en su ordenador necesita instalar una tarjeta PCMCIA con todos los controladores y drivers y un CD-Rom, con todos los problemas que ello puede implicar si esta tarea no la hace un profesional informático.

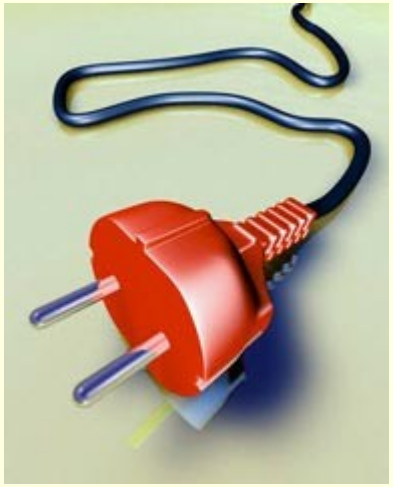
ADSL/VDSL:

- Conectividad por la red telefónica, lo que implica una duplicación del panel teléfonico, costes de servicio,
- Disponibilidad de internet solo en el punto donde está el teléfono en la habitación (normalmente en la mesita de noche),
- Instalación muy costosa y que implica muchos extras, como la instalación de filtros si en las habitaciones hay otras tomas telefónicas y se desean eliminar las interferencias del teléfono.

PLC (Power Line Comunications),

también denominada BPL (Broadband over Power Lines)

- Es una tecnología basada en la transmisión de datos utilizando como infraestructura la red eléctrica.
- Esto implica la capacidad de ofrecer, mediante este medio, cualquier servicio basado en IP, como podría ser telefonía IP, Internet, videovigilancia, videoconferencia, datos a alta velocidad, etc..



Tipos principales de PLC

- PLOC (Power Line Outdoors Telecoms)
  - comunicaciones extrahogareñas utilizando la red eléctrica. la comunicación entre la subestación eléctrica (denominada media tensión) y la red doméstica (denominada baja tensión).
- PLIC (Power Line Indoors Telecoms)
  - comunicaciones intrahogareñas utilizando la red eléctrica) la red eléctrica interior de la casa, para establecer comunicaciones internas.
- Todos los electro-modems y hardware PLC cumplen el estandar ETSI (European Telecommunications Standards Institute o Instituto de Estándares de Telecomunicación Europeos

Banda PLC

- La señal utilizada para transmitir datos a través de la red eléctrica suele ser de 1,6 a 30 Mhz, la cual difiere mucho de la frecuencia de la red eléctrica convencional (50 – 60 Hz)
- Tecnología de banda ancha: Velocidades de transmisión de hasta 45 Mbps en el tramo de la Baja Tensión (Domicilios) y de hasta 135 Mbps en el tramo de la Media Tensión.
- http://www.cibersuite.com/ suministrador soluciones

Satélite

- Permite el acceso a internet con velocidades de 2Mbits/s y superiores, con capacidad de recepción y transmisión para el usuario final.
- El servicio en su modalidad unidireccional utiliza un canal de bajada de alta velocidad por satélite y el retorno a través de redes terrestes convencionales.
- En la modalidad bidireccional, los dos sentidos de la comunicación se establecen por satélite

Zonas WIFI libres en el Hotel

- Un servicio para conseguir mayor grado de satisfacción para sus clientes.
- Atraerá a nuevos clientes que deseen en la habitación:
  - Enviar y recibir correos electrónicos.
  - Consultar páginas web en internet.
  - Traspasar datos a su empresa.
  - Actualizar y consultar su agenda personal.
- Es un servicio distintivo para competir con otros hoteles de la zona.

Wireless Interior

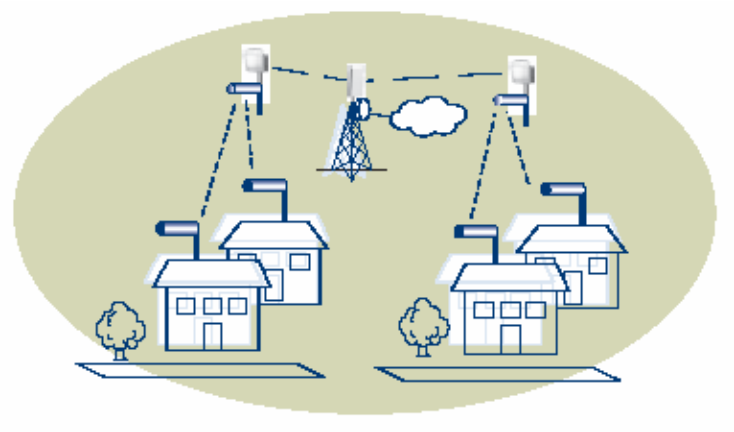
Wi Fi™
The Standard for Wireless Fidelity

Salas de conferencias

- Reuniones de empresas con conexión a internet y a sus oficinas.
- Permitirá conectar los portátiles de los clientes a los proyectores e impresoras del hotel para dar más servicios de valor añadido.

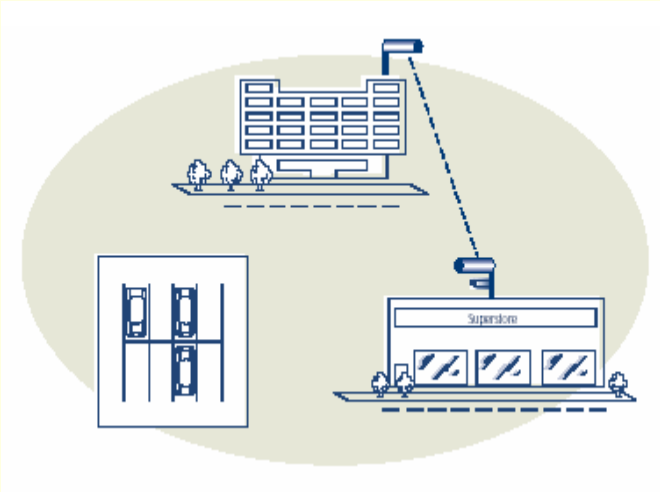
Casa Rurales

- Dotar de Internet y Telefonía vía satélite.



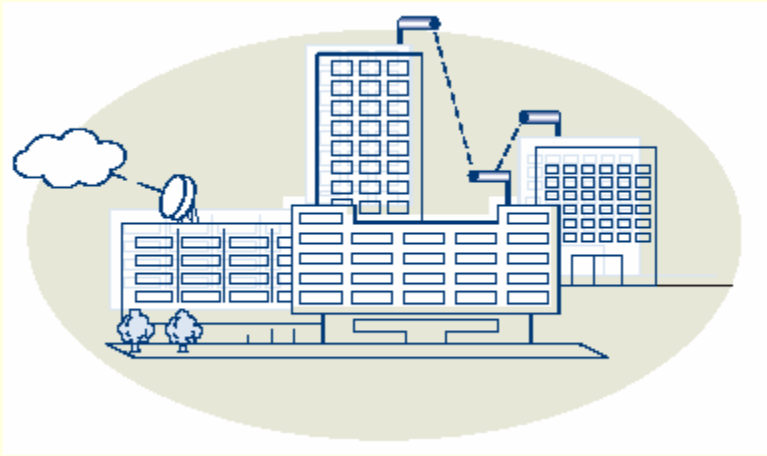
Wireless de medio alcance

- Servicios de vigilancia
- Sistema de vigilancia en las zonas del hotel sin tener que tirar cableados.
- Control de zonas de interior y exterior.
- Permite instalar cámaras hasta un radio de 10 kms.



Unión entre edificios

- Unión de edificios centralizando los datos a velocidades entre 8 y 36Mbs.
- Red inalámbrica entre los edificios creando una intranet privada.
- Sistemas de seguridad WAP, Radius, Mac y de autenticación.
- Soporta distancias hasta 10Kms..



Administración y Almacén

- Permitirá movilidad a las personas que controlan el almacén del hotel.
- Conexión a la gestión administrativa para:
  - Registrar entradas o salidas de almacén.
  - Inventarios “on-line” con dispositivos inalámbricos.

Beneficios Inalámbrico

- Fácil despliegue
- Movilidad
- Reutilización
- Bajo coste
- Simplicidad

Wireless Standard	802.11b		802.11a		802.11g	
Popularity		Widely adopted. Readily available everywhere.		New technology. Limited adoption.		New technology. Limited adoption, but rapid growth expected.
Speed	11 Mbps	Up to 11Mbps	54 Mbps	Up to 54Mbps (5X greater than 802.11b)	54 Mbps	Up to 54Mbps (5X greater than 802.11b)
Cost	$	Inexpensive	$$$	Expensive	$$	Moderate
Frequency	2.4 GHz	Crowded 2.4GHz band. May conflict with other 2.4GHz devices like cordless phones, microwave ovens, etc.	5 GHz	Uncrowded 5GHz band.	2.4 GHz	Crowded 2.4GHz band. May conflict with other 2.4GHz devices like cordless phones, microwave ovens, etc.
Range	100-150	Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.	25-75	Limited range. Typically no more than 25 to 75 feet indoors.	100-150	Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.
Public Access		The number of public "Hot Spots" is growing rapidly, allowing wireless connectivity in many airports, hotels, college campuses, public areas, and restaurants.	X	None at this time.		Compatible with current 802.11b "Hot Spots" (at 11Mbps)
Compatibility	OK 802.11b	Widest adoption Wi Fi	OK 802.11a	Incompatible with 802.11b or 802.11g	OK 802.11b 802.11g	Interoperates with 802.11b networks (at 11Mbps) Incompatible with 802.11a

802.11n

Año 2006/2007

- 540 Mbps

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard (1999)
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F - Inter-Access Point Protocol (2003)
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i - Enhanced security (2004)
- IEEE 802.11j - Extensions for Japan (2004)
- IEEE 802.11k - Radio resource measurement enhancements
- IEEE 802.11l - (reserved, typologically unsound)
- IEEE 802.11m - Maintenance of the standard; odds and ends.
- IEEE 802.11n - Higher throughput improvements
- IEEE 802.11o - (reserved, typologically unsound)
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
- IEEE 802.11q - (reserved, typologically unsound, can be confused with 802.1q VLAN trunking)
- IEEE 802.11r - Fast roaming
- IEEE 802.11s - ESS Mesh Networking
- IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics
- IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11v - Wireless network management
- IEEE 802.11w - Protected Management Frames

Modo infraestructura

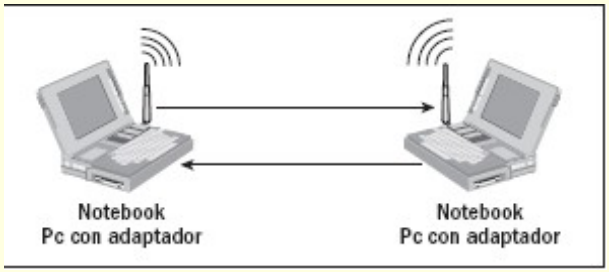
Modo infraestructure

- Extienden una red LAN
- Punto de Acceso (AP)
  - Puente entre la LAN y las estaciones inalámbricas
  - Identificados por su SSID
  - Todo el tráfico pasa a su través
  - Roaming: Posibilidad de que una estación se asocie a otros AP
  - Interfaz web para su configuración
  - Desplegando varios se puede cubrir un gran área
- Estaciones:
  - PCs, portátiles, PDAs, etc.

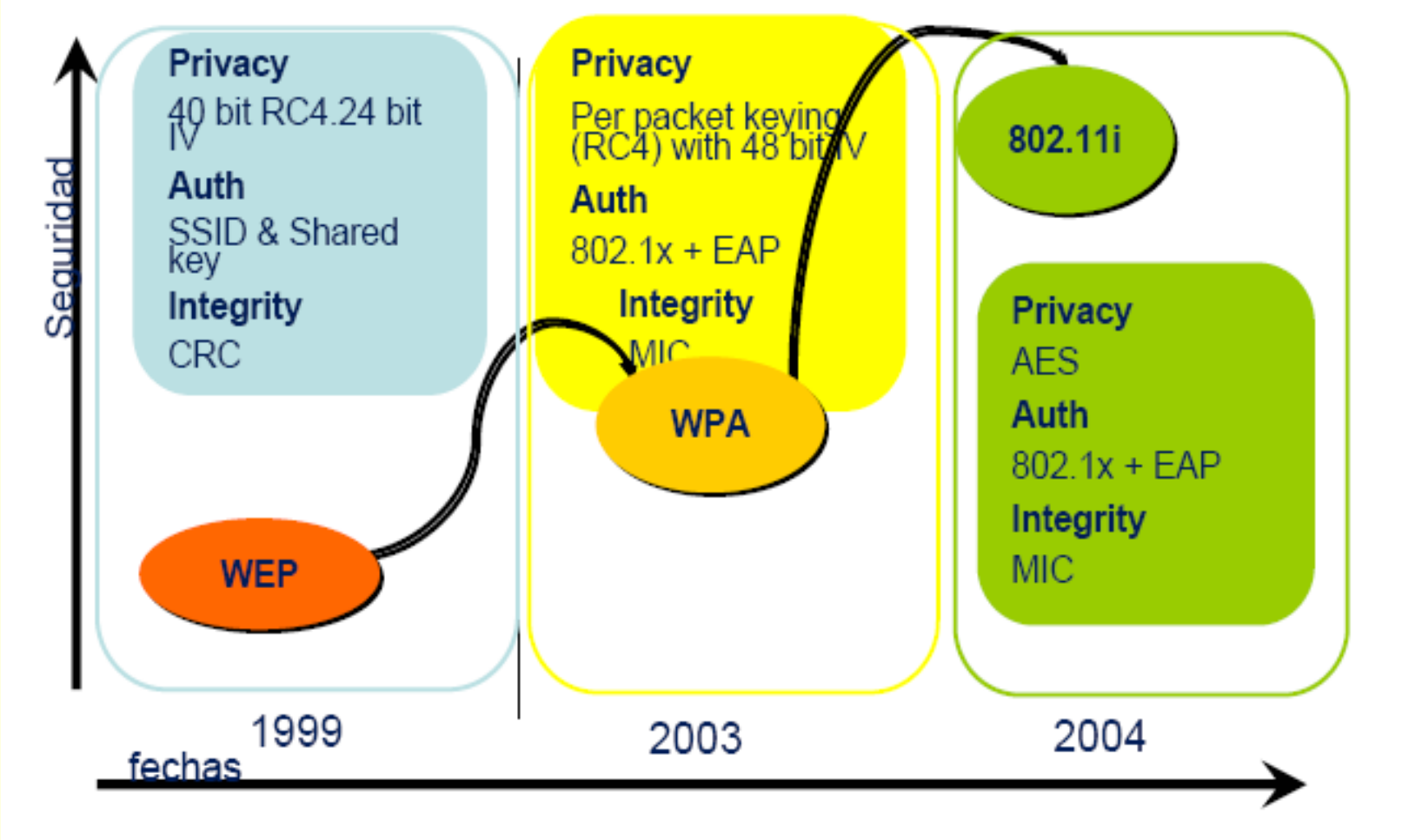
Ad hoc

Redes Ad hoc

- Sin controlador central ni AP
- Formada por las estaciones
- Sin acceso a otras redes
- Para acceder a Internet una estación deberá actuar como proxy y poseer dos interfaces de red



Evolución de seguridad



Fuente: G. Álvarez / P.P. Pérez (CSIC)

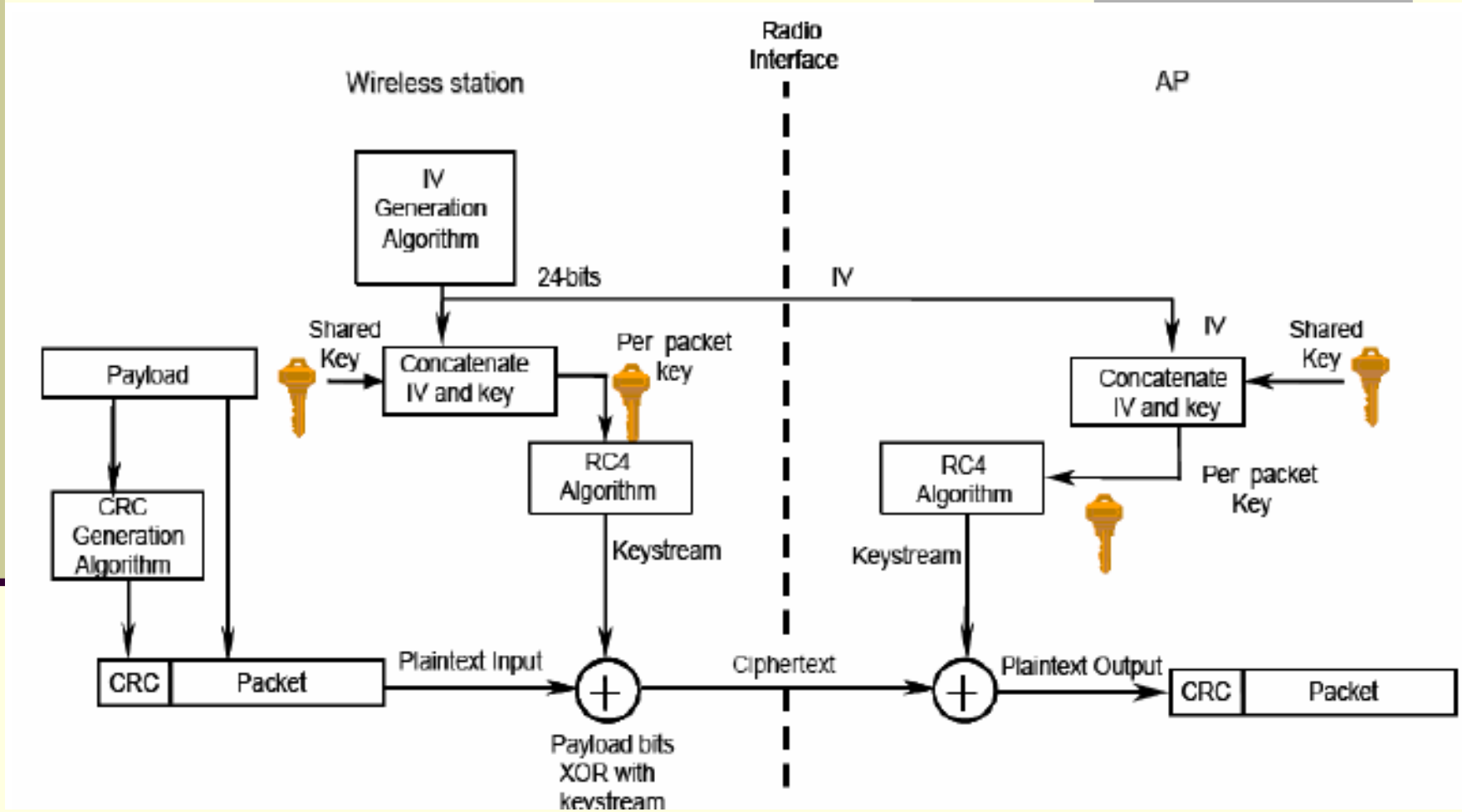
Seguridad WEP

- Todo el tráfico es accesible a un atacante
- Servicios de seguridad necesarios
  - Autenticación:
    - Identificación con un grado aceptable de confianza de los usuarios autorizados
  - Confidencialidad:
    - La información debe ser accesible únicamente a las personas autorizadas
  - Integridad:
    - La información debe mantenerse completa y libre de manipulaciones fortuitas o deliberadas, de manera que siempre se pueda confiar en ella
- ¡WEP no consigue ofrecer ninguno!

Problemas WEP

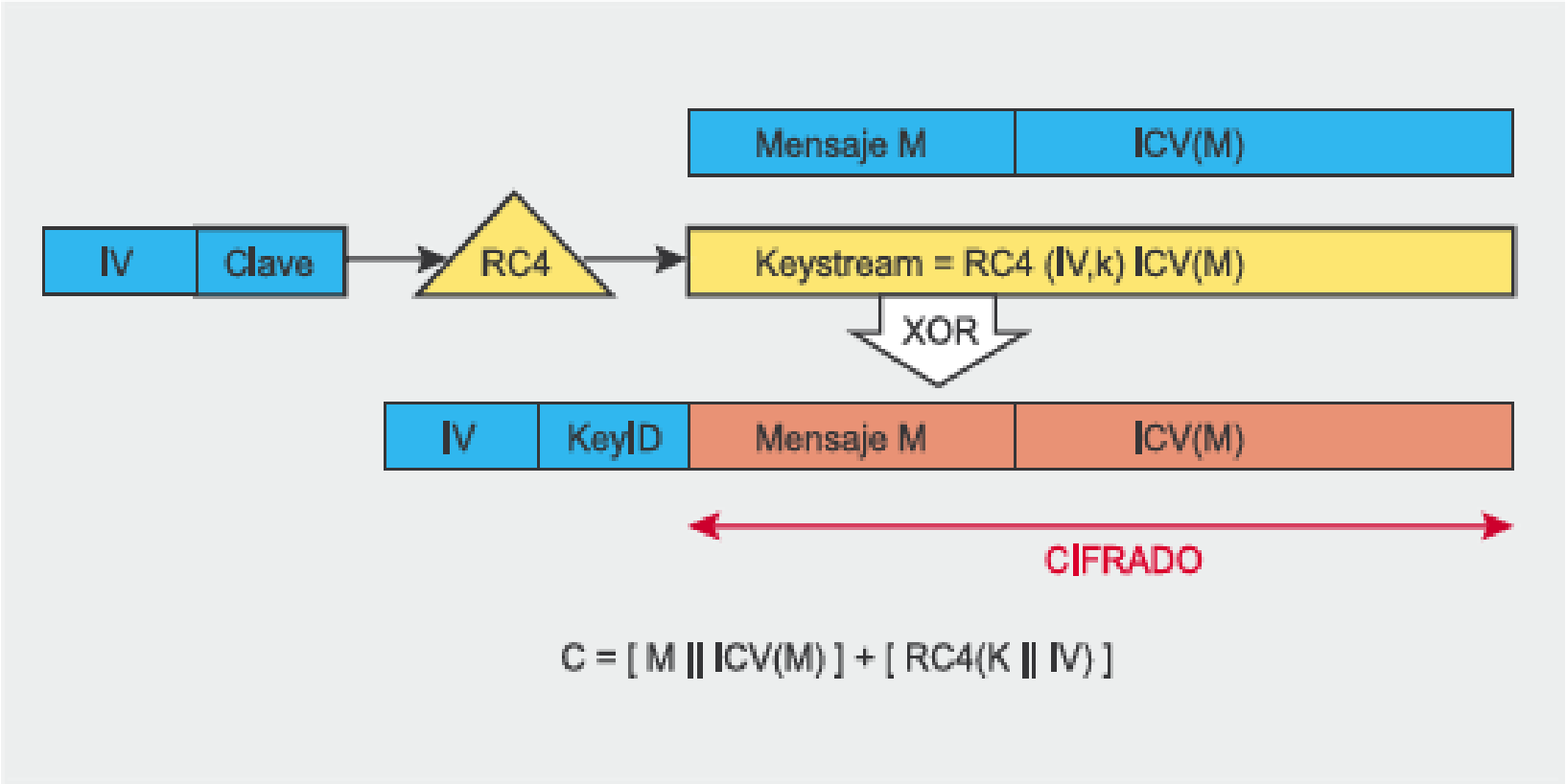
- Uso de claves estáticas
  - No existe ningún mecanismo de gestión de claves
  - Se comparten entre numerosos usuarios por tiempo ilimitado
  - Se genera mucho tráfico, lo que permite su análisis
- El vector de inicialización (IV) se envía en claro
  - El IV posee 24 bits: demasiado corto
  - Si se repite el IV (es típico inicializarlo a 0 con cada conexión), se produce la misma secuencia cifrante
  - Conocida ésta, se puede descifrar el tráfico cifrado con ella

Procedimiento WEP



Fuente: G. Álvarez / P.P. Pérez (CSIC)

Encriptación WEP



Fuente: hakin9

Debilidades WEP

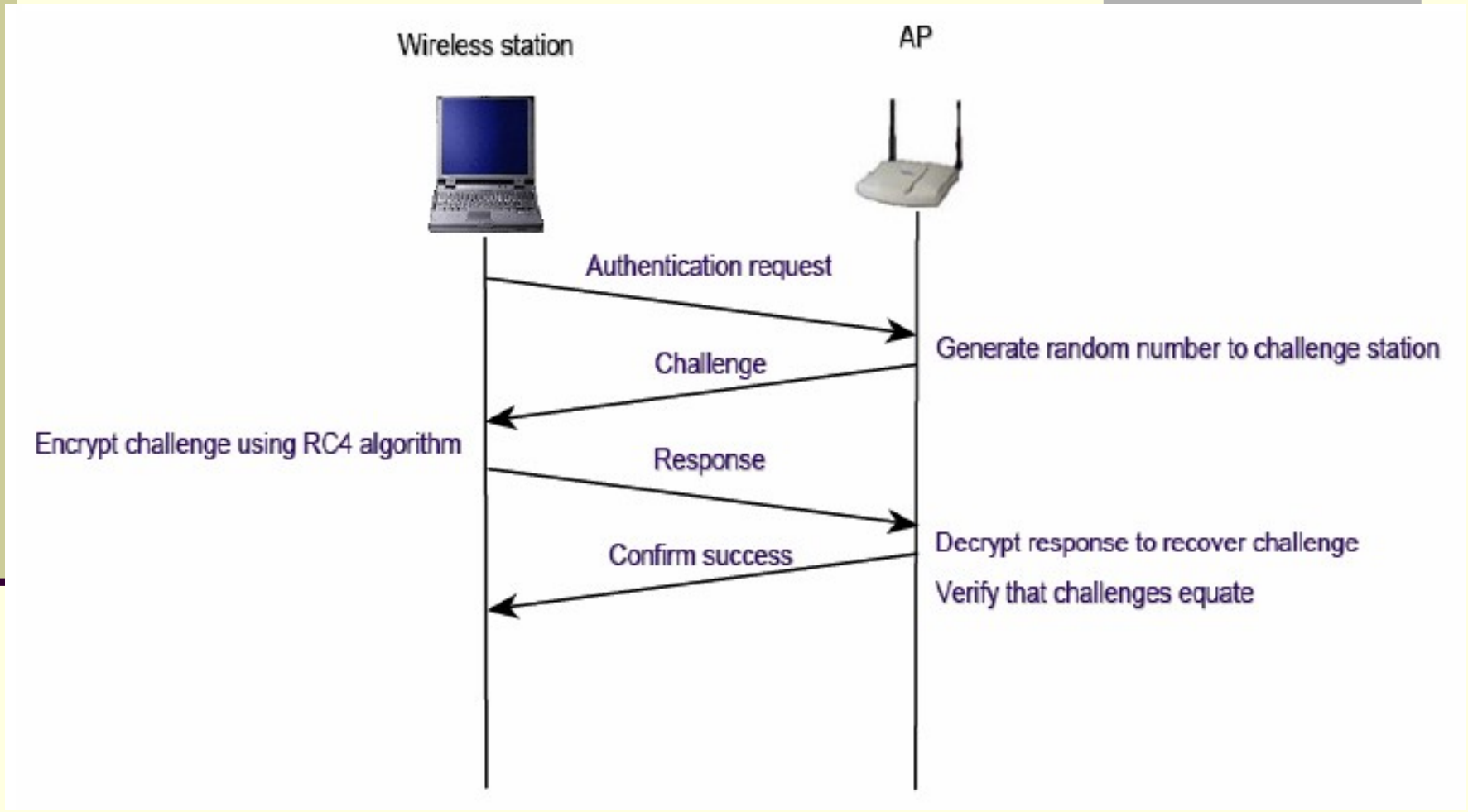
Fecha	Descripción
Septiembre 1995	Vulnerabilidad RC4 potencial (Wagner)
Octubre 2000	Primera publicación sobre las debilidades de WEP: *Insegura para cualquier tamaño de clave; Análisis de la encapsulación WEP* (Walker)
Mayo 2001	Ataque contra WEP/WEP2 de Arbaugh
Julio 2001	Ataque CRC *bit flipping* – *Intercepting Mobile Communications: The Insecurity of 802.11* (Borisov, Goldberg, Wagner)
Agosto 2001	Ataques FMS – Debilidades en el algoritmo de programación de RC4 (Fluhrer, Mantin, Shamir)
Agosto 2001	Publicación de AirSnort
Febrero 2002	Ataques FMS optimizados por h1kari
Agosto 2004	Ataques KoreK (IVs únicos) – publicación de chopchop y chopper
Julio/ Agosto 2004	Publicación de Aircrack (Devine) y WepLab (Sánchez), poniendo en práctica los ataques KoreK.

Fuente: hakin9

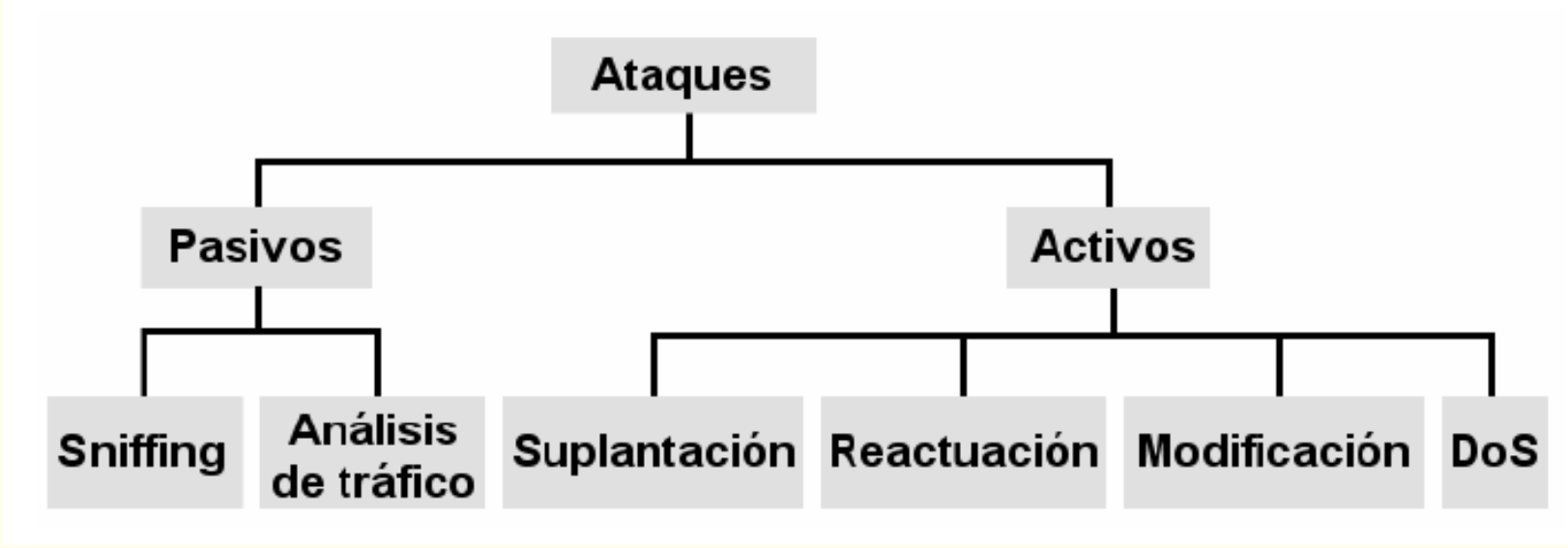
Autenticación: Proceso previo a la asociación.

- Existen dos tipos:
- Autenticación de sistema abierto:
  - Obligatoria en 802.11, se realiza cuando el cliente envía una solicitud de autenticación con su SSID a un AP, el cual autorizará o no.
  - Este método aunque es totalmente inseguro, no puede ser dejado de lado, pues uno de los puntos más fuertes de WiFi es la posibilidad de conectarse desde sitios públicos anónimamente (Terminales, hoteles, aeropuertos, etc.).
- Autenticación de clave compartida:
  - Es el fundamento del protocolo WEP (hoy totalmente desacreditado), se trata de un envío de interrogatorio (desafío) por parte del AP al cliente.

Autentificación con clave compartida



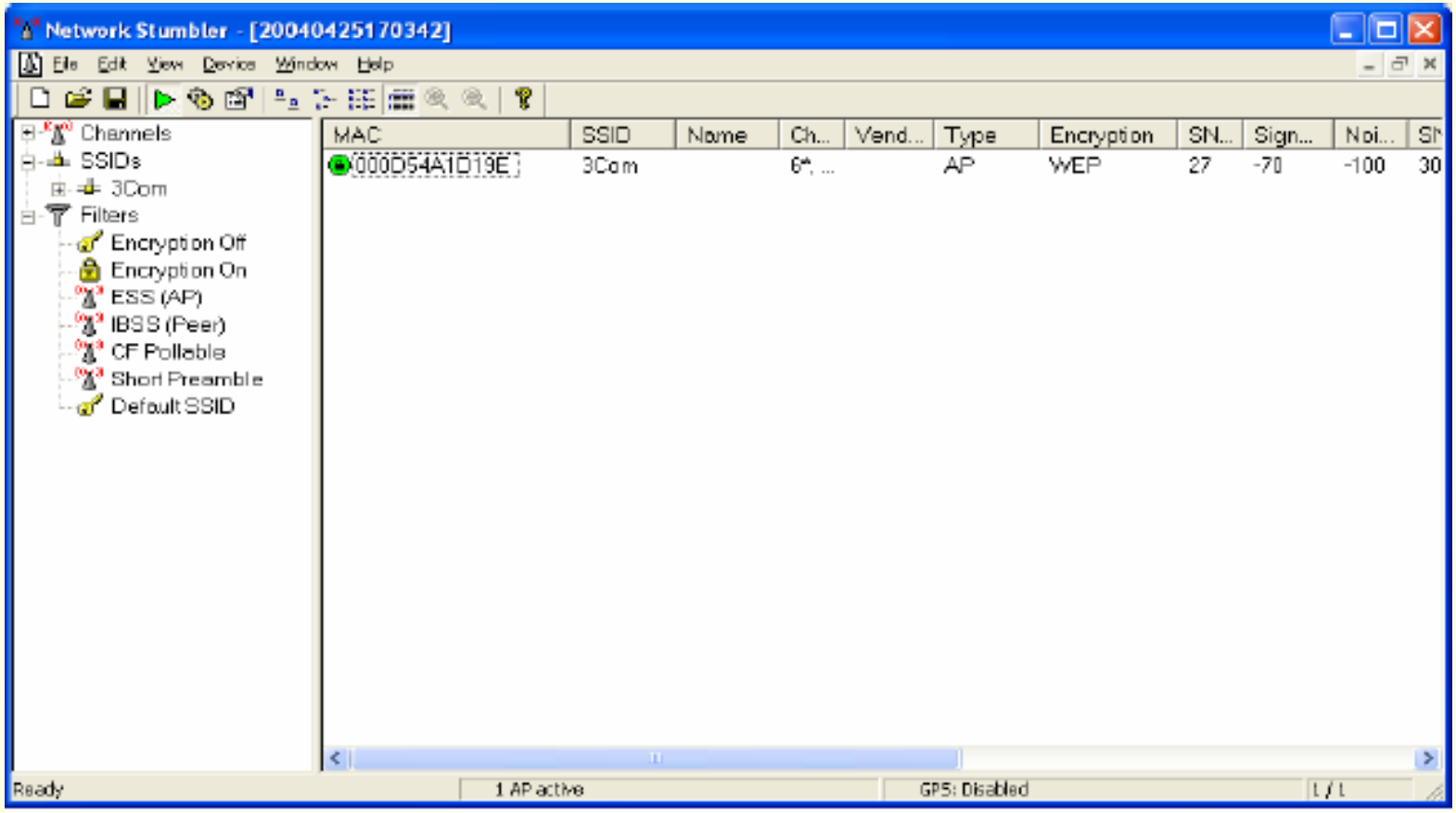
Tipos de ataques



Ataques pasivos

- Sniffing
  - El tráfico de redes inalámbricas puede espiarse con mucha más facilidad que en una LAN
  - Basta con disponer de un portátil con una tarjeta inalámbrica
  - El tráfico que no haya sido cifrado, será accesible para el atacante y el cifrado con WEP también
- Análisis de tráfico
  - El atacante obtiene información por el mero hecho de examinar el tráfico y sus patrones: a qué hora se encienden ciertos equipos, cuánto tráfico envían, durante cuánto tiempo, etc.

Network Stumbler & kismet (Linux)

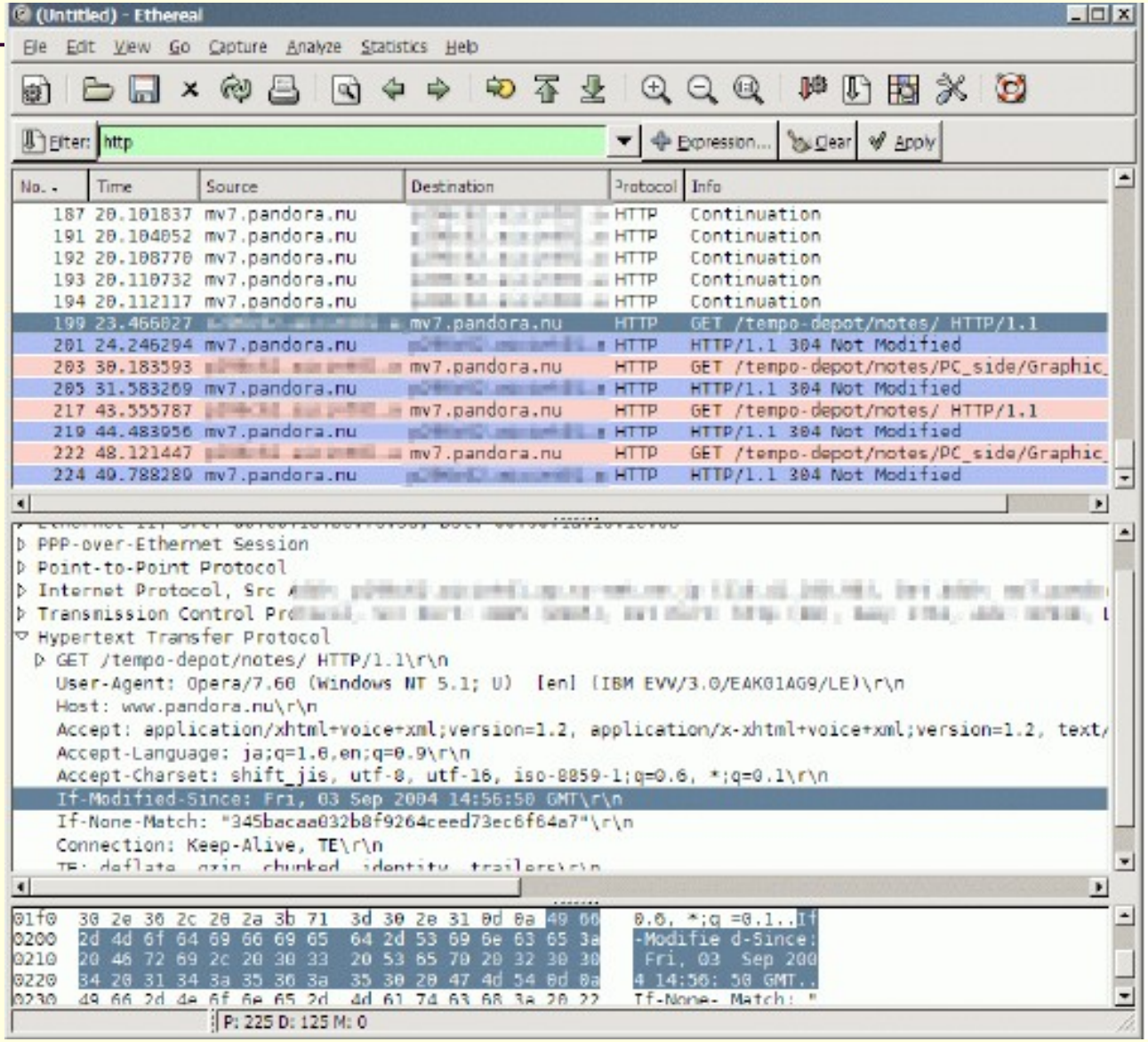


Cambio dirección MAC

- La MAC puede cambiarse mediante software
  - Ejemplo:
    - ifconfig (Linux)
    - SimpleMAC (Win)

cd auditor

Ethereal sniffer



Ataques Activos

- Suplantación
  - Mediante un sniffer para hacerse con varias direcciones MAC válidas
  - El análisis de tráfico le ayudará a saber a qué horas debe conectarse suplantando a un usuario u otro
  - Otra forma consiste en instalar puntos de acceso ilegítimos (rogue) para engañar a usuarios legítimos para que se conecten a este AP en lugar del autorizado
- Modificación
  - El atacante borra, manipula, añade o reordena los mensajes transmitidos
- Cain & abel y ettercap

Activos (II)

- Reactuación
  - Inyectar en la red paquetes interceptados utilizando un sniffer para repetir operaciones que habían sido realizadas por el usuario legítimo
- Denegación de servicio
  - El atacante puede generar interferencias hasta que se produzcan tantos errores en la transmisión que la velocidad caiga a extremos inaceptables o la red deje de operar en absoluto.
- Otros ataques: inundar con solicitudes de autenticación, solicitudes de deautenticación de usuarios legítimos, tramas RTS/CTS para silenciar la red, etc.

Obtención clave WEP

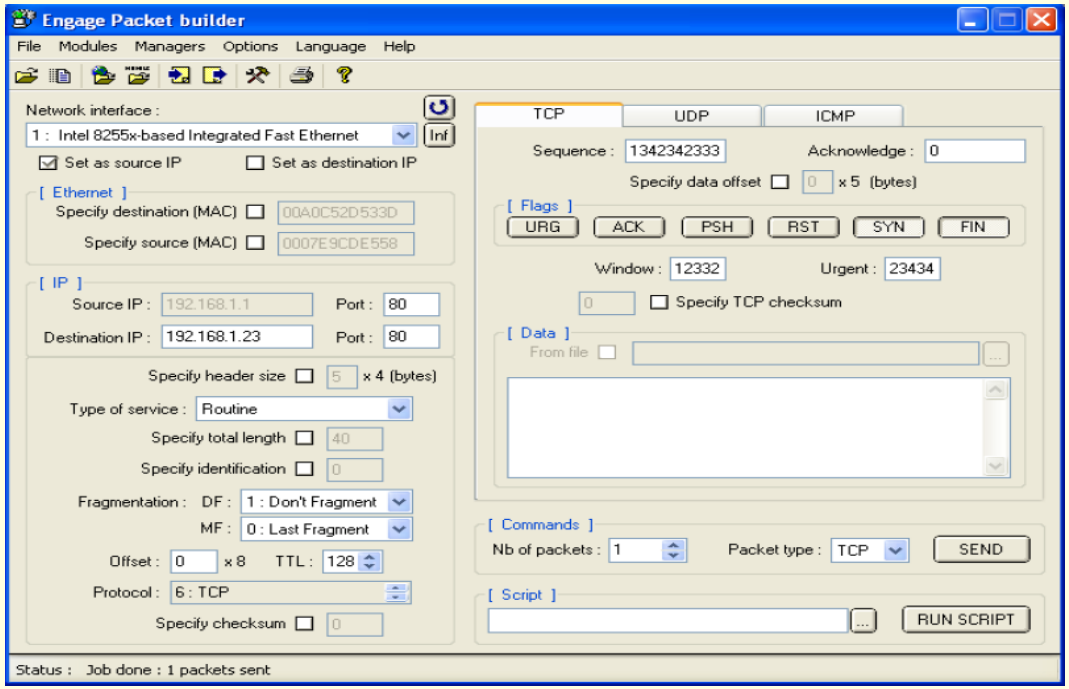
- Aircrack (incluye aireplay, airodump).
  - Airodump:
    - herramienta de sniffing para descubrir las redes que tienen activado wep
  - Aireplay:
    - Herramienta de Inyección para incrementar el tráfico
  - Aircrack :
    - Crakeador de claves WEP que utiliza los IVs únicos recogidos
  - http://freshmeat.net/projects/aircrack
- Airsnort:
  - http://airsnort.shmoo.com/
- Wepcrack:
  - http://wepcrack.sourceforge.net/

Inyección de tráfico

- WEPWedgie

Inyectar paquetes

- Engage packet builder



Soft seguridad

- Ataque inductivo inverso
  - Desencriptación de paquetes de datos WEP arbitrarios sin conocer la clave
  - Chopchop (KoreK)
    - http://www.netstumbler.org/showthread.php?t=12489
- MItm
  - Hotspotter
- generador de password
  - https://www.grc.com/passwords.htm

Seguridad wi-fi

- No existencia clara de un perímetro
  - Facilidad para rastreo
  - Accesibilidad sin acceso físico (por proximidad)
- Valores por defecto
  - Cambiar valores
- Posibilidad de cambiar MAC
  - Detección
- Autenticación por máquina
  - 802.1X (usuario)
- Debilidad de WEP
  - WPA o WPA2

Acciones

- Eliminar todos los valores predeterminados
  - SSID
  - Contraseña de la aplicación de administración (fuerte)
  - Acceso al router desde Internet
- Activar el cifrado de datos (mínimo 128 bits)
- Cerrar la red a dispositivos ajenos
  - Desactivar la difusión del SSID
  - Especificar lista de direcciones MAC permitidas

Acciones avanzadas

- Utilizar WPA/WPA2 (no WEP)
- Autenticar a los usuarios de manera individualizada
- Segregar el entorno WiFi
  - Protección por FW/VPN/IPS

WPA

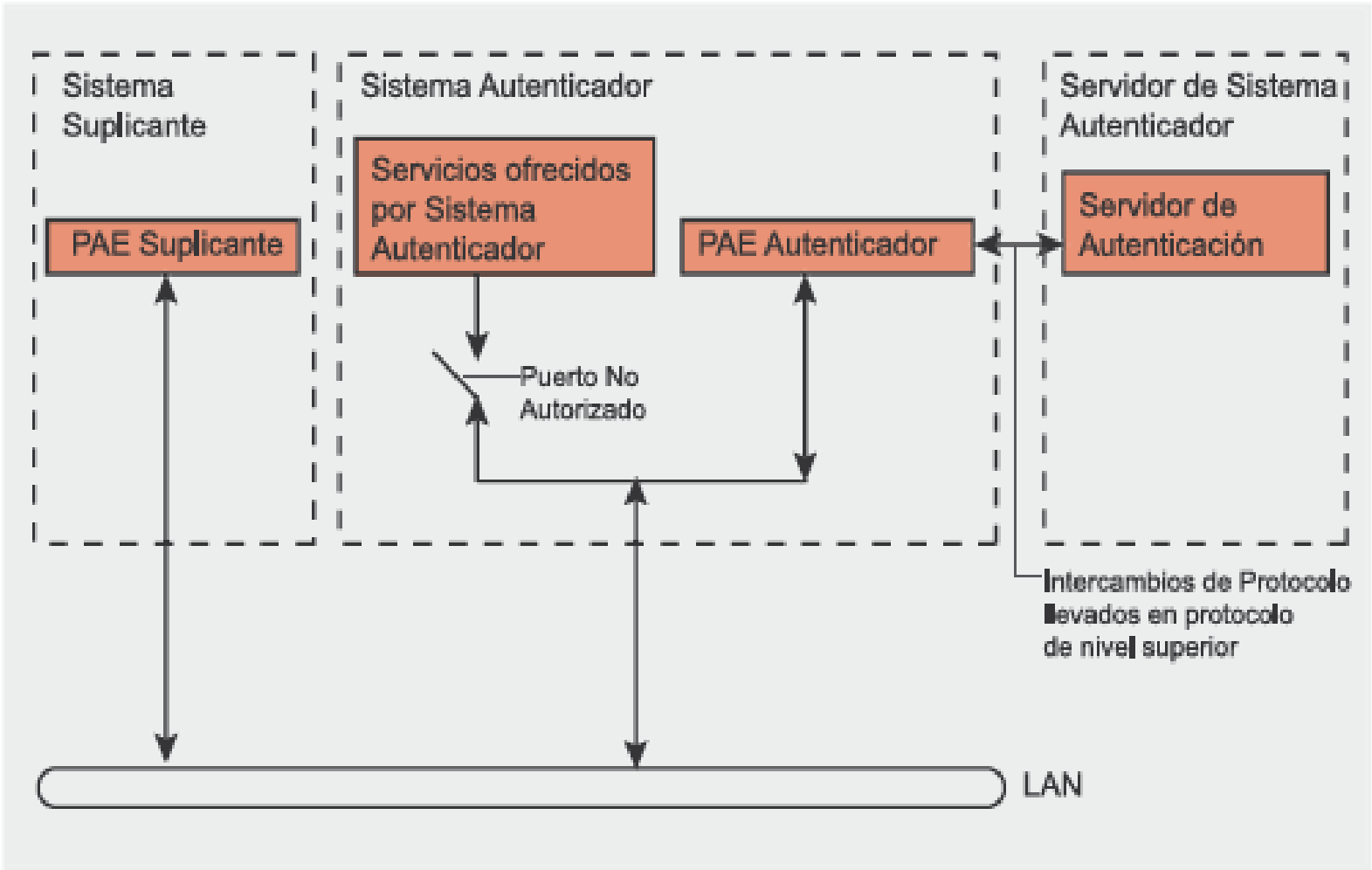
- Define múltiples claves:
  - PSK (compartida),
  - PMK (maestra),
  - PTK (temporales)…

- WPA Personal (clave compartida, PSK) o
- WPA Empresarial (RADIUS,802.1x/EAP).
- ¿Es WPA vulnerable?
  - Cowpatty.

Conceptos: 802.1X

- Es un mecanismo estándar para autenticar centralmente estaciones y usuarios.
- Posee mecanismos de autentificación, autorización y distribución de claves. Incorpora control de acceso para los usuarios que se unan a la red)
- Es un estándar abierto que soporta diferentes algoritmos de encriptación.
- Se apoya en el protocolo de autenticación EAP (Extensible Authentication Protocol)
- Está compuesto por tres entidades funcionales:
  - El suplicante (cliente) (Xsupplicant en Linux)
  - El autenticador que hace el control de acceso. Punto de Acceso
  - El servidor de autenticación, que toma la decisión de autorización
- EAP es soportado por muchos Puntos de Acceso y por HostAP.
- Antes de la autenticación sólo se permite tráfico 802.1X (petición de autenticación).

Modelo de 802.1x



Fuente: hakin9

La arquitectura 802.1x

- Está compuesta por tres partes:
- Solicitante
  - Generalmente se trata del cliente WiFi
- Autenticador
  - Suele ser el AP (Punto de acceso), que actúa como mero traspaso de datos y como bloqueo hasta que se autoriza su acceso (importante esto último).
- Servidor de autenticación
  - Suele ser un Servidor RADIUS (Remote Authentication Dial In User Service) o Kerberos, que intercambiará el nombre y credencial de cada usuario. El almacenamiento de las mismas puede ser local o remoto en otro servidor de LDAP, de base de datos o directorio activo.

EAP RFC 2284 (Extensible Authentication Protocol)

- LEAP (Lightweigth EAP)
  - Implementacion de Cisco, autenticación mutua, permite el uso dinámico de WEP
- EAP-TLS (Extensible Authentication Protocol with Transport Layer Security - RFC: 2716).
  - se basa en certificados en lugar de contraseñas como credenciales de autenticación. Autenticación mutua, cifrada y depende de certificados de una CA. Soportado por hostapd.Propuesta por Microsoft (W XP)
- EAP-MD5
  - El servidor envia un mensaje desafío al cliente y este contesta con otro mensaje MD5 o no autentica. Fácil de implementar pero menos fiable

EAP RFC 2284 (Extensible Authentication Protocol)

- EAP-TTLS (EAP with Tunneling Transport Layer Security)
  - realiza un túnel de nivel 2 entre el cliente y el AP, una vez establecido el túnel, EAP/TTLS opera sobre él, lo cual facilita el empleo de varios tipos de credenciales de autenticación que incluyen contraseñas y certificados,
  - no deja de ser una variante de EAP/TLS.
  - No necesita ambos certificados, solo el de el servidor para crear un tunel.
- PEAP (Protected Extensible Authentication Protocol)
  - el una amplia variedad de credenciales de autenticación.
  - Se considera que PEAP es el método más seguro del momento.
  - desarrollado por M$, Cisco y RSA, similar a EAP-TTLS

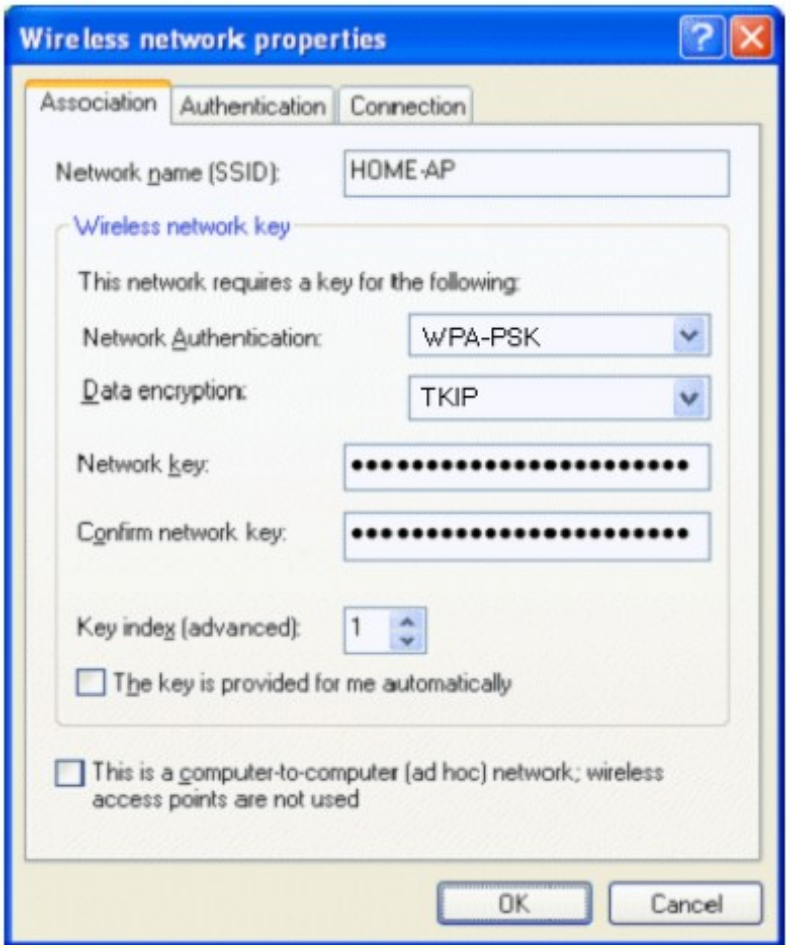
RADIUS

- Es un servicio (servidor) para autenticación remota, estándar de facto.
- Se compone de un servidor y un cliente.
- Admite varios tipos de bases de datos de contraseñas, y usar varios tipos de esquemas de autenticación, por ejemplo PAP y CHAP (se integra prácticamente con cualquier BBDD y SO).
- Algunos incorporan protección contra "sniffing" y ataques activos.
- Permite administración centralizada.
- Autorización viene definida en el RFC 2865.
- Los servicios de Accounting están disponibles en el RFC 2866.

RADIUS

- Autenticación:
  - Verificar que una entidad es quien dice ser. Suele incluir unas credenciales (usuario/contraseña, certificados, tokens, etc.).
- Autorización:
  - Decidir si la entidad, una vez autenticada, tiene permiso para acceder al recurso.
- Control de Acceso:
  - Conceder el permiso definitivo. ACL. Registro, monitorización, contabilidad e informes.

WPA-PSK


Wireless network properties
Association
Authentication
Connection
Network name (SSID):
HOME-AP
Wireless network key
This network requires a key for the following:
Network Authentication:
WPA-PSK
Data encryption:
TKIP
Network key:
Confirm network key:
Key index (advanced):
1
The key is provided for me automatically
This is a computer-to-computer (ad hoc) network; wireless access points are not used
OK
Cancel

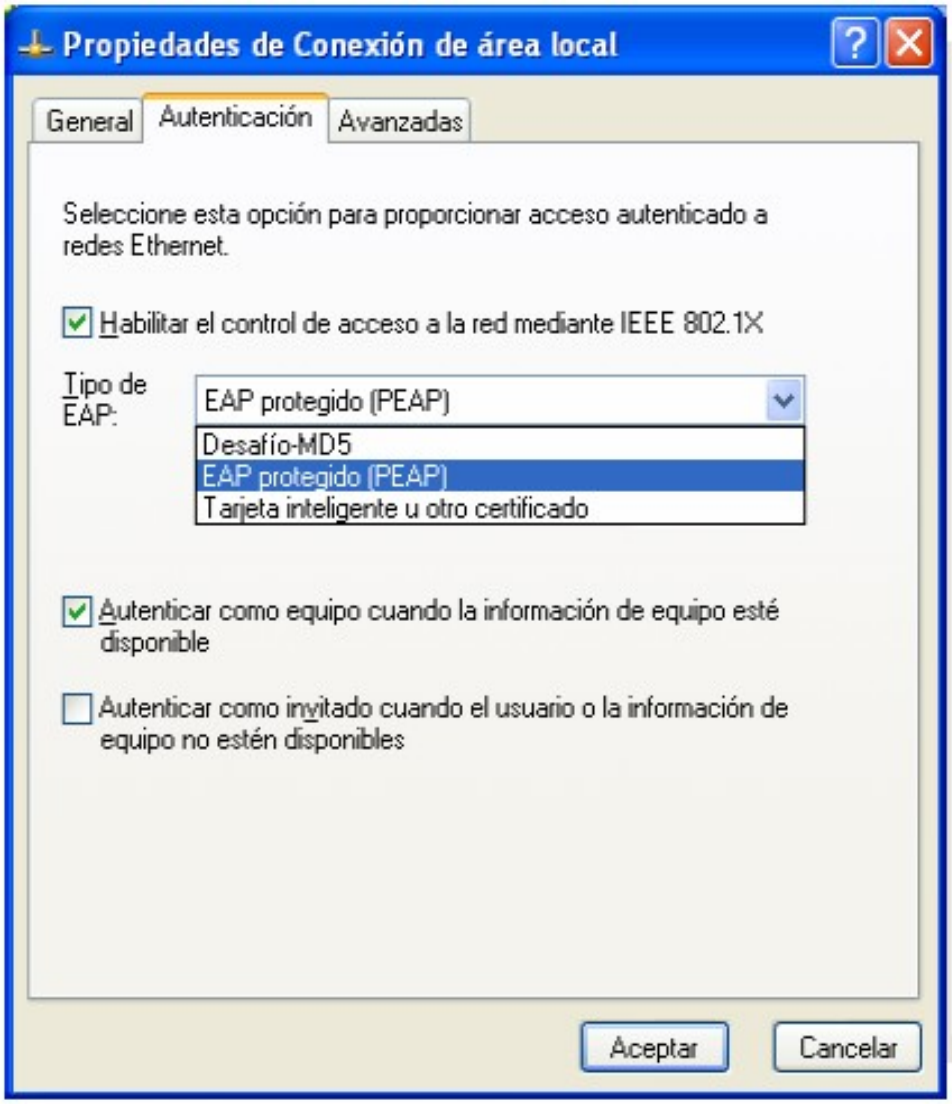
Protocolo TKIP (Temporal Key Integrity Protocol).

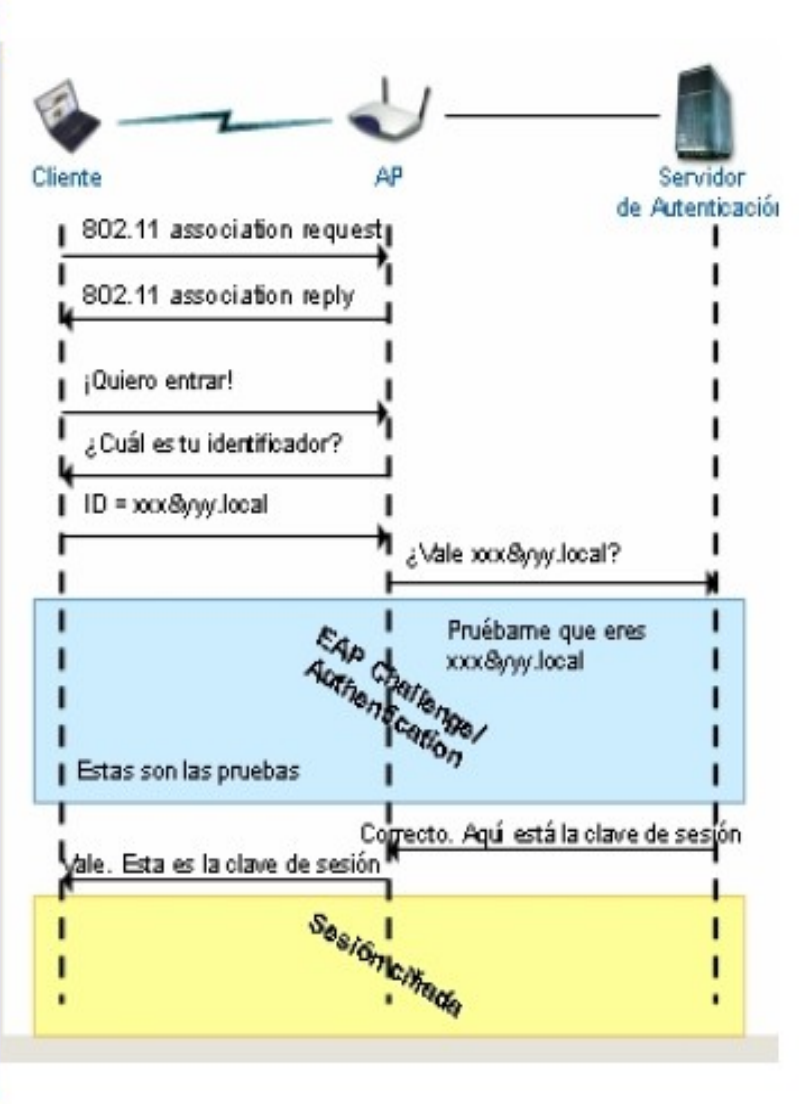
- propone tres mejoras importantes:
  - Combinación de clave por paquete:
    - combina con la dirección MAC y el número secuencial del paquete.
    - Se basa en el concepto de PSK (Pre-shared Key).
    - Esta metodología, genera dinámicamente una clave entre 280 trillones por cada paquete.
  - MIC (Message Integrity Check):
    - Se plantea para evitar el conocido ataque inductivo o de hombre del medio.
    - Y propone descartar todo mensaje que no sea validado.

TPKI (II)

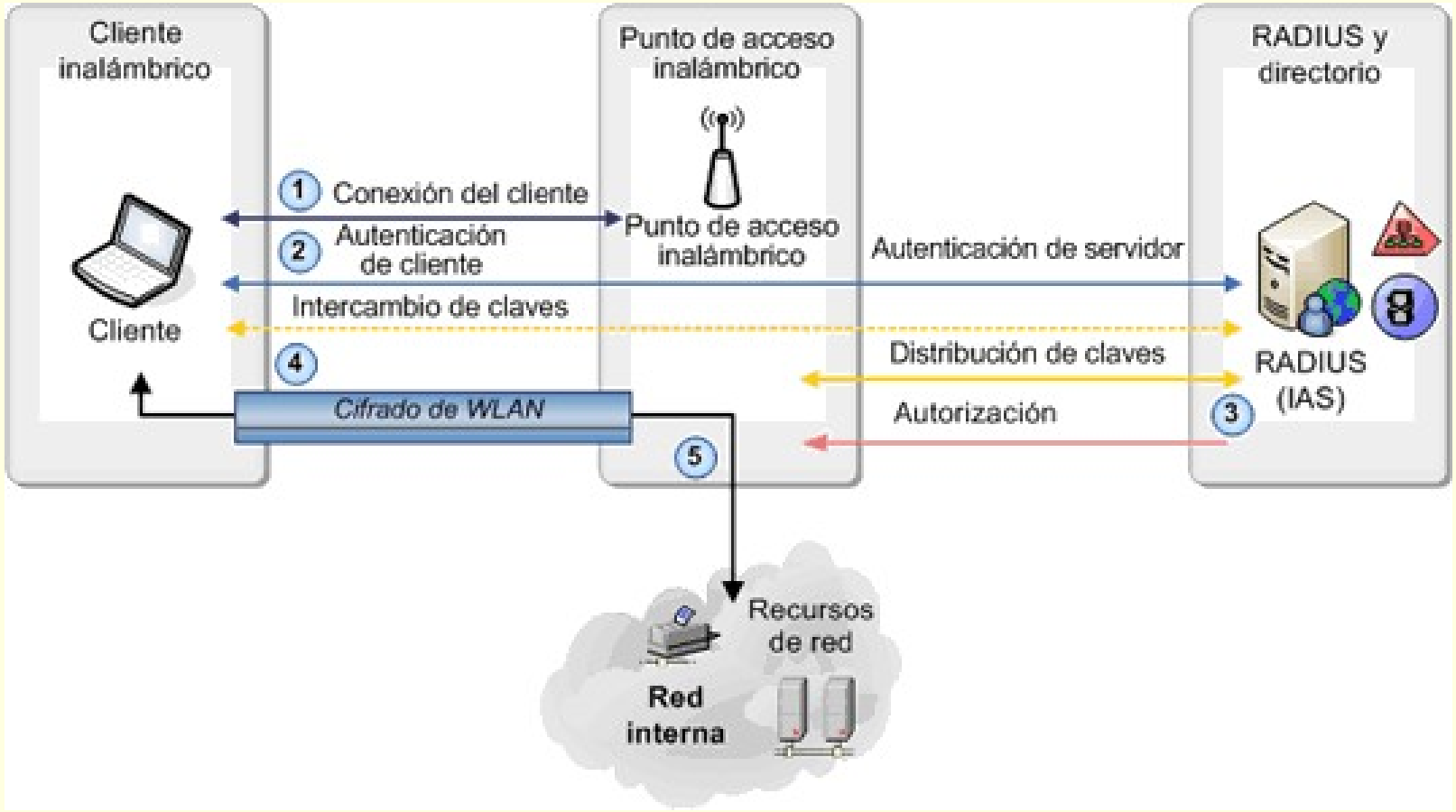
- VI (Vector de inicialización) de 48 bits:
  - Este tema era una de las mayores debilidades de WEP al emplear sólo 24 bits.
  - 24 bits son 16 millones de combinaciones, 48 bits son 280 billones.
  - se divide 280 billones sobre 16 millones, el resultado es: 17.500.000
  - si un VI de 24 bits se repite en el orden de 5 horas en una red wireless de una mediana empresa, entonces un VI de 48 bits = 5 x 17.500.00 horas = 87.500.000 horas = 3.645.833 días = 9.988 años

Autenticación por cliente con EAP (802.1X)





Funcionamiento de 802.1X con PEAP y contraseñas

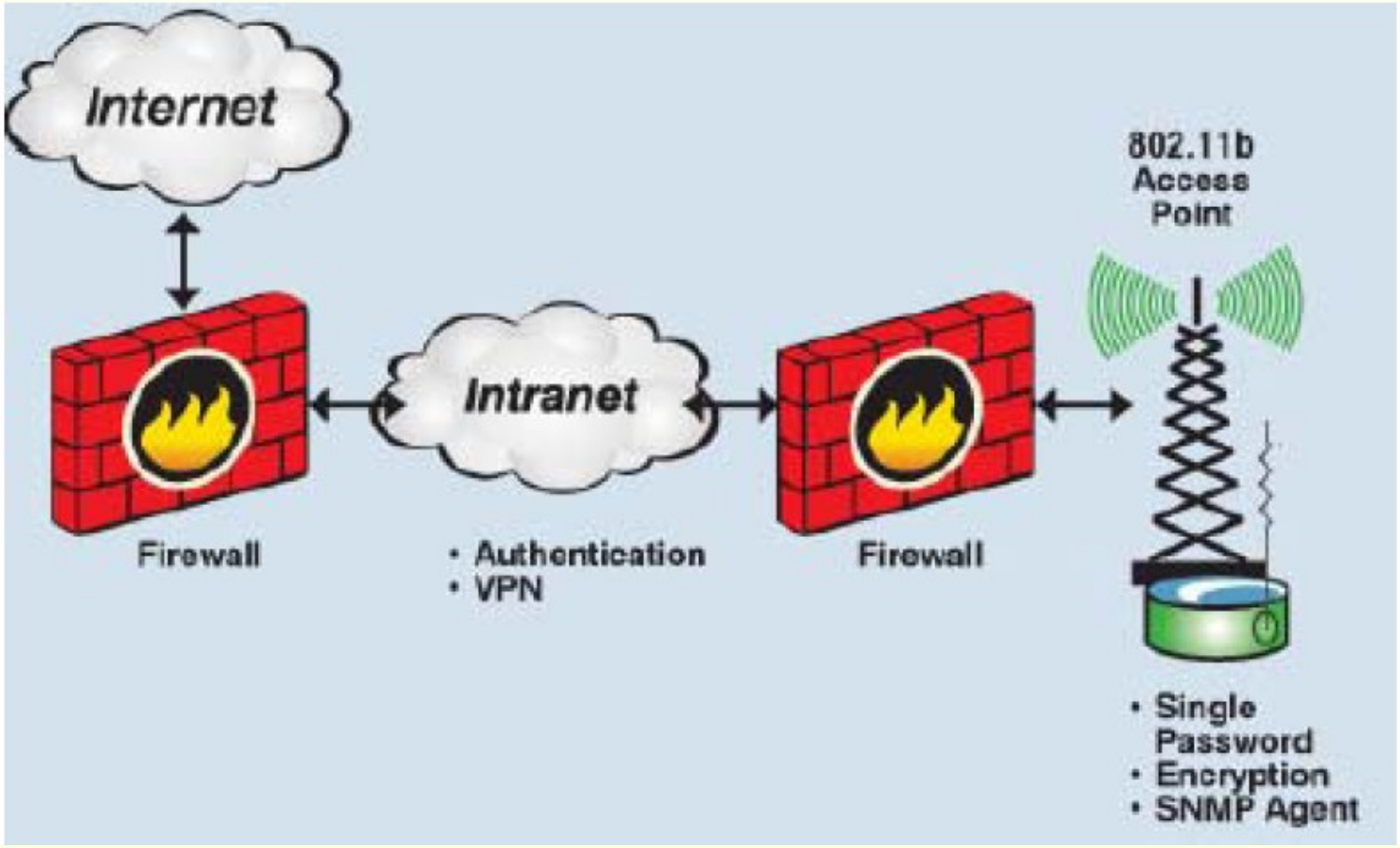


Fuente: Microsoft

Propuesta de La WiFi Alliance

- Modelo Empresas:
  - WPA:
    - Autentication: IEEE 802.1x/EAP.
    - Encryptation: TKIP/MIC.
  - WPA2:
    - Autentication: IEEE 802.1x/EAP.
    - Encryptation: AES-CCMP.
- Modelo personal (SOHO/personal):
  - WPA:
    - Autentication: PSK.
    - Encryptation: TKIP/MIC.
  - WPA2:
    - Autentication: PSK.
    - Encryptation: AES-CCMP.

Segregación de entornos



Herramientas de gestión

- Cisco WLSE
  - 2 APs dedicados a WDS
  - Gestión y seguridad RF
  - Planos
  - Gestión de elementos: configuraciones, IOS
  - Alarmas
- Airwave AMP
  - Complementaria
  - Se integra con NoCat, ACS, WLSE, switches y routers
  - Especialmente útil para helpdesk, reports y estadísticas

Enlaces y referencias

- 802.11 Wireless Networks, 2nd Edition (O'Reilly)
- RADSec Whitepaper
  - http://www.open.com.au./radiator/radsec-whitepaper.pdf
- SecureW2
  - http://www.securew2.com/
- GN2 JRA5 Deliverables
  - http://www.geant2.net./server/show/nav.778
  - (DJ5.x.y; coming soon: policy document DJ5.1.3-2)
- TERENA TF-Mobility Website
  - http://www.terena.nl./activities/tf-mobility/

Referencias

- ESTÁNDARES:
  - IEEE 802.11. http://grouper.ieee.org/groups/ 802/ 11/
  - Wi-Fi Alliance. http://www.wi- f i.org
  - IETF: http://www.ietf.org/
- ARTÍCULOS:
  - Weaknesses in the Key Scheduling Algorithm of RC4. S. Fluhrer1,I. Mant in2, & A. Shamir. Aug, 2001. ht tp:/ / www.drizzle.com/ ~aboba/ IEEE/ rc4_ksaproc.pdf.
  - (In)Security of the WEP algorithm. N. Borisov, I. Goldberg & D.Wagner. 2001.http://www.isaac.cs.berkeley.edu/ isaac/ wepfaq.html
  - Cracking WEP. Seth Fogie. July 12, 2002. http://www.samspublishing.com/ articles/printerfriendly.asp? p=27666&rl= 1~

Referencias

- ARTÍCULOS (cont.):
- Cracking Wi- Fi Protected Access (WPA), Part 1. Seth Fogie. March4, 2005.http://www.informit .com/articles/printerfriendly.asp?p= 369221
- Cracking Wi-Fi Protected Access (WPA), Part 2. Seth Fogie. March 11, 2005.http://www.informit.com/art icles/ printerfriendly.asp?p= 370636
- Four Ways To Monitor Your Wireless Network SANS Webcast.October, 2005. https://www.sans.org/webcasts/show.php?webcastid=90561
- Migrat ing from WEP to WPA2. SANS Webcast January, 2006.https://www.sans.org/webcasts/show.php?webcastid=90559
- FORMACIÓN:
  - SANS “SECURITY 617: Assessing and Securing Wireless Networks”. ht tp:/ / www.sans.org
- Más referencias:
  - http://www.raulsiles.com/resources/wifi.htmlb

WAP referencias

- Cliente: Configuración
  - Linux:
    - Xsupplicant: http://www.open1x.org/
    - AEGIS Client http://www.mtghouse.com
    - wpa_supplicant http://hostap.epitest.fi/wpa_supplicant
- Mac OS X:
  - Soporte nativo del sistema.
  - AEGIS Client http://www.mtghouse.com
- FreeBSD:
  - PANA: http://www.opendiameter.org/

Referencias (clientes wap)

- Windows:
  - Soporte nativo del sistema Windows XP SP2.
  - WIRE1x: http://wire.cs.nthu.edu.tw/wire1x/
  - AEGIS Client (98/CE/Me/2K/NT4) http://www.mtghouse.com
- Solaris:
  - AEGIS Client http://www.mtghouse.com

Referencias WAP

- Wi-Foo: The secrets of wireless hacking. Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky. http://www.wi-foo.com
- http://www.freeradius.org/doc/EAPTLS.pdf
- http://www.missl.cs.umd.edu/wireless/eaptls/?tag=missl-802-1
- http://www.alphacore.net/contrib/nantes-wireless/eap-tls-HOWTO.html
- http://www.fi.infn.it/system/WiFi/802.1X/macosx/
- http://www.dartmouth.edu/~pkilab/greenpass/gp-web-images/internetconnect2.● http://www.alphacore.net/spipen/article.php3?id_article=1
- http://oriol.joor.net/blog-dev/?itemid=1574

HERRAMIENTAS

- Auditor CD
  - http://new.remoteexploit.org/ index.php/Auditor_main
- BackTrack
  - http://www.remoteexploit.org/ index.php/ BackTrack
- SimpleMAC.
  - http://dukelupus.pri.ee/ simplemac.php
- Aircrack (incluyle aireplay, airodump).
  - http://freshmeat .net/projects/ aircrack
- WEPWedgie.
  - http://sourceforge.net /projects/wepwedgie
- Chopchop.
  - http://www.netstumbler.org/showthread.php?t=12489
- Hotspotter.
  - http://www.remoteexploit.org/index.php/Hotspotter

Herramientas

- Sistema Operativo Linux:
  - Kismet: http://www.kismetwireless.net/
  - Airsnort: http://airsnort.shmoo.com/
  - Ethereal: http://www.ethereal.com/
- Sistema Operativo Windows:
  - Airopeek:
    - http://www.wildpackets.com/products/airopeek
  - NetStumbler:
    - http://www.netstumbler.com/
- Instalar wireless-tools:
  - http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

Instalar pcmcia-cs:

- Pone a la tarjeta en modo MONITOR (Es como promiscuo de Ethernet, aunque no igual)
- http://pcmcia-cs.sourceforge.net/
- Si la tarjeta tiene el chipset Orinoco hay que parchear el pcmcia-cs para poder ponerla en modo monitor, el parche se puede encontrar en la siguiente página:
  - Orinoco Monitor Mode Patch Page
  - http://airsnort.shmoo.com/orinocoinfo.html

Medición de la capacidad de salida

- Se refiere a la medición del desempeño de la red. Las herramientas más conocidas son:
  - TCPSpeed de Maximed Software:
    - www.maximed.com
  - Chariot de MetIQ:
    - www.netiq.com

Aplicaciones que proporcionan autenticación, encriptación y/o privacidad con Software Libre

- Sin emplear EAP:
- No Cat Auth:
  - http://nocat.net
- LANRoamer:
  - http://lanroamer.net
- Wireless Hearbeat:
  - http://www.river.com/tools/authhb/
- FirstSpot:
  - http://www.patronsoft.com/firstspot/
- WiCap:
  - http://www.geekspeed.net/wicap/
- SLAN:
  - http://slan.sourceforge.net/

Otras redes inalámbicas

redes PAN

Ultra-wideband (también UWB)

- Se usa para referirse a cualquier tecnología de radio que usa una banda ancha de más grande que 500 MHz o el 25% de la frecuencia central, de acuerdo con la FCC (Federal Communications Commission).
- UWB (Ultra Wide Band) es una tecnología en el rango de las PAN (Personal Area Network).
- Permite ratios de información muy grandes (480 Mbit/s) conseguidos en distancias cortas, de unos pocos metros.
- Los dispositivos wireless USB actuales son implementados con UWB

UWB

- UWB usa un ancho muy alto de banda del espectro de RF para transmitir información.
- UWB es capaz de transmitir más información en menos tiempo que las tecnologías BLUETOOTH Y WIFI
- http://www.uwbforum.org/

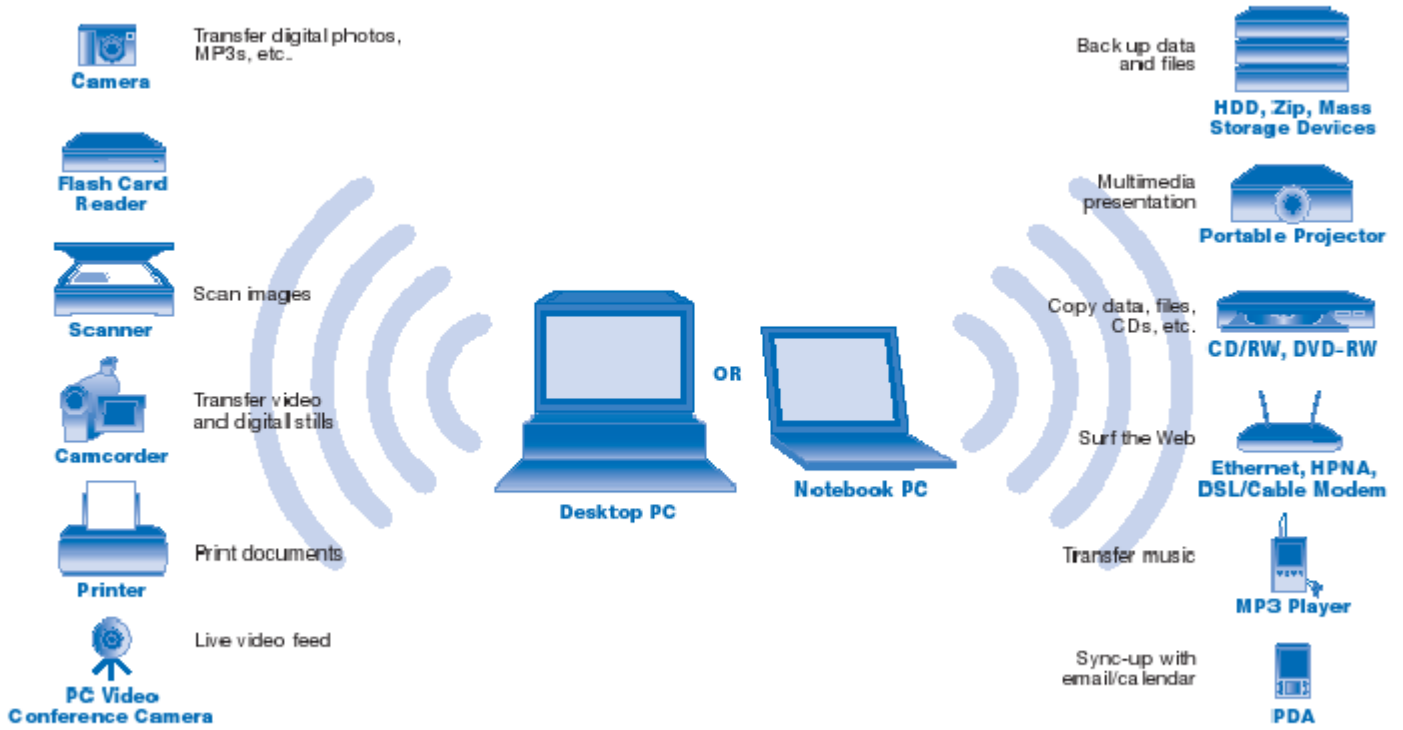
UWB

- Bluetooth, WiFi, teléfonos inalámbricos y demás dispositivos de radiofrecuencia están limitadas a frecuencias sin licencia en los 900 MHz, 2.4 GHz y 5.1 Ghz
- UWB puede usar frecuencias que van desde 3.1 GHz hasta 10.6 GHz:
  - una banda de más de 7 GHz de anchura.
- Cada canal de radio tiene una anchura de más de 500 Mhz, dependiendo de su frecuencia central.

Aplicaciones UWB

- Reemplazo de IEEE 1394 en dispositivos multimedia (cámaras de fotos o vídeo, reproductores MP3,...) con conectividad inalámbrica.
- Permitir conectividad WUSB (Wireless Universal Serial Bus) de gran velocidad (periféricos de ordenador, como escáners, impresoras e incluso dispositivos de almacenamiento externo).
- Reemplazo de cables en la siguiente generación de dispositivos Bluetooth, como los móviles de 3G.
- Creando conectividad inalámbrica ad-hoc de alto ratio para CE, PC y dispositivos móviles.
- La anchura de la señal (528 MHz o 2736 MHz de ancho de banda) puede usarse para aplicaciones de streaming de vídeo.

Figure 3. PC clusters interconnected through USB



ZigBee

- Es un protocolo de comunicaciones inalámbrico, similar al bluetooth, y basado en el estándar para redes inalámbricas de area personal (WPANs) IEEE_802.15.4
- Características del sistema
  - Bandas en las que opera: 2.4 Ghz (mundial), 915 MHz (EEUU) y 868 MHz (Europa).
  - Métodos de transmisión: DSSS, se focaliza en las capas inferiores de red (Física y MAC).
  - Velocidad de transmisión: 20 kbit/s por canal.
  - Rango: 10 y 75 metros.

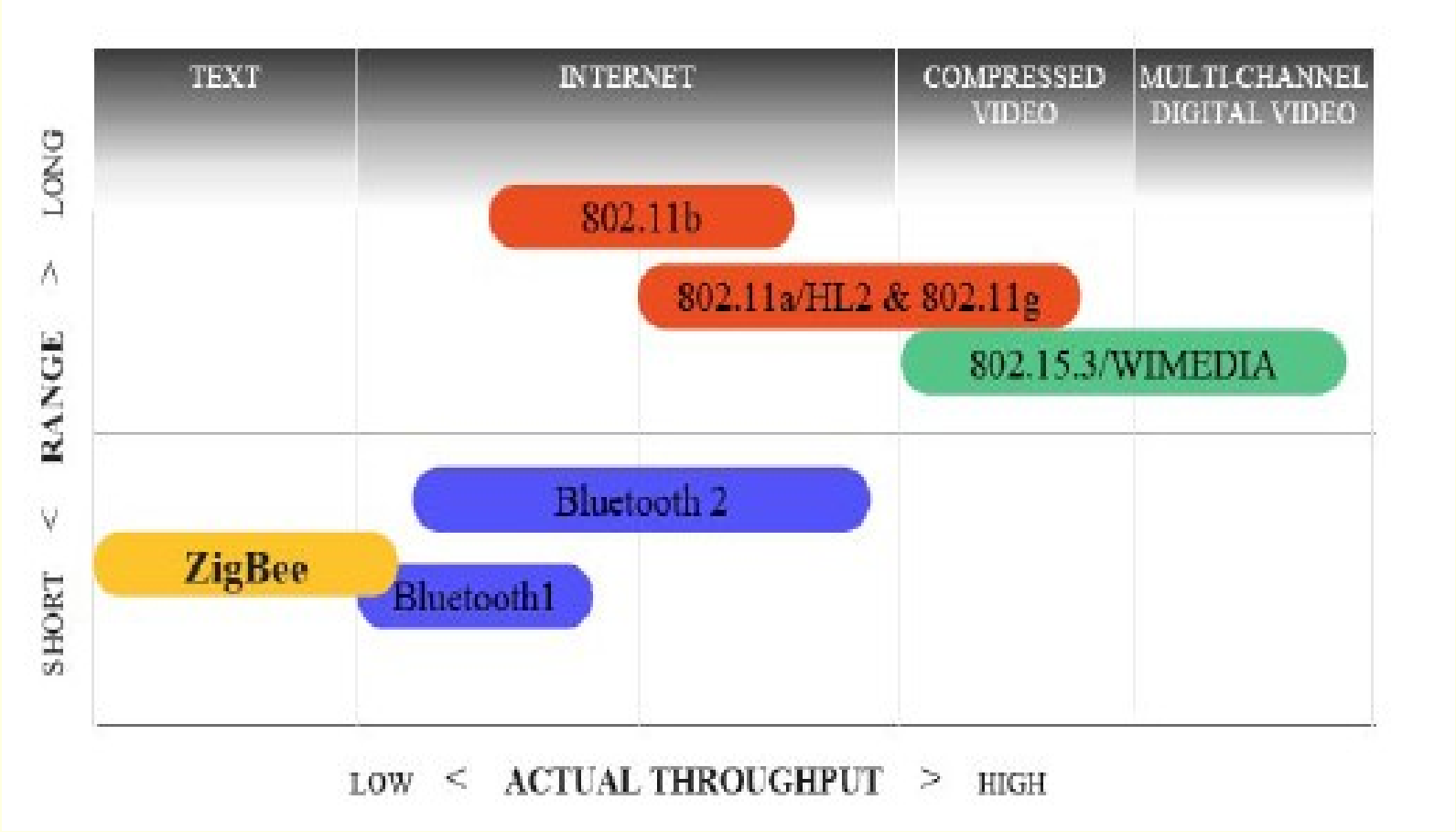
CARACTERISTICAS ZigBee

- Una red ZigBee puede constar de un máximo de 255 nodos, frente a los 8 máximos de una red Bluetooth.
- Menor consumo eléctrico
- Tiene un ancho de banda de 250 kbps, mientras que el bluetooth tiene 1 Mbps.
- usos
  - los controles remotos, los productos dependientes de la batería, los sensores médicos, y en artículos de juguetería, en los cuales la transferencia de datos es menor.

COMPARACIÓN CON BLUETOOTH

- Una red ZigBee puede constar de un máximo de 255
- Menor consumo eléctrico
- Tiene un ancho de banda de 250 kbps, mientras que el bluetooth tiene 1 Mbps.
- el ancho de banda del ZigBee UTIL PARA los controles remotos, los productos dependientes de la batería, los sensores médicos, y en artículos de juguetería, en los cuales la transferencia de datos es menor.

ZIGBEE


TEXT
INTERNET
COMPRESSED VIDEO
MULTI-CHANNEL DIGITAL VIDEO
802.11b
802.11a/HL2 & 802.11g
802.15.3/WIMEDIA
Bluetooth 2
ZigBee
Bluetooth1
SHORT < RANGE > LONG
LOW < ACTUAL THROUGHPUT > HIGH