Seguridad en Ambientes Inalámbricos

Roberto Gómez Cárdenas

rogomez@itesm.mx

http://webdia.cem.itesm.mx/ac/rogomez

Las redes

- RED
  - unión de dos o más computadoras, para crear una comunicación entre ellas que les permita compartir información y recursos.
- Para realizar esta conexión se requiere de un medio físico, en el cual viajará la información.

Haciendo cuentas ...

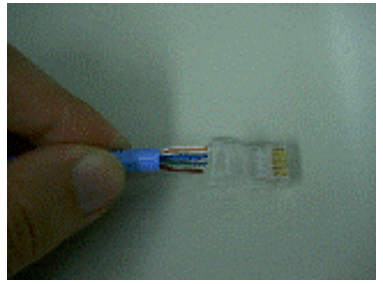
- Computación electrónica 60 años !
- Redes sólo tienen 40 años de vida !
- Seguridad 27 años !
- Internet 25 años !
- Web 12 años !
- Intranets 10 años...
- Extranets 8 años...

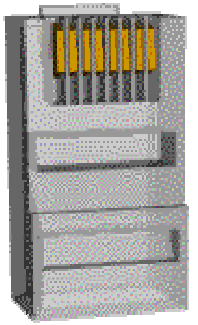
Conectividad

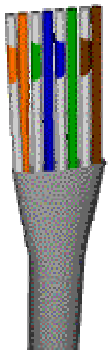
- ¿Cómo se conecta nuestro usuario a la red?
  - Narrowband
    - Dial-Up
      - 56Kbps (con suerte…)
  - Broadband
    - Ds0/E1…
      - Enlaces dedicados.
      - Oficinas / Escuelas
    - DSL
      - 128Kbps – 2Mbps
      - Requiere cobertura por el ISP

El Spaghetti

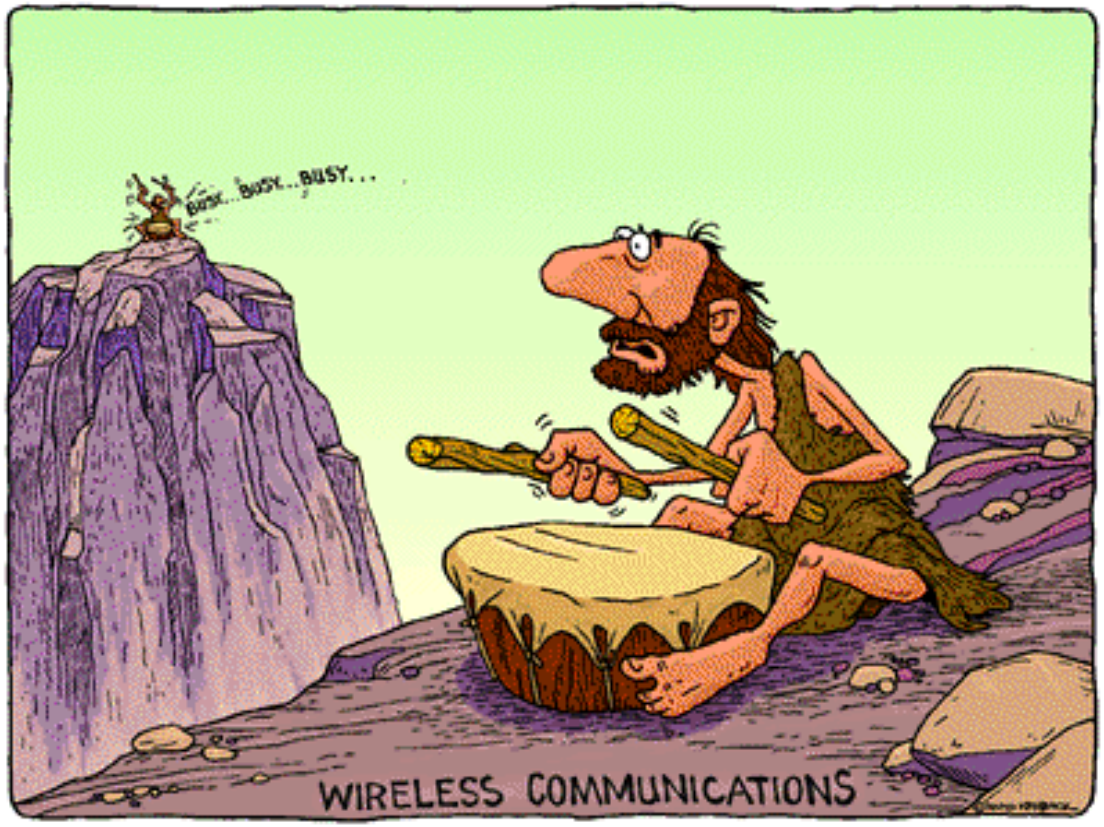
- Los datos requieren de un medio de transmisión
- Evolución de los cables
  - Coaxial
  - UTP
  - Fibra
- Problemas
  - Aumentar velocidad
  - Crecer la red
  - Costo







¿Alternativas?



¿Qué es una red inalámbrica o WLAN?

- El medio de transmisión más utilizado es el cable, pero para el caso de una red inalámbrica ese medio físico es el aire.
- WLAN: Siglas en inglés de Wireless Local Area Network.

¿Por qué Wireless LAN?

- Ausencia de cableado.
  - Bajo costo (cuidado con el TCO)
  - Liberación rápida.
- Movilidad del usuario.
- Interactividad
- Comunicación bidireccional
- Tecnología broadcast

¿Por qué no Wireless LAN?

- Ausencia de seguridad física.
- Baja tasa de flujo de datos.
- Espectro ruidoso y sin regulación.

¿Qué va a pasar con el cableado de red?

- Una red inalámbrica NO va a desplazar a una red por medio de cable.
- La red inalámbrica complementa a la red cableada en situaciones como
  - difícil montar una red,
  - realizar más conexiones
  - se requiere estar moviéndose de un área a otra sin necesidad de desconectarse de la red (computo móbil)

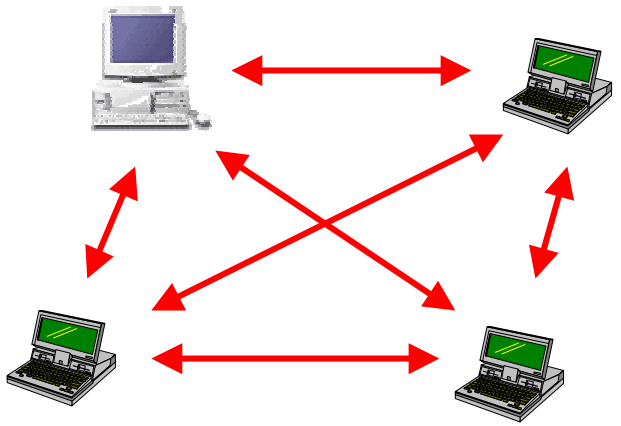
Tipos WLANS

- Ad-hoc

- Infraestructura permanente

WLAN Ad hoc

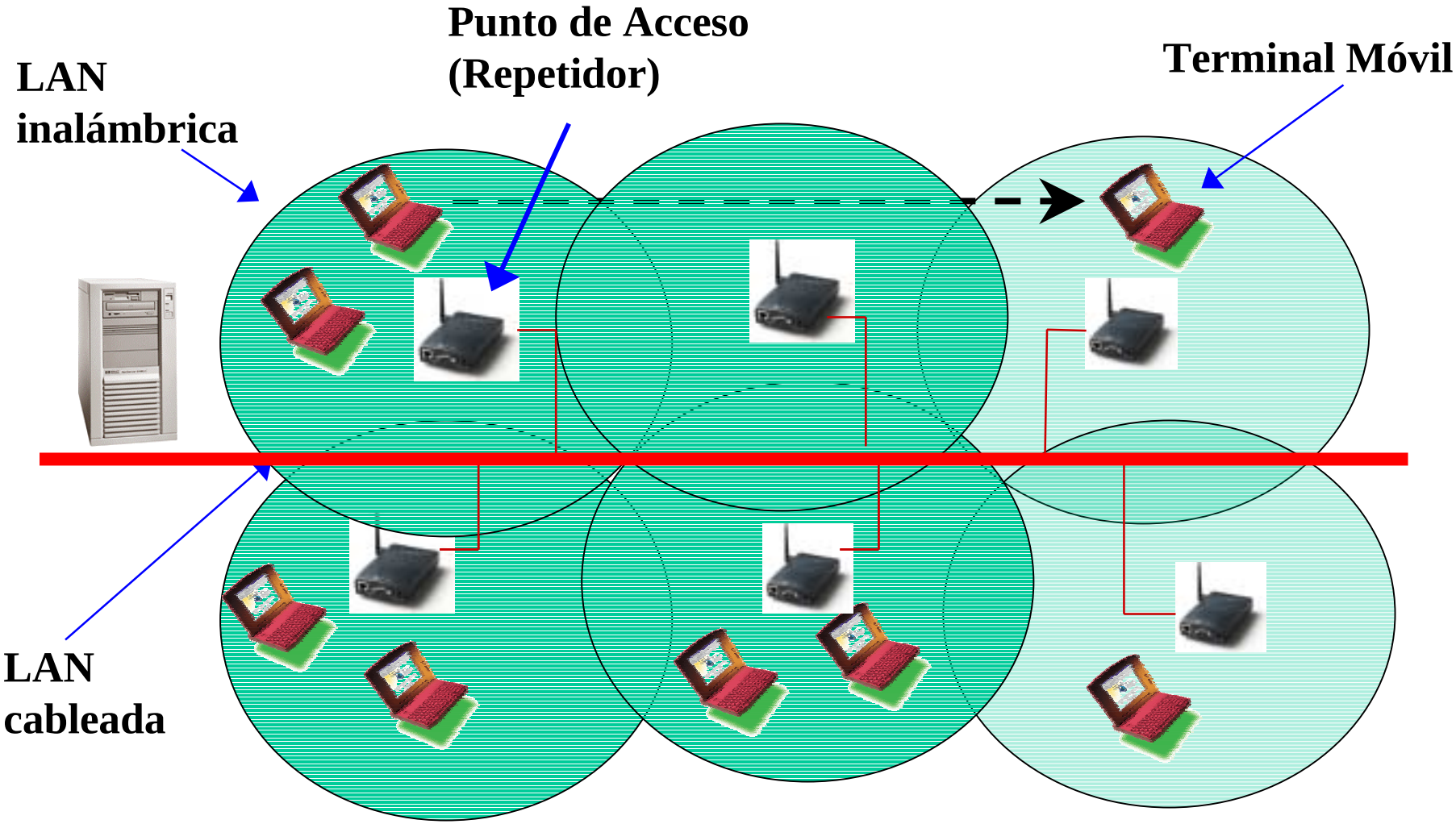
- Se juntan varios nodos móviles en una área reducida
- Se establece una comunicación entre ellos sin la ayuda de ningún tipo de columna (backbone).
- Para implementar redes ad hoc se tienen dos maneras:
  - Broadcasting/flooding
  - Infraestructura temporal



WLAN con infraestructura permanente

- Regularmente la infraestructura principal es una columna vertebral cableada (backbone).
- Esta estructura tiene puntos de contacto (puntos de acceso) con el medio inalámbrico.
  - estos pueden ser estaciones base o repetidores
- A partir del backbone existen dos tipos de comunicación
  - subida
  - bajada.

Ejemplo estructura WLAN



Elementos de una WLAN

Las entidades involucradas

- IETF
  - Internet Engineering Task Force
  - http://www.ietf.org
- IEEE
  - Institute of Electrical and Electronica Engineers
  - http://www.ieee.org
- WECA
  - Wi-Fi Alliance
  - Formada en 199
  - certifica la interoperabilidad de productos WLAN bas la especificación 802.11
  - http://www.weca.net

802.1x

802.11

Un poco sobre Wi-Fi

- En un principio, la expresión solo abarcaba únicamente a los aparatos con tecnología 802.11b
- Con el fin de evitar confusiones en la compatibilidad de los aparatos y la interoperabilidad de las redes, el término Wi-Fi se extendió a todos los aparatos provistos con tecnología 802.11
- Wi-Fi alliance
  - asociación de más de 130 fabricantes y proveedores de aplicaciones, y que garantiza que un producto que incorpore este logo es interoperable con aparatos de otros fabricantes para trabajar en una red sin cables.
  - Actualmente existen alrededor de 450 aparatos que cuentan con este certificado.

IEEE 802.11

- Estándar transmisión de datos a través señales de radio
- Capa MAC semejante a Ethernet
- Soporta el stack de protocolos de TCP/IP y otros.
- Basado en
  - Direct Sequence Spread Spectrum (DSSS),
  - Frequency Hoping Spread Spectrum (FHSS),
  - Orthogonal Frequency Division Multiplexing (OFDM)
- Tipos
  - 802.11a (Wi-Fi-5)
  - 802.11b (Wi-Fi)
  - 802.11g

Los estándares 802.x

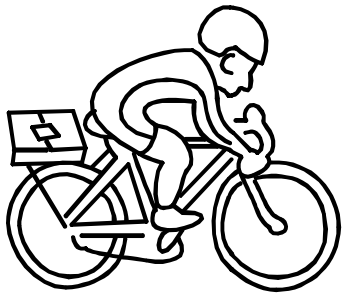
Estándar	Velocidad	Banda Frecuencia
802.11	1 y 2 Mbps	2.4 Ghz
802.11s	54 Mbps	5.15 Ghz
802.11b	11 Mbps	2.4 Ghz
802.11g	54 Mbps	2.4 Ghz
802.11i	**Por liberar en esta año (2004)**	

Algunos comentarios

- La banda de 5GHz tiene menor interferencia a la banda de 2.4GHz principalmente porque ésta es utilizada por gran cantidad de dispositivos
- 802.11b es el más económico y utilizado pero el más lento
- 802.11a es técnicamente superior (5GHz), velocidades superiores 54Mbps
- 802.11a y 802.11b no son compatibles
- 802.11g es compatible con 802.11b no con 802.11a
- 802.11i aun no es aprobado

Riesgos de una WLAN

- Monitoreo de tráfico inalambrico
  - datos de usuarios
  - localización de usuarios
  - identidad de usuarios
  - análisis de tráfico
- Acceso no autorizado a una red a través de un enlace inalambrico
  - persona pasaendose en una bicicleta
- Corrupción de servicios inalambricos

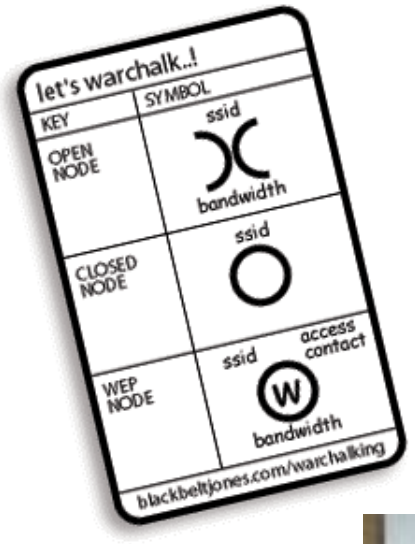


Descubrimiento

- El SSID (Service-Set Identifiers) es esencialmente el nombre de una red inalámbrica.
- La mayoría de los Access Points envían vía broadcast el SSID, esta situación permite el descubrir APs de manera sencilla.
  - probar a FF:FF:FF:FF:FF:FF con SSID nulo o “any”
  - AP envía su SSID
- El SSID se incluye en cada uno de los paquetes que no se cifran (sniffing del SSID a pesar de que el AP no los envíe por broadcast).

Descubrimiento

- Netstumbler y amigos
- Wardriving
- Warchalking
- Sniffing – Ethereal/Airopeek
- Window XP y cierto softwa de tarjetas de red detectan AP's disponibles



- Antennas
  - Omnidireccionales
  - Direccionales

http://www.ocf.berkeley.edu/~cfarivar/ warchalking/

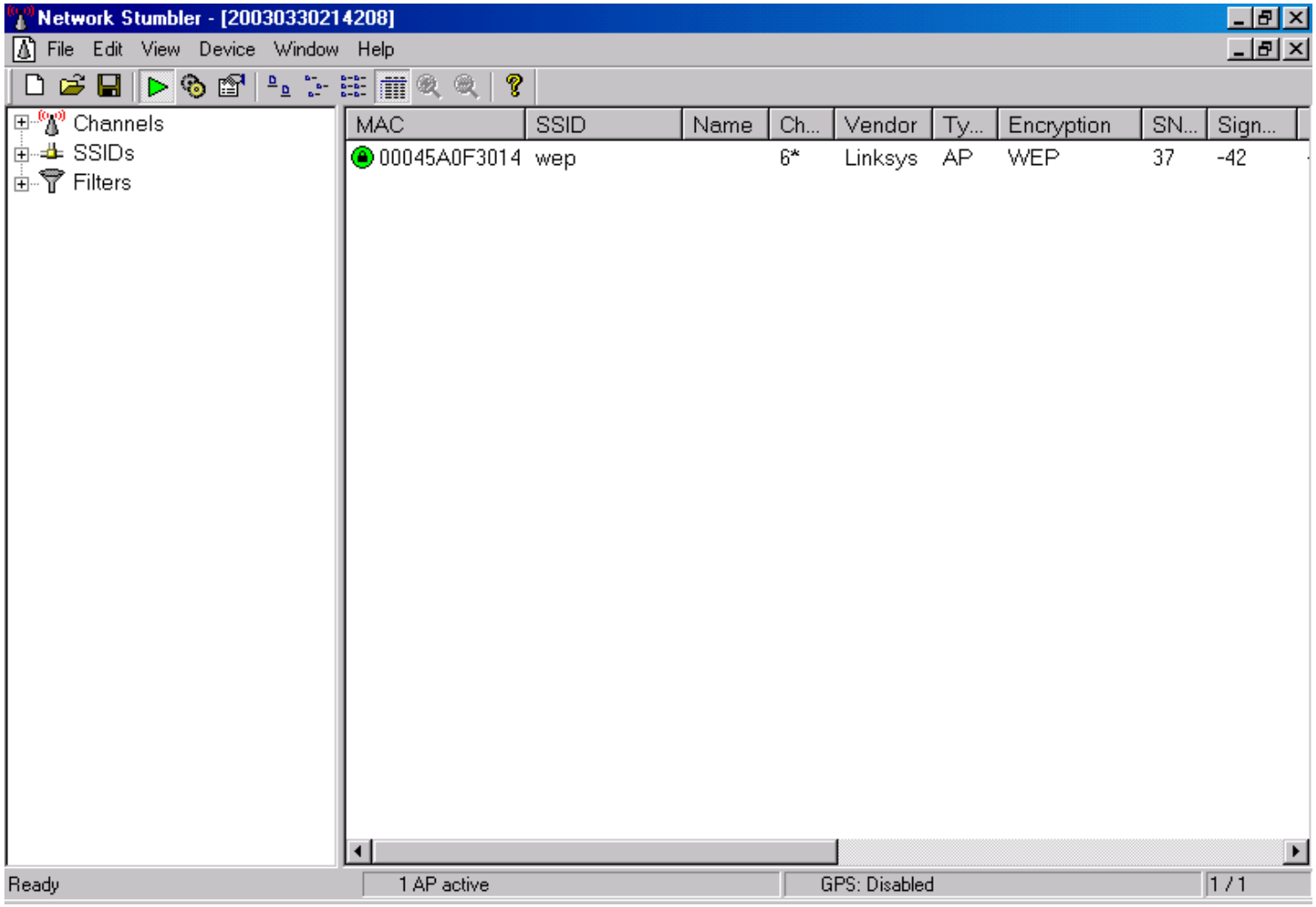
Wardriving

- Acto de descubrir redes inalámbricas en un área a través de conducir en esa área con el equipo necesario (laptop, tarjeta de red inalámbrica, software necesario, posiblemente antena externa).

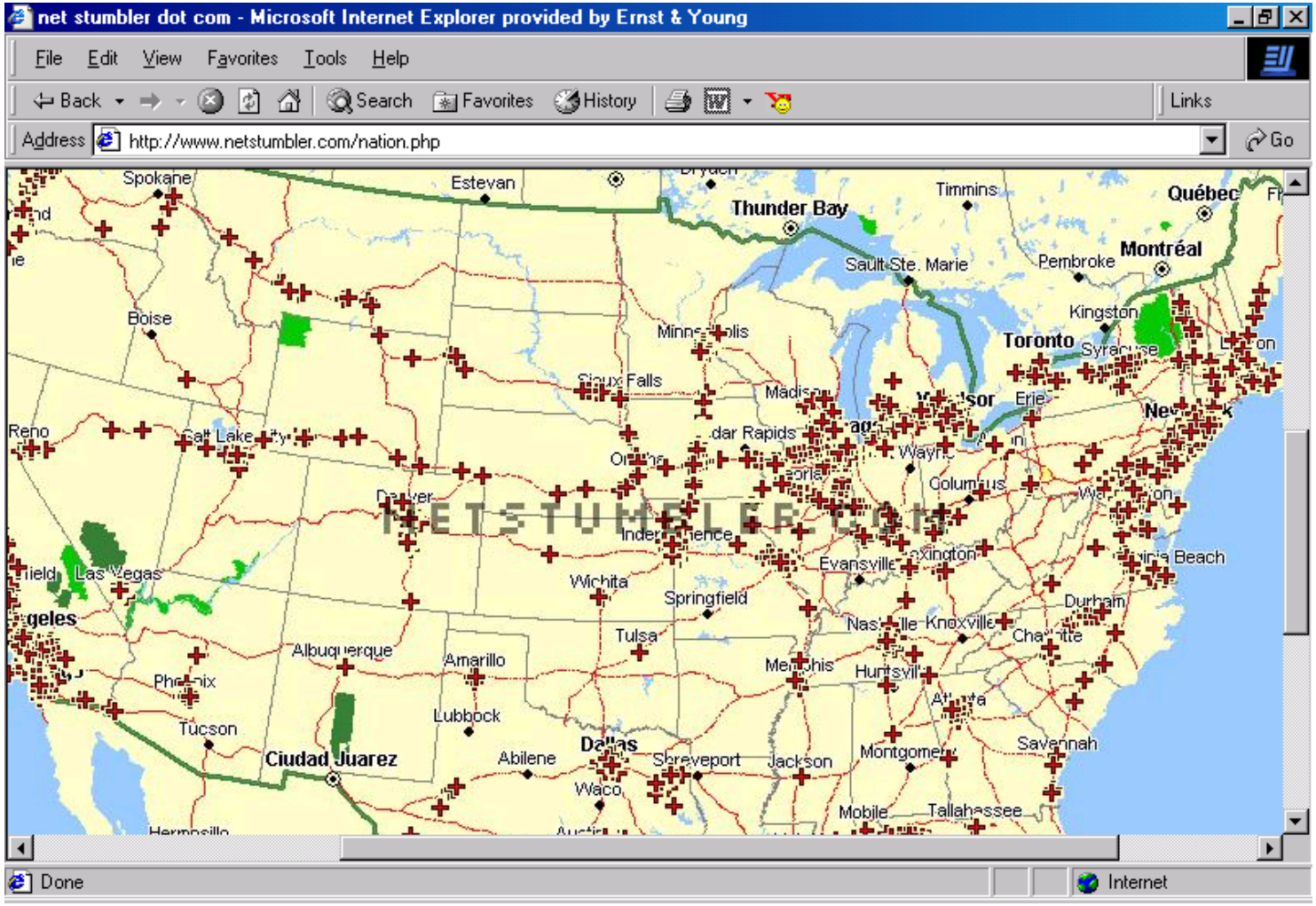
Wardriving

http://www.monolith81.de/wirelesslan/mirrors/?path=audiovideo/

Wardriving - Netstumbler



Wardriving - Netstumbler

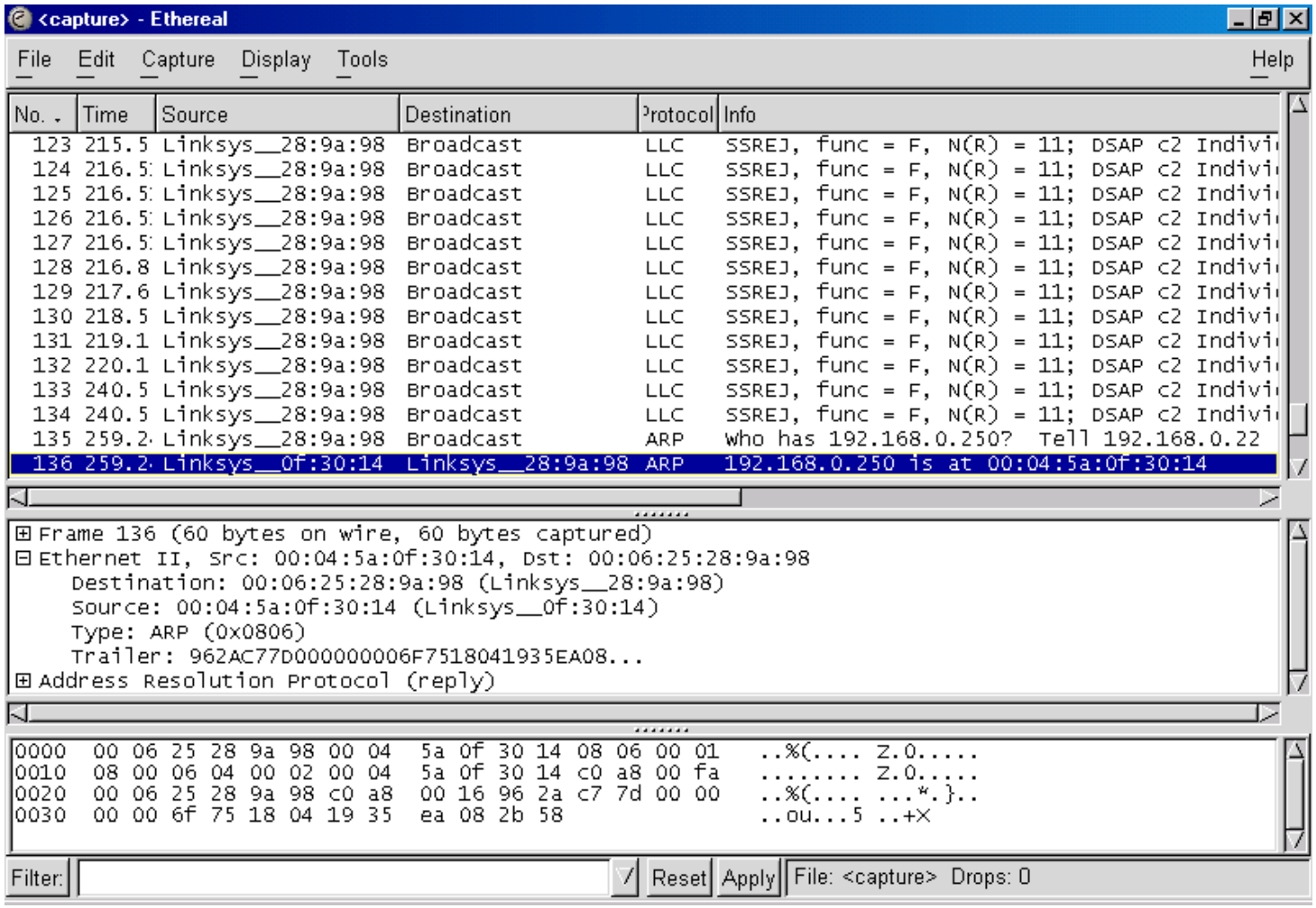


Y si no cuento con GPS

Clave	Simbolo
Nodo Abierto	SSID  Ancho de Banda
Nodo Cerrado	SSID 
Nodo WEP	SSID  Access Contact Ancho de Banda

Wardriving/Warchalking - Ministumbler

Descubrimiento - Sniffing



¿Pero que estamos buscando?

- Redes inalámbricas
  - Preferentemente con WEP deshabilitado
  - Preferentemente con DHCP habilitado

Seguridad ofrecida por protocolos

- Por defecto, el protocolo 802.11b (Wi-Fi) provee de un mecanismo de cifrado de datos llamado WEP

WEP: Wired Equivalency Privacy (WEP)

- Protección igual o mejor que las redes alambradas
- Uso de llaves para autenticar cada estación
- Puntos de acceso también requieren una llave para ser admitidos en la red
- Desarrollo de protocolos de autenticación y de distribución de llaves se les deja a los vendedores
- Encripción opcional de datos entre estaciones usando algoritmo RC4
- Intento del estándar por proteger la confidencialidad y proveer autenticación.
- Tamaño de las llaves (64-40 / 128-104)

Problemas inherentes

- Administración de las llaves
- Distribución de las llaves
- Vectores iniciales débiles

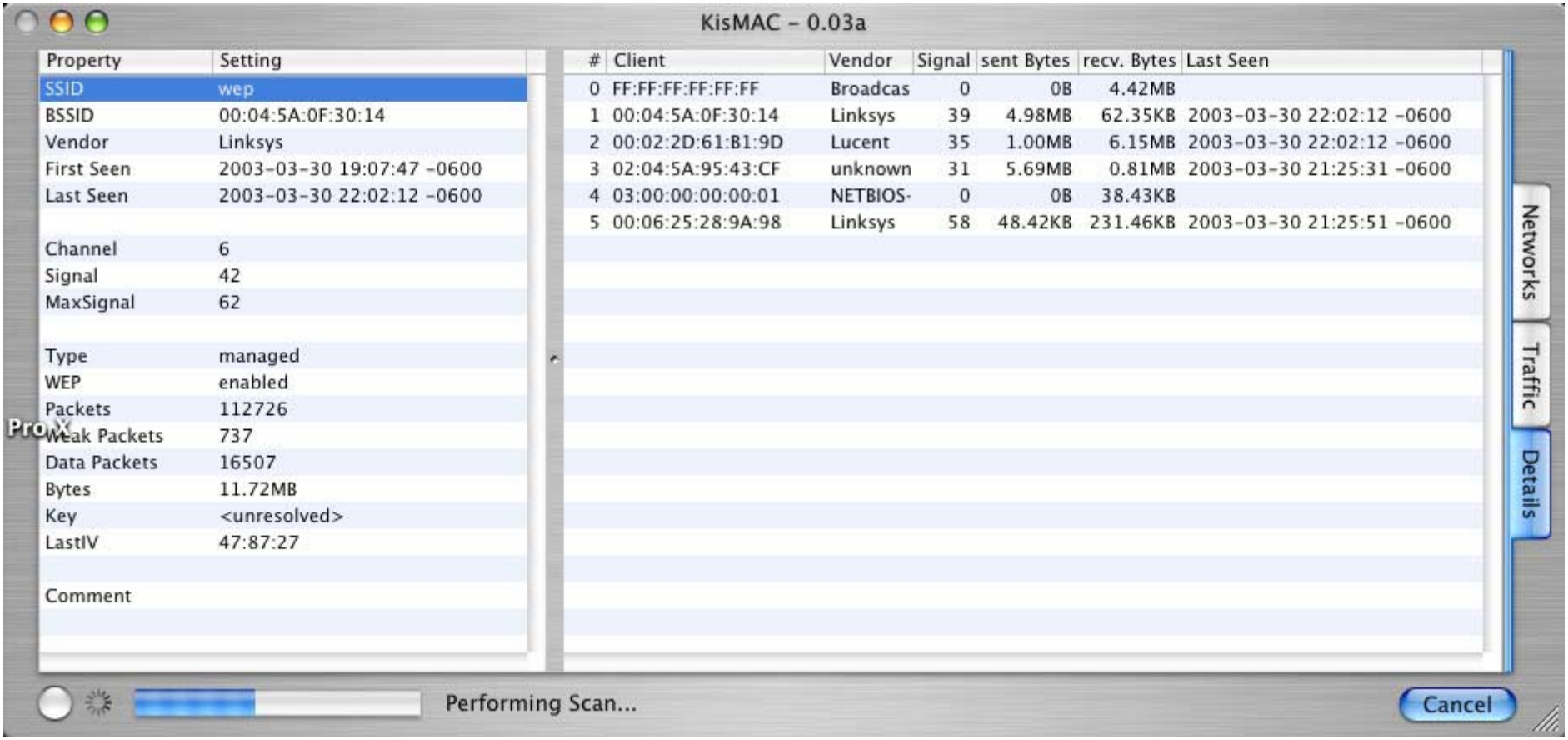
Atacando WEP

- Explotar las vulnerabilidades de la implementación de WEP en IEEE 802.11b:
  - colisiones del vector de inicialización (“Weak Scheduling attack)
  - brute-forcing (40 bits)
- Wired Equivalent Privacy
  - WEP utiliza un campo de 24 bits conocido como Vector de Inicialización (IV) que es utilizado como parte de la llave secreta compartida.
  - Sin embargo, el IV es incluido en el paquete en la porción de texto claro.
  - Debido a que el IV es solo de 24 bits (2^{24}=16,777,216)

Atacando WEP

- Un atacante lo que debe hacer es interceptar la cantidad de tráfico suficiente para capturar lo que se conoce como una colisión del IV, esencialmente la reutilización de un flujo de llave.
  - esta información puede ser utilizada para decifrar el tráfico.
- Se requiere entre 100MB y 1GB de información para que este ataque sea factible.

Atacando WEP



Airsnort

- Herramienta para wireless LAN que recupera llaves de encriptación.
- Opera rastreando las transmisiones que pasan por la red inalámbrica.
- Una vez que han sido enviados suficientes bloques de información calcula la llave de encriptación utilizada.
- Todas las redes de 802.11b con 40/128 bit WEP (Wired Equivalent Protocol) son vulnerables, ya que tienen numerosas grietas de seguridad.

¿Cuanta información requiere?

- AirSnort, junto con WEPCrack son las primeras implementaciones públicas de este tipo de ataque.
- Requiere interceptar aproximadamente de 100MB a 1GB de datos, una vez que los tiene, AirSnort puede adivinar la llave de encriptación utilizada en menos de un segundo.

Prerequisitos de Airsnort

- Linux, wlan-ng drivers, 2.4 kernels.
- Para compilar AirSnort se requiere:
  - fuente del Kernel
  - paquete de PCMCIA CS.
  - paquete de wlan-ng
  - patch wlan-monitor-airsnort
- AirSnort requiere el juego de chips Prism2,
  - las tarjetas que lo poseen son las únicas capaces de llevar a cabo el sniffing necesario.

¿Es posible obtener tantos datos?

- Negocio con cuatro empleados que utilizan el mismo password.
- Estos empleados navegan por la red todo el día
  - generando alrededor de 1,000,000 de bloques de información al día,
  - de los cuales aproximadamente 120 de ellos son débiles.
- Después de 16 días es casi seguro que la red haya sido crackeada.
- En este ejemplo la red no esta saturada
  - en el caso de una red saturada generalmente este tiempo se reduciría a un solo día.

Algunas observaciones

- Se esta atacando un *protocolo* que utiliza un *algoritmo de encripción*, no al algoritmo en si.
- Posibles acciones a tomar:
  - encriptar a niveles más altos del protocolo
  - actualizar a los estandares 802.11 cuando estos estén disponibles
  - tener cuidado con la generación de llaves
- RC4 es utilizado en otros protocolos “sin problemas”.

Otras herramientas

- KisMAC
- WepCrack
- Kismet
- ssidsniff
- WarDrive
- APTools
- AirIDS
- Wellenreiter

¿Y una vez conectado?

- Una vez que alguien ha logrado conectarse a una red inalámbrica todos los métodos de ataque en capa 2, capa 3, capa 4, ..., capa 7 son posibles:
  - Spoofing
  - Hijacking
  - Sniffing
  - DOS
  - Exploits
  - BruteForcing
  - Código Malicios (Worms)
  - ...

IEEE 802.11i

- IETF de la IEEE está trabajando en un nuevo estándar para redes inalámbricas, el IEEE 802.11i, que poseerá alta seguridad de manera intrínseca.
- Mientras no está preparado y los primeros dispositivos que lo implementan aparezcan en el mercado, los principales fabricantes, agrupados bajo la conocida alianza Wi-Fi, se han puesto de acuerdo en un estándar provisional de alta seguridad que ayuda a capear el temporal: WPA.

Wi-Fi Protected Access (WPA)

- Abril 2003
  - Más fuerte que WEP
  - Mejorable a través de nuevas versiones de software
  - Uso empresarial y casero
  - Obligatorio a finales del 2003
- Mejoras de Seguridad
  - TKIP (Temporal Key Integrity Protocol)
  - Autenticación de usuarios

WEP y WPA

Función	WEP	WPA
Encripción	Débil	Soluciona debilidades
Llaves	40 bits	128 bits
Llaves	Estáticas	Dinámicas
Llaves	Distribución manual	Automática
Autenticación	Débil	Fuerte, según 802.1x y EAP

Como actualizarse a WPA

- El uso de WPA requiere la actualización de todos los componentes que intervienen en una red inalámbrica,
  - los puntos de acceso,
  - las tarjetas de red inalámbricas,
  - los controladores de dispositivo y
  - el software que se instala en los equipos cliente
- En teoría WPA puede operar simultáneamente con equipos antiguos basados todavía en 802.11 y WEP,
  - desventaja de que las claves de cifrado no son dinámicas

Autenticación en Wireless

- Objetivo
  - solo las personas autorizadas pueden hacer uso de la red inalámbrica
- ¿Y los usuarios invitados?
- Opciones
  - LEAP
  - EAP-MD5
  - EAP-TLS
  - EAP-TTLS
  - EAP-PEAP

LEAP (EAP-Cisco Wireless)

- Lightweight Extensible Authentication Protocol
- Desarrollado por Cisco en 2000 para proporcionar autenticación para LANs 802.11
- Basado en nombre de usuario y contraseña
- Soporta plataformas Windows, Macintosh y Linux
- Patentado por Cisco (basado en 802.1x)
- El nombre del usuario se envía sin protección.
- La contraseña se envía se envía sin protección
- Requiere
  - LEAP “aware” RADIUS Server
  - Infraestructura Cisco Wireless

Otras opciones de autenticación

- EAP-MD5
  - basado en nombre de usuario y password
  - requiere llave fija WEP y no da distribución automática llaves
- EAP-TLS
  - desarrollado por Microsoft
  - distribución certificados a clientes y servidores RADIUS
- EAP-TTLS
  - usuarios se autentican mediante usuario/password
  - requiere certificados solo para servidores RADIUS
- EAP-PEAP
  - propuesto por Microsft/Cisco/RSA
  - no requiere certificados y usa TLS

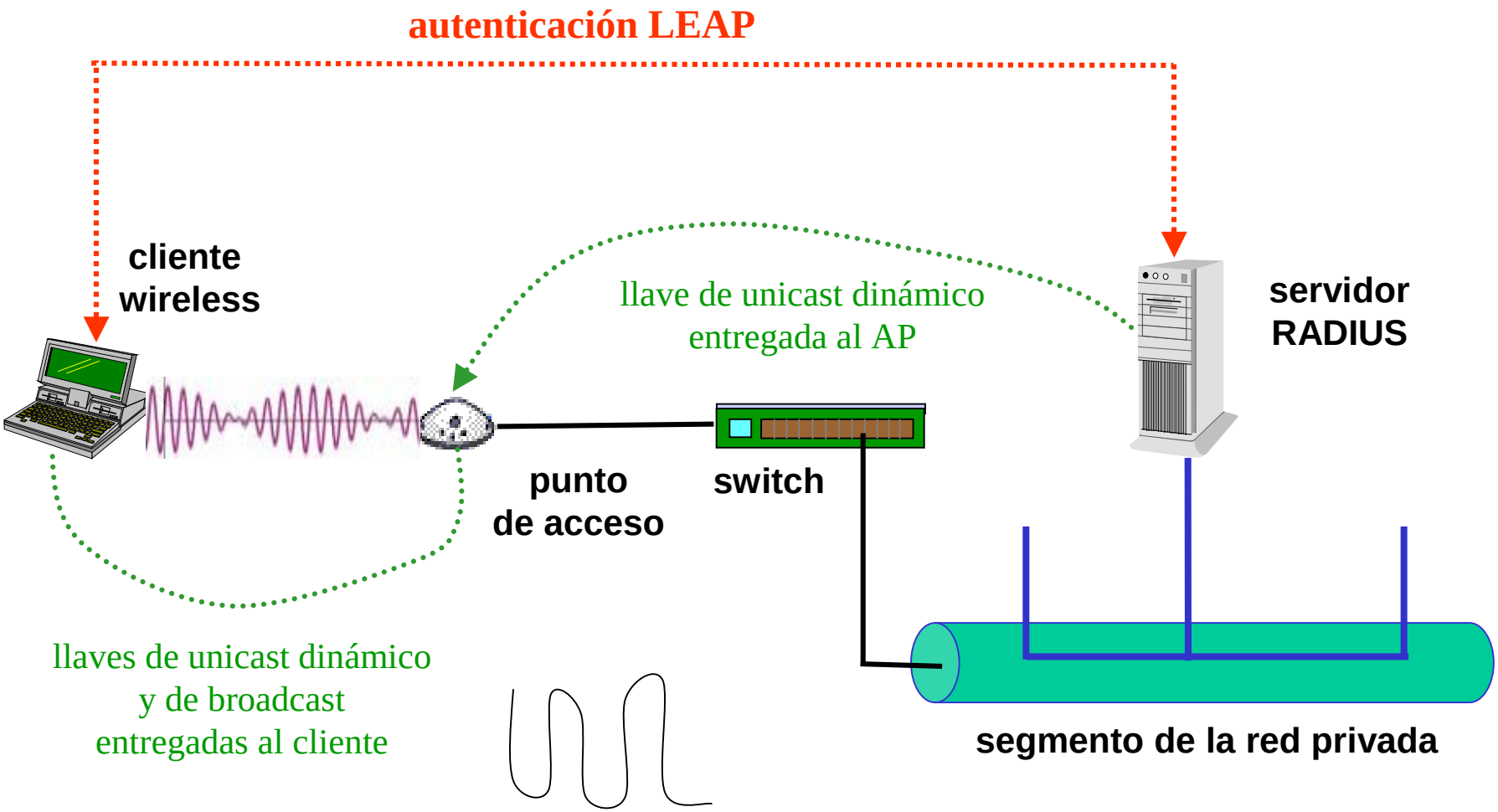
Comparativo protocolos EAP

Tema	EAP-MD5	LEAP (Cisco)	EAP-TLS (MS)	EAP-TTLS (Funk)	EAP-PEAP
Solución de seguridad	Estándar	Patente	Estándar	Estándar	Estándar
Certificados Cliente	NO	N/A	SI	NO (opcional)	NO (opcional)
Certificados Servidor	NO	N/A	SI	SI	SI
Credenciales Seguridad	Ninguna	Deficiente	Buena	Buena	Buena
Soporta Autenticación BD	requiere borrar BD	Active Directory, Dominios NT	Active Directory	Act. Dir. Token, SQL, Doms NT, LDAP	----------
Intercambio llaves dinámicas	NO	SI	SI	SI	SI
Autenticación mutua	NO	SI	SI	SI	SI

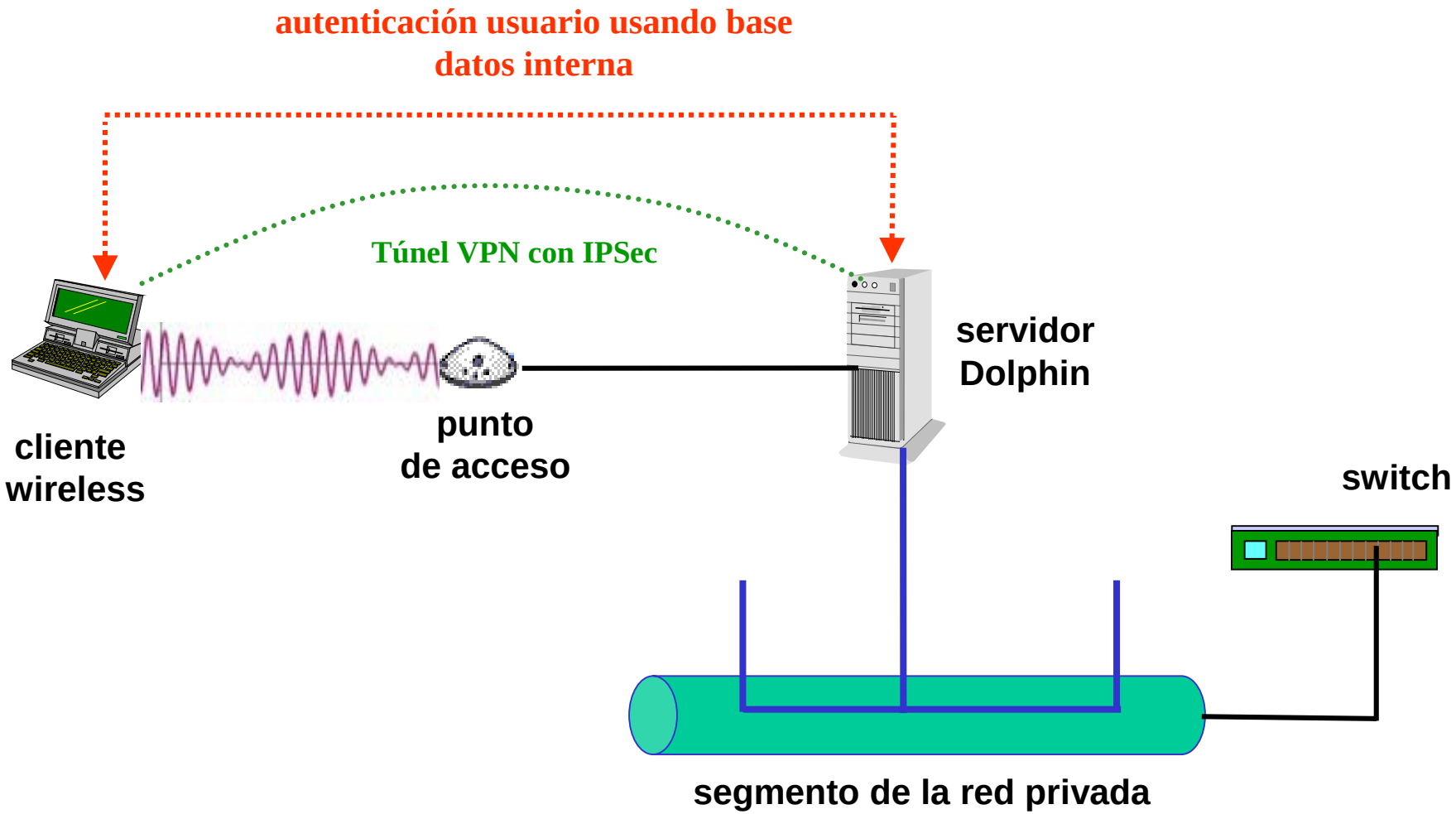
Consejos

- Habilitar WAP
  - si no es posible habilitar WEP con llave de 104 bits (128 bits)
- Conectar los Access Points en una zona de seguridad “pública” (ó de bajo riesgo) posiblemente en una DMZ, jamás conectar la red inalámbrica a la red alámbrica de manera transparente.
- Implementar un segundo nivel de seguridad:
  - VPN
  - IPSEC
  - SSL
  - SSH

Esquema autenticación RADIUS



Usando Simple Wireless Gateway para autenticación usuarios



Conclusiones

- El ambiente inalámbrico es una necesidad hoy en día.
- Tanto en ambiente alámbrico como inalámbrico existen riesgos
- La seguridad al 100% NO EXISTE
- Es deber del administrados planificar la red de acuerdo a las necesidades de la empresa.

Seguridad en Ambientes Inalámbricos

Roberto Gómez Cárdenas

rogomez@itesm.mx

http://webdia.cem.itesm.mx/ac/rogomez