Unidad VI: Tecnologías inalámbricas

Partamos de la definición de inalámbrico, este término se refiere al uso de la tecnología sin cables la cual permite la conexión de varios computadores entre sí.
Es así como se ha ido convirtiendo en uno foco de estudio para los temas de transmisión de datos, adquiriendo mayor interés en lugares donde no es posible la instalación de redes alámbricas.

El uso de esta tecnología inalámbrica permite dejar en el olvido de los cables sin la necesidad de dejar de establecer una conexión, desapareciendo las limitaciones de espacio y tiempo, dando la impresión de que puede ubicarse una oficina en cualquier lugar del mundo.

Una aplicación de este caso podría ser la relación que se establece entre empleados ubicados en un lugar que no sea su centro de labores y una red adquiriendo la empresa mayor flexibilidad. Los dispositivos son conectados a otros dispositivos inalámbricos con el fin de brindar a los trabajadores dinámicos una estrategia de trabajo más efectiva y con menos complicaciones.

Los aplicativos de escritorio también hacen que la carga de la red sea más ligera.
Usando la tecnología inalámbrica determina que la empresa incremente su productividad y eficacia, de este modo el empleado se dedica exclusivamente a lo que sabe hacer mejor, evitando los inconvenientes de tipo tecnológico.

3.1 Clasificación de redes inalámbricas:
PAN, LAN, WAN

Red de área personal (PAN): Wireless Personal Área Networks, Red Inalámbrica de Área Personal o Red de área personal o Personal área network es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a Internet, teléfonos celulares, PDA, dispositivos

de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella.

Red de área local (LAN): Una red de área local, o red local, es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de hasta 100 metros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

Redes de área local (WAN): red de área amplia interconectan equipos en un entorno muy amplio, como un país usando la red telefónica

3.2 Estándares y protocolos de comunicación:
Bluetooth, Infrarrojo, Wi-Fi, Wi-Max

Estándares WPAN

1. El grupo de trabajo 802.15.1 realiza el estándar basado en las especificaciones del SIG de Bluetooth. Este grupo de trabajo publicó el estándar IEE 802.15.1 el 14 de junio de 2002.
2. El grupo de trabajo 802.15.2 desarrolló un modelo de coexistencia entre las WLAN y WPAN, así como de los aparatos que las envuelven.
3. El grupo de trabajo 802.15.3. Trabaja para establecer los estatus y publicar un estándar nuevo de alta velocidad para WPANs. Además de ofrecer una alta velocidad de transmisión, este estándar está diseñado para consumir

poca energía y ofrecer soluciones a bajo costo así como aplicaciones multimedia.

4. El grupo de trabajo T4 para el desarrollo IEEE 802.15.4, investiga y desarrolla soluciones que requieren una baja transmisión de datos y con ello una duración en las baterías de meses e incluso de años así como una complejidad relativamente baja. Dicho grupo de trabajo ha publicado el estándar que lleva su nombre; IEEE 802.15.4

Estándares WLAN

802.11a Permite realizar transmisiones con velocidades de hasta 54 Mbps y opera sobre la banda de 5 GHz, el alcance aproximado para este estándar es de 25m.

802.11b Soporta velocidades en condiciones ideales de hasta 2.4 a 2.5 MHz, y tiene un alcance de hasta 50m.

802.11g Opera con potencias de hasta medio vatio y antenas parabólicas, tiene un alcance de 50 km.

80211n Se prevé que tendrá una velocidad de 100 Mbps y trabajar con frecuencias de 2.4 y 5 GHz.

80211e El objetivo del estándar es definir los requisitos de diferentes paquetes de cuanto al ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y video.

802.11f Le permite al usuario itinerante cambiarse claramente de un punto de acceso al otro mientras está en movimiento sin importar que marcas de punto de acceso se usen en la estructura de la red.

Tabla comparativa estándares

	Estándar	Uso	Capacidad de proceso	Alcance	Frecuencia
UWB	802.15.3a	WPAN	De 110 a 480 Mbps	Hasta 10 metros	7,5 GHz
Bluetooth	802.15.1	WPAN	Hasta 720 Kpbs	Hasta 10 metros	2,4 GHz
Wi-Fi	802.11a	WLAN	Hasta 54 Mbps	Hasta 100 metros	5 GHz
Wi-Fi	802.11b	WLAN	Hasta 11 Mbps	Hasta 100 metros	2,4 GHz
Wi-Fi	802.11g	WLAN	Hasta 54 Mbps	Hasta 100 metros	2,4 GHz
WiMAX	802.16d	WMAN fija	Hasta 75 Mbps (20 MHz AB)	Aprox. de 6 a 10 Km.	Sub 11 GHz
WiMAX	802.16e	WMAN portátil	Hasta 30 Mbps (10 MHz AB)	Aprox. de 1,5 a 5 Km.	De 2 a 6 GHz
Edge	2.5G	WWAN	Hasta 384 Kbps	Aprox. de 1,5 a 8 Km.	1900 MHz
CDMA2000/1 x EV-DO	3G	WWAN	Hasta 2,4 Mbps (aprox. de 300 a 600 Kbps)	Aprox. de 1,5 a 8 Km.	400, 800, 900, 1700, 1800, 1900, 2100 MHz
WCDMA/UMTS	3G	WWAN	Hasta 2 Mbps (hasta 10 Mbps con tecnología HSDPA)	Aprox. de 1,5 a 8 Km.	1800, 1900, 2100 MHz

3.3 Dispositivos y configuración

El uso de dispositivos inalámbricos para formar redes de área local con computadores moviles (e.g portátiles) es cada vez más común, después de la estandarización del protocolo IEEE 802.11b.

Esto ha permitido que los precios de dispositivos que lo soportan haya disminuido. En estas redes móviles hay un "punto de acceso" "en inglés acces point" que se conecta a una red Ethernet y que puede comunicarse con tarjetas especiales instaladas en cada computador portatil; para efectuar la comunicación se emplean

ondas electromágnéticas de baja potencia a una frecuencia de 2.4GHz"Para comparar, por ejemplo, las emisoras AM en Colombia emplean frecuencias entre 535Khz y los 1.705Khz".

El Ministerio de telecomunicaciones tiene claramente estipulado el uso de este tipo de frecuencia, según la Resolución 797 de 8 de Junio de 2001 artíiculo 3 tabla 3.6. Según el cual podemos como colegio con propósito de educación o en ambientes de investigación emplear este espacio radioeléctrico sin necesidad de tributar.

Dependiendo de la potencia del punto de acceso, cada portatil puede separarse hasta una distancia máxima del punto de acceso (120 mt. en el caso del Intel 2011A con línea de vista a 11MBps), la velocidad de transmisión máxima es de 11Mbps "La velocidad de una red Ethernet típica como la del colegio es 10Mbps, aunque cada vez son más populares de 100Mbps y existen de 1000Mbps"}, sin embargo en la práctica la velocidad es menor porque depende de condiciones climáticas y disminiye si hay obstáculos (e.g paredes) entre punto de acceso y portátil.

Los puntos de acceso y las tarjetas pueden encriptar/desencriptar información con el esquema WEP (Wired Equivalent Privacy) "El esquema WEP no es seguro por lo que deben emplearse otras aplicaciones para mejorar privacidad (e.g IPsec a nivel de IP, ssh, Kerberos en el caso de TCP o Radius para autenticación).".

Puede consultarse más sobre redes móviles con este protocolo por ejemplo en: http://www.cis.ohio-state.edu/~jain/cis788-97/wireless_lans/index.htm|

Algunos puntos de acceso, además de ofrecer la funcionalidad descrita, pueden conectarse inalámbricamente con otro punto de acceso y funcionar como puente entre dos redes de área local. Puede amplificarse la señal de alguno (o de ambos) puntos de acceso empleando antenas, por ejemplo si están muy separados o si hay obstáculos entre ellos.

Existen antenas omnidireccionales y unidireccionales, las primeras emiten y captan señales que no necesitan una dirección específica para establecer la comunicación vía inalámbrica, por otra parte las segundas necesitan estar colocadas de forma tal que apunten hacia el lugar con el cuál se desea establecer el enlace.

Adicionalmente las antenas dependiendo de su especificación pueden tener distintas potencias, que eventualmente pueden emplear unos amplificadores de señal para maximizar su alcance.

Importación de dispositivos

Cuando se compran dispositivos con tarjeta de crédito, generalmente los bancos dueños de las tarjetas cobran la tasa de cambio en el momento en el que se hace efectivo el cobro, no en la fecha de compra, y dado que el peso colombiano frente al dólar se mantiene en una continua decadencia, los costos siempre son más altos que los presupuestados inicialmente.

Adicionalmente a los costos de envío de las compras hechas por Internet la Dirección de Impuestos y Aduanas Nacionales DIAN cobra un porcentaje sobre el costo del equipo a importar.

3.4 Mecanismos y protocolos de seguridad: WEP, WAP, WPA-PSK, WEP2, Filtrado de MACs.

- **R.I.P. WEP**

WEP (Wired Equivalent Privacy) fue el primer protocolo de encriptación introducido en el primer estándar IEEE 802.11 allá por 1999. Está basado en el algoritmo de encriptación RC4, con una clave secreta de 40 o 104 bits, combinada con un *Vector de Inicialización* (IV) de 24 bits para encriptar el mensaje de texto *M* y su

checksum – el ICV (*Integrity Check Value*). El mensaje encriptado *C* se determinaba utilizando la siguiente fórmula:

$$C = [\ M \ ||\ \text{ICV}(M)\ ] + [\ \text{RC4}(K \ ||\ \text{IV})\ ]$$

donde || es un operador de concatenación y + es un operador XOR. Claramente, el vector de inicialización es la clave de la seguridad WEP, así que para mantener un nivel decente de seguridad y minimizar la difusión, el IV debe ser aplicado a cada paquete, para que los paquetes subsiguientes estén encriptados con claves diferentes. Desafortunadamente para la seguridad WEP, el IV es transmitido en texto simple, y el estándar 802.11 no obliga a la incrementación del IV, dejando esta medida de seguridad como opción posible para una terminal inalámbrica particular (punto de acceso o tarjeta inalámbrica).

Tabla 1. *Cronología de la muerte de 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.

IEEE 802.1X y EAP

El protocolo de autenticación IEEE 802.1X (también conocido como *Port-Based Network Access Control*) es un entorno desarrollado originalmente para redes de cable, y posee mecanismos de autenticación, autorización y distribución de claves y además incorpora controles de acceso para los usuarios que se unan a la red. La arquitectura IEEE 802.1X está compuesta por tres entidades funcionales:

- El suplicante que se une a la red,
- El autenticador que hace el control de acceso,
- El servidor de autenticación que toma las decisiones de autorización.

Fase 1: Acuerdo sobre la política de seguridad

La primera fase requiere que los participantes estén de acuerdo sobre la política de seguridad a utilizar. Las políticas de seguridad soportadas por el punto de acceso son mostradas en un mensaje *Beacon* o *Probe Response* (después de un *Probe Request* del cliente). Sigue a esto una autenticación abierta estándar (igual que en las redes TSN, donde la autenticación siempre tiene éxito). La respuesta del cliente se incluye en el mensaje de *Association Request* validado por una *Association Response* del punto de acceso. La información sobre la política de seguridad se envía en el campo RSN IE (*Information Element*) y detalla:

- Los métodos de autenticación soportados (802.1X, Pre-Shared Key (PSK)),
- Protocolos de seguridad para el tráfico unicast (CCMP, TKIP etc.) – la suit criptográfica basada en pares,
- Protocolos de seguridad para el tráfico multicast (CCMP, TKIP etc.) – suit criptográfica de grupo,
- Soporte para la pre-autenticación, que permite a los usuarios.

Fase 2: autenticación 802.1X

La segunda fase es la autenticación 802.1X basada en EAP y en el método específico de autenticación decidido: EAP/TLS con certificados de cliente y

servidor (requiriendo una infraestructura de claves públicas), EAP/TTLS o PEAP para autenticación híbrida (con certificados sólo requeridos para servidores), etc. La autenticación 802.1X se inicia cuando el punto de acceso pide datos de identidad del cliente, y la respuesta del cliente incluye el método de autenticación preferido.

Fase 3: jerarquía y distribución de claves

La seguridad de la conexión se basa en gran medida en las claves secretas. En RSN, cada clave tiene una vida determinada y la seguridad global se garantiza utilizando un conjunto de varias claves organizadas según una jerarquía. Cuando se establece un contexto de seguridad tras la autenticación exitosa, se crean claves temporales de sesión y se actualizan regularmente hasta que se cierra el contexto de seguridad. La generación y el intercambio de claves es la meta de la tercera fase.