Aplicación de tecnologías Wireless para operativas en situaciones de emergencia

Javier Coso - Mayo 2007

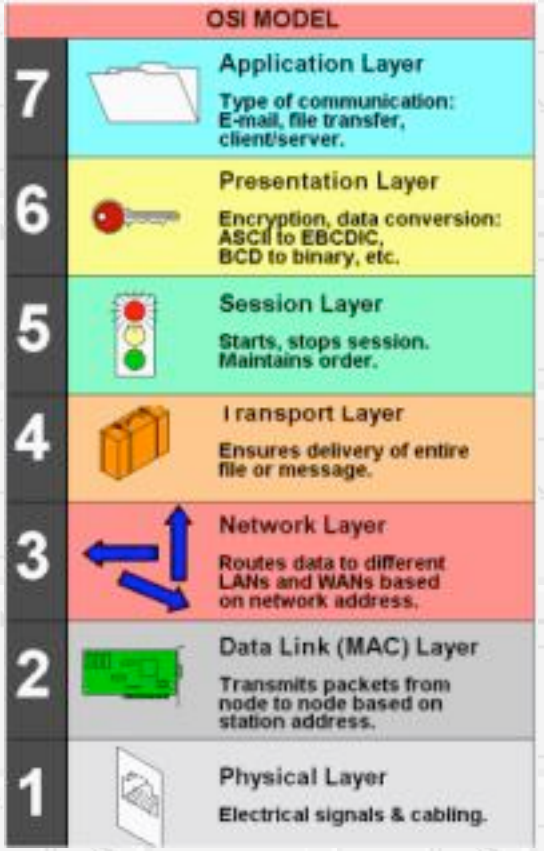
Dirección General de Protección Civil y Emergencias - Red Radio de Emergencia

Aplicación de tecnologías WiFi
Introducción

- **Wireless**: Tipo de comunicación en la que se utiliza como medio de propagación la modulación de las ondas electromagnéticas.

- **WiFi** (**WI**reless **FI**delity): Conjunto de estándares para redes inhalambricas basados en las especificiaciones IEEE-802.11.

- **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork): Red de área local inhalámbrica.

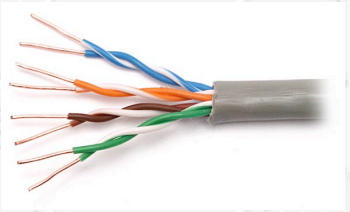


Aplicación de tecnologías WiFi
Historia I

- ★ Problema principal: Resolver la compatibilidad.
- ★ 1999 surge la WECA (Wireless Ethernet Compability Aliance): Asociación de principales vendedores de soluciones inhalámbricas (3com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies).
- ★ Aparición de la marca WiFi bajo la norma IEEE-802.11b

Aplicación de tecnologías WIFI
Historia II

★ La norma IEEE-802.11 surge para suplir a las capas físicas y MAC de la norma IEEE-802.3 (Ethernet).



★ Lo único que diferencia una red WiFi de una red Ethernet es la manera de acceder a la red por lo que es completamente compatible una red WiFi con todos los servicios de una red Ethernet.

★ Tipos de WIFI, basados en el estandar IEEE-802.11:

Denominación	Banda	Velocidad máxima
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz	+ 600 Mbps
802.11a	5 GHz	54 Mbps

★ Principal problema: SEGURIDAD.

★ Alternativas para garantizar la seguridad de estas redes:

- Protocolos de cifrado para estándares WiFi que se encargan de codificar la información transmitida (WEP, WPA).
- Cifrado en la capa de transporte (SSL y TSL).

★ WEP (Wired Equivalent Privacy):

- Basado en el algoritmo de cifrado RC4.
- Claves de 64 bits o 128 bits.
- Es inseguro debido a su implementación. Aumentando el tamaño de la clave sólo aumentamos el tiempo para romperla.
- Es posible alterar la información y el CRC del mensaje sin conocer la clave WEP.
- Cualquier sistema lo implementa y es fácil de configurar.

★ WPA (WiFi Protected Access):

- WPA no elimina el cifrado de WEP, lo fortalece.
- Creado para utilizar un servidor RADIUS que centralice las claves. Se puede usar en un modo menos seguro a través de claves pre-compartidas.
- Basado en el algoritmo de cifrado RC4.
- Claves de 128 bits y vector de iniciación de 48 bits.

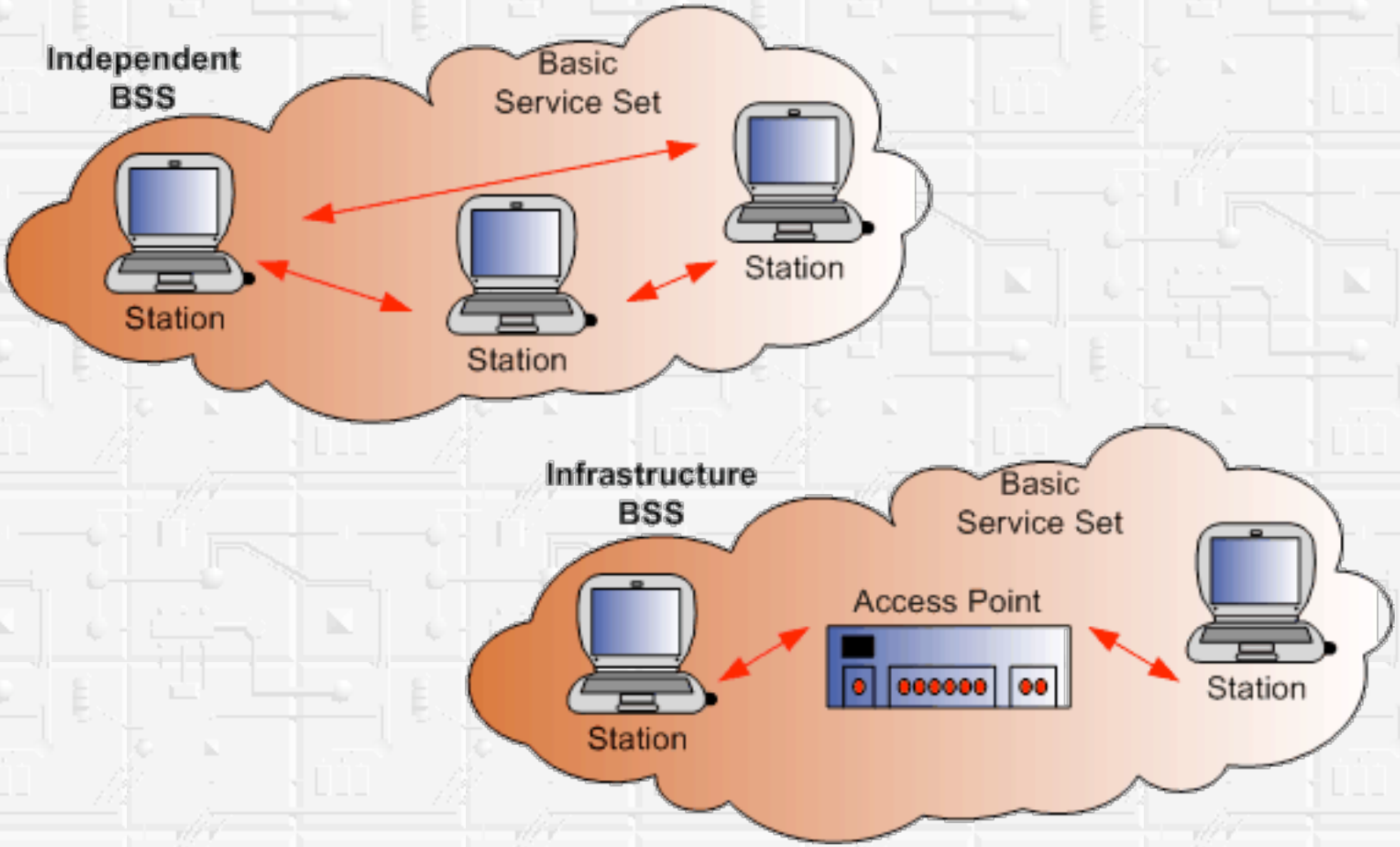
★ WPA (cont.):

- Se mejora también la integridad de la información cifrada. Se implementa un código de integridad de mensaje (MIC), conocido como “Michael”.
- Protección contra ataques de “repetición”, a través de un contador de tramas.

★ SSL (Secure Socket Layer) y TLS (Transport Layer Security):

- Seguridad en la capa de transporte.
- Proporciona autenticación y privacidad de la información entre extremos.
- Habitualmente el servidor es el autenticado (se garantiza su identidad).
- Se necesita de un intercambio de claves públicas y autenticación basada en certificados digitales.
- Cifrado del tráfico basado en cifrado simétrico.

Aplicación de tecnologías WIFI
Tipos de redes I



Redes independientes o Ad-hoc

★ Cada equipo se conecta directamente con el otro por lo que deben estar en el rango de cobertura.

★ Muy usada para redes de corta vida.

Red en modo infraestructura

- ★ Se utiliza un punto de acceso (AP) para conectar los diferentes equipos.
- ★ Se debe establecer comunicación con el AP para poder conectarse a la red.
- ★ Los equipos sólo pueden conectarse a un AP.

Aplicación de tecnologías WIFI
Posibilidades

- ★ Posibilidad de acceder a servicios de VoIP, mail, mensajería...
- ★ No hace falta tener que cablear ningún área para dar conectividad a los equipos.
- ★ Se pueden utilizar diversos equipos como clientes: ordenadores de sobremesa, portátiles, ordenadores de bolsillo, teléfonos...
- ★ Con una red "troncal" es fácil ampliar el área de cobertura.
- ★ Acceso a la información on-line desde cualquier punto de la zona de cobertura.
- ★ Grandes posibilidades de cifrado.

Aplicación de tecnologías Wireless para operativas en situaciones de emergencia

Gracias por su atención

Javier Coso Gutiérrez
<coso@turcel.com>