Redes inalámbricas y móviles

7.1 Introducción

Elementos de una red inalámbrica:

- **Host inalámbricos**: dispositivos que actuan como sistemas terminales y que ejecutan las aplicaciones (Laptop, celular, tablet, PC). Pueden ser movibles o no.

- **Enlaces inalámbricos**: Un host se conecta a una estacion base u otro host inalámbrico por medio de un enlace de comunicaciones inalámbrico. Dos caracteristicas clave: area de cobertura y velocidad del enlace. Ademas posee tasas de errores de bit y las causas de esos errores.

- **Estacion base**: parte clave de la red inalámbrica. Es responsable de enviar y recibir datos(paquetes) hacia y desde un host inalámbrico que está asociado con esa estacion base. Es la responsable de coordinar la transmision de los multiples host inalámbricos que estén asociados a ella, es decir que:
    - El host se encuentra dentro de la distancia de comunicacion inalambria de la estacion base
    - El host utiliza la estacion base para reenviar datos hacia y desde la red de mayor tamaño

  Ejemplos de estacion base: Las torres de telefonia de los celus y los puntos de acceso en la redes LAN inalámbricas wifi

  De los host asociados con una estacion base se suele decir que operan en **modo infraestructura** puesto que todos los servicios de red tradicionales son proporcionados por la red con la que un host se conecta a traves de la estacion base.

  En las **redes ad hoc** los hosts inalámbricos no tienen ninguna infraestructura de ese tipo a la que conectarse. sino que los host se comunican entre ellos directamente.

  Cuando un host movil se desplaza por fuera del alcance de una estacion base y entra en el area de cobertura de otra cambia su conexion a la red mayor, es decir, cambia la estacion base a la que estaba asociada. Este proceso se lo conoce como **transferencia(handoff)**

- Infraestructura de red: es la red de mayor tamaño con la que un host inalámbrico puede comunicarse

Clasificación de las redes

Se pueden clasificar las redes segun dos criterios:

1. Si dentro de la red inalámbrica realiza un salto inalámbrico o varios
2. Si existe una infraestructura

Redes basadas en infraestructura y un solo salto: Estas redes tienen una estacion base conectada a una red cableada de mayor tamaño

Redes sin infraestructura y con un solo salto: No existe una estacion base conectada a una red inalámbrica. Uno de los nodos actua como coordinador de los demás. Ej: bluetooth

Redes basadas en infraestructura y multiples saltos: Existe una estacion base conectada a una red de mayor tamaño. Sin embargo, algunos nodos pueden transmitir sus comunicaciones a tarves de otros nodos inalambricos.Las redes de malla inalámbrica caen en esta categoría.

Redes sin infraestructura y multiples saltos: No existe una estacion base y los nodos pueden tener que transmitir sus mensajes a traves de otros diversos nodos para alcanzar cierto destino. Los nodos también pueden ser móviles, con lo que la conectividad entre los nodos irá variando: redes móviles ad hoc

7.2 Caracteristicas de las redes y enlaces inalambricos

Diferencias entre un enlace cableado y un enlace inalámbrico:

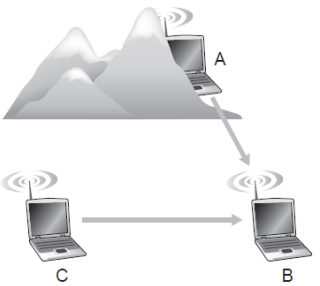
- **Intensidad decreciente de la señal**: las señales inalámbricas se ven afectadas de forma importante cuando se propagan por objetos sólidos. Lo que genera que la señal descresca (pérdida de propagacion) a medida que se incrementa la distancia entre el emisor y el receptor.
- **Interferencia de otros origenes**: Las señales inalámbricas son muy susceptibles a la interferencia. Ejemplo: el ruido electromagnetico del entorno o telefonos inalambricos a 2,4 con redes lan inalámbricas wifi
- **Propagacion multicamino (multipath)**: Partes de la onda electromagnética se reflejan en los objetos y en el suelo, tomando caminos de diferentes longitudes entre un emisor y un receptor. Esto hace que se “difumine” (blurring) la señal recibida en el receiver.

Como los errores de bits son más comunes en los enlaces inalámbricos, los protocolos de enlace inalámbrico emplean CRC y las capas superiores deberán emplear mecanismos RDT para poder reenviar los frames corruptos.

SNR (Señal-ruido): es una **medida** relativa **de la intensidad de la señal recibida** (es decir de la informacion que se está transmitiendo) y de este ruido. Se mide en decibelios(dB). Cuanto mayor sea la relacion SNR, más fácil le será al receptor extraer la señal transmitida del ruido de fondo.

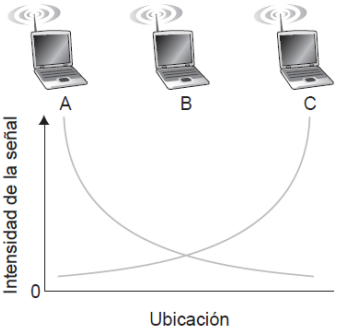
BER(Bit Error Rate): es la probabilidad de que un bit transmitido llegue de forma errónea al receptor. Para un determinado esquema de modulacion, cuanto mayor es la SNR menor es la BER

Problemas comunes: generan que puedan ocurrir colisiones indetectables.



Problema del terminal oculto
A y C transmiten a B, por las **obstrucciones fisica** presentes en el entorno pueden impedir que A y C escuchen las transmisiones del otro y esto genera intervenciones cuando mandas sus paquetes.

Desvanecimiento
A y C están colocadas de forma que sus señales no son lo suficientemente intensas como para que puedan ambas estaciones detectar las transmisiones de las otras a pesar de que si tienen la intensidad suficiente para ser esuchadas por B.
Esto ocurre porque la intensidad de la señal se va desvaneciendo a medida que se propaga a traves del medio inalámbrico.



7.2.1 CDMA Code Division Multiple Access

Es un protocolo que pertenece a la familia de protocolos de particionamiento del canal que coordina el acceso de transmision de tramas al canal de difusion para que sea lo más eficiente.

Le asigna a cada usuario un código unico. A cada usuario se le asigna la misma frecuencia de transferencia pero antes de transferir la data, debe encodear la informacion utilizando el código asignado. Luego los receptores utilizan el mismo código para desencodear la inforacion

CDMA funciona bajo la suposicion de que las señales interferentes de los bits transmitidos son aditivas. Esto permite tener multiples sender enviando tramas ya que eligiendo bien los codigos, cada receptor puede recuperar los datos enviados por un emisor a partir de esta señal agregada utilizando el mismo código del emisor.

CDMA es un protocolo de particionamiento ya que particiona el espacio de codigos y asigna a cada nodo una parte dedicada de ese espacio de codigos.

7.3 WiFi: redes LAN inalámbricas 802.11

Las redes LAN inalámbricas son hoy en día una de las tecnologias más importantes de redes de acceso para internet.

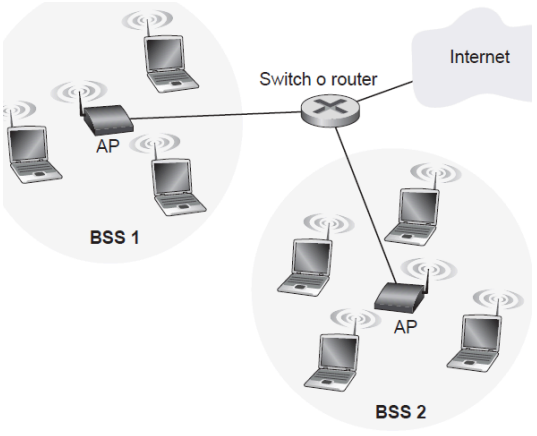
Existen varios estándares de WIFI donde todos emplean el mismo protocolo de acceso al medio CSMA/CA (carrier senses multiple access Collision Avoidance). Todos utilizan la misma estructura de trama para sus tramas de la capa de enlace y tienen la capacidad de reducir su velocidad de transmision con el fin de alcanzar mayores distancias.

Entre sus diferencias podemos encontrar que utilizan distintos rangos de frecuencia:

- a 2.4 es una frecuencia sin licencia, compiten con el espectro de frecuencia de telefono a 2.4 GHZ
- a 5 GHZ, las redes lan 802.11(wifi) proporcionan una distancia de transmisión más corta para un determinado nivel de potencia y se ven más afectadas por la propagacion multicamino.

7.3.1 La arquitectura Wifi (802.11)

El componente fundamental de la arquitectura wifi es el **conjunto de servicio basico (BSS)**. Un BSS contiene una o más estaciones inalámbricas y una estacion base central llamada **punto de acceso** (AP).
Los puntos de acceso se interconectan a un dispositivo de interconexion (como un switch o router) que a su vez lleva hacia internet.
En una red doméstica típica existirá un punto de acceso y un router (normalmente integrados en una misma unidad), que conectarán el BSS con Internet



Cada estacion inalámbrica tiene una direccion MAC de 6 bytes que está almacenada en la tarjeta adaptadora de la estacion. Cada punto de acceso también tiene una direccion MAC para su interfaz inalámbrica.

Las redes LAN inalámbricas que incorporan puntos de acceso suelen denominarse **redes LAN inalámbricas de infraestructura**.
Las estaciones IEEE 802.11 también se pueden agrupar para formar una red ad hoc: una red sin ningún control central y que no tiene conexiones con el "mundo exterior". En este caso, la red es formada "sobre la marcha" por una serie de dispositivos móviles que se han encontrado con que están próximos entre sí,

Canales y asociacion

En wifi, cada estacion inalámbrica necesita asociarse con un punto de acceso antes de poder enviar o recibir datos de la capa de red.

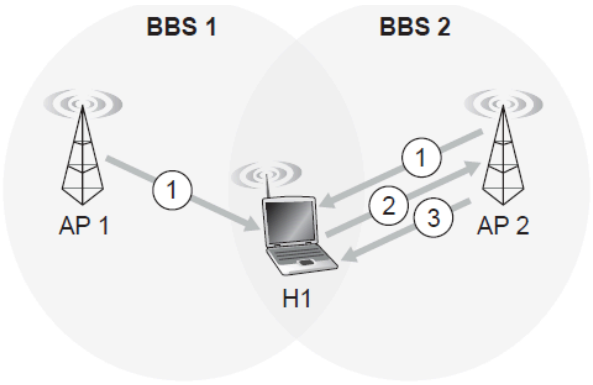
Cuando un administrador de red instala un punto de acceso, asigna un **Identificador de service set (SSID)** de una o dos palabras a ese punto de acceso. También debe asignar un número de canal a ese punto de acceso.

Wifi define 11 canales parcialmente solapados. Dado dos canales cualquiera diremos que no están solapados si y sólo si están separados por 4 o más canales. En particular, el conjunto de canales 1, 6 y 11 es el único conjunto de tres canales no solapados. Entonces un administrador podria crear una red LAN inalámbrica con una velocidad máxima de transmision de 33 Mbps instalando 3 puntos de acceso en la misma ubicacion fisica asignando los canales 1,6 y 11 a los puntos de acceso e interconectando todos los puntos de acceso mediante un switch.

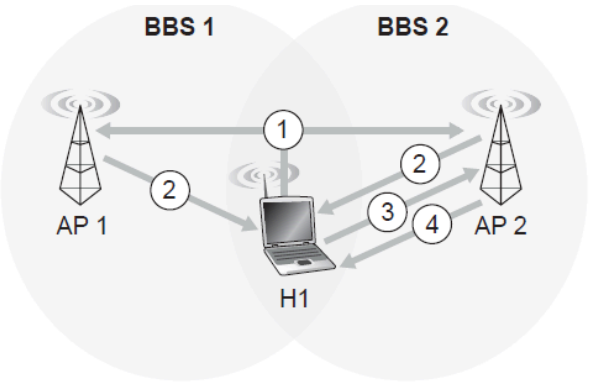
Una **jungla WiFi** es cualquier ubicaciones fisica en la que **una estacion inalámbrica** está **recibiendo** una **señal** suficientemente **intensa desde dos o más puntos de acceso.** Si quisiéramos entrar a una jungla debemos **asociarnos** a algun punto de acceso. Asociarse quiere decir que se crea un cable virtual entre el mismo y el punto de acceso. Así nuestro telefono recibira y enviará frames desde el punto de acceso

Para enterarnos de que existen estos puntos de acceso, se requiere que un punto de acceso envíe de forma periodica **tramas baliza** (beacon frames) donde cada una incluye **la direccion MAC y el identificador SSID** del punto de acceso. El dispositivo inalámbrico, explora los 11 canales buscando tramas baliza de cualquier punto de acceso cercano. Luego el dispositivo selecciona uno de los puntos de acceso para asociarse. Generalmente el dispositivo elige el punto de acceso con mayor intensidad de señal (aunque no garantiza que su rendimiento sea el máximo ya que puede estar sobrecargado de otros dispositivos)

Exploracion pasiva y activa



a. Exploración pasiva
1. Tramas baliza enviadas desde los puntos de acceso (AP).
2. Envío de la trama de solicitud de asociación desde H1 al AP seleccionado.
3. Envío de la trama de respuesta de asociación desde el AP seleccionado a H1.



a. Exploración activa
1. Difusión desde H1 de una trama de solicitud de sondeo.
2. Envío de tramas de respuesta de sondeo desde los AP.
3. Envío de trama de solicitud de asociación desde H1 al AP seleccionado.
4. Envío de trama de respuesta de asociación desde el AP seleccionado a H1

El proceso de exploración de los canales y de escucha de las tramas baliza se conoce con el nombre de **exploración pasiva**. Un dispositivo inalámbrico también puede realizar una **exploración activa**, difundiendo una trama de sondeo que será recibida por todos los puntos de acceso que caigan dentro del alcance del dispositivo inalámbrico

Una vez que el dispositivo se asocia a un AP, va a querer unirse a la subred a la que pertenece el AP. En general, envía un mensaje DHCP a la subred a través de la AP para obtener la IP, y una vez que obtiene esa IP el resto del mundo va a ver al dispositivo simplemente como un host más con una IP de esa subred.

7.3.2 El protocolo MAC WiFi

Una vez asociado un dispositivo inalámbrico con un punto de acceso, el dispositivo puede comenzar a enviar y recibir frames de datos hacia y desde el punto de acceso.

Dado que múltiples dispositivos inalámbricos, o el propio punto de acceso, pueden desear transmitir tramas de datos al mismo tiempo a través del mismo canal, es preciso utilizar un protocolo de acceso múltiple para coordinar esas transmisiones. WiFi utiliza el protocolo de acceso aleatorio llamado **CSMA/CA** (CARRIER SENSE MULTIPLE ACCESS Collision Avoidance).

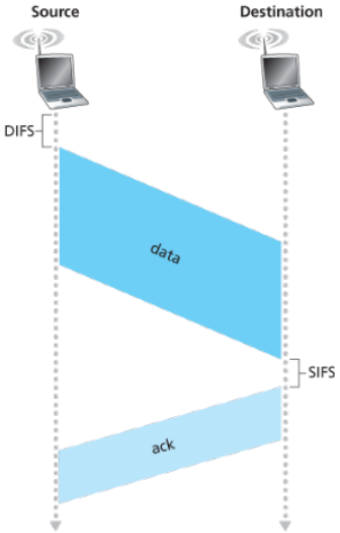
“estaciones” = dispositivos o a los puntos de acceso inalámbricas que comparten el canal de acceso múltiple

Cada estacion sondea el canal antes de transmitir y se abstiene de transmitir cuando detecta que el canal está ocupado.

A diferencia de ethernet, en WiFi en vez de detectar colisiones, las **evitan**.
¿Por qué no detecta colisiones? Por los problemas de terminal oculto y desvanecimiento.

Tecnicas para evitar colisiones

Protocolo CSMA/CA WiFi:
Suponga que una estación (estación inalámbrica o punto de acceso) dispone de una trama para transmitir.



1. Si la estación detecta inicialmente que el canal está inactivo, transmite la trama después de un corto periodo de tiempo (**DIFS**)
2. En caso contrario, espera un valor de espera (**backoff**) **aleatorio.** Cuando detecta que el canal está ocupado, el valor del contador permanece congelado.
3. Cuando el **contador** alcanza el valor **cero**, la estación **transmite** la trama completa y luego **espera** a recibir un **reconocimiento**. (*)
4. Si recibe el ACK sabe que su trama fue recibida correctamente. Si no, vuelve a entrar en la fase de backoff del paso 2, con un tiempo más largo.
    a. Si la estación transmisora no recibe una trama de reconocimiento dentro de un periodo de tiempo especificado retransmite la trama.
    b. Si no se recibe después de un número fijo de retransmisiones, la descarta.

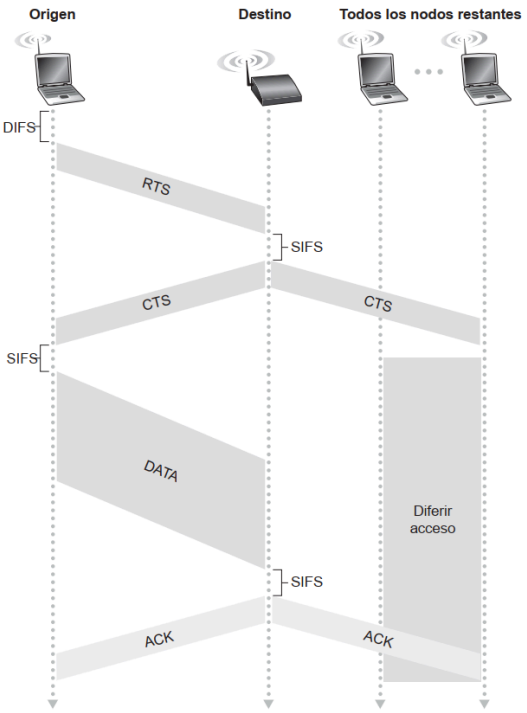
(*) Cuando la estación de destino recibe una trama que pasa la prueba de comprobación de CRC, espera un corto periodo de tiempo **SIFS** (Short Inter-frame Spacing) y luego devuelve una trama de reconocimiento.

El objetivo de CSMA/CA es evitar las colisiones siempre que sea posible. Si las dos estaciones detectan que el canal está ocupado ambas esperan aleatoriamente. Si dichos valores de backoff son distintos, una vez que el canal pase a estar inactivo una de las dos estaciones empezará a transmitir antes que la otra y (si las dos estaciones no están ocultas a ojos una de otra) la "estación perdedora" escuchará la señal de la estación "ganadora", congelará su cuenta atrás y se abstendrá de transmitir hasta que la estación ganadora haya completado su transmisión. De esta forma se evita una costosa colisión.

Pero sigue existiendo el problema de que estas estaciones esten ocultas entre si y elijan un backoff muy proximo

Enfrentados al problema de terminales ocultas: RTS y CTS

El protocolo MAC trae un esquema de reserva, que ayuda a evitar las colisiones incluso en presencia de terminales ocultos.



El protocolo permite a una estacion utilizar una trama corta de **control** de **solicitud** de **transmision** (**RTS**) y otra trama corta de control **preparado para enviar** (CTS) para reservar el acceso al canal. Pide **exclusividad**

Cuando un emisor quiere mandar data en una trama, primero debe enviar una trama RTS al punto de acceso indicando el **tiempo total requerido** para transmitir la DATA y recibir el ACK. Cuando el punto de acceso recibe la trama RTS, difunde una trama **CTS** (que será escuchada por todas las estaciones dentro de su cobertura) que **le da al emisor un permiso explícito** para enviar y además informa a otras estaciones que no deben transmitir por ese periodo de tiempo.

El uso de RTS y CTS puede mejorar el rendimiento de dos formas:

- el problema de las estaciones ocultas queda mitigado ya que una trama de data solo enviará cuando haya reservado el canal.
- Si hay una colision entre tramas RTS o CTS solo durará mientras duren estas tramas cortas.

Esta tecnica solo se utiliza para tramas de datos larga xq **agrega retardo** y consume recursos del canal.

Utilizacion de WiFi como enlace punto a punto

Si hay dos nodos, cada uno de los cuales dispone de una antena direccional, ambos pueden apuntar sus atentas hacia el otro nodo y ejecutar el protocolo sobre lo que es un enlace punto a punto.

7.3.3 La trama IEEE WiFi (802.11)

Trama (los números indican la longitud del campo en bytes):

2	2	6	6	6	2	6	0-2312	4
Control de trama	Duración	Dirección 1	Dirección 2	Dirección 3	Control secuencia	Dirección 4	Carga útil	CRC

Campo de control de trama expandido (los números indican la longitud de los subcampos en bits):

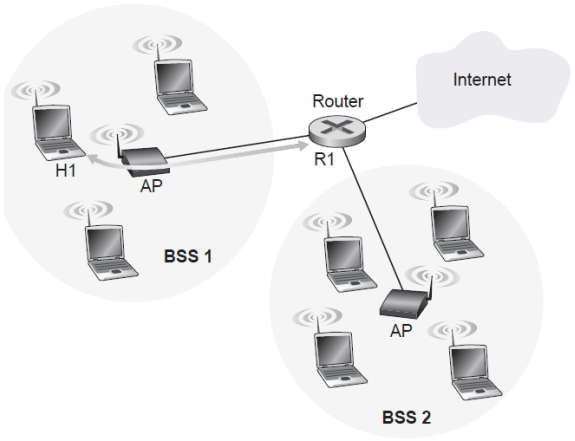
2	2	4	1	1	1	1	1	1	1	1
Versión protocolo	Tipo	Subtipo	Hacia AP	Desde AP	Más frag.	Reintentar	Gest. potencia	Más datos	WEP	Rsvd

Figura 7.13 ♦ La trama 802.11.

- **Campos de carga util y CRC**: compuesto por un datagrama IP o un paquete ARP. CRC
- **Campos de direccion**: Tiene 4 campos de direcciones, cada uno puede contener una direccion MAC. 3 de esos campos se utilizan para **mover el datagrama**

de la capa de red de una espacio inalámbrico hasta una interfaz de un router a traves de un punto de acceso. El **cuarto** se utiliza cuando los puntos de acceso se reenvian tramas entre sí en **modo ad hoc**.

- Direccion 2: direccion MAC de estacion origen
- Direccion1: direccion MAC de estacion destino
- Direccion 3: direccion MAC de la interfaz del router de la subred de la que forma parte el BSS. Se utiliza para la comunicacion entre bss y una red cableada.
  Ejemplo:
  Se quiere transferir una trama desde el router hasta la estacion inalámbrica h1.



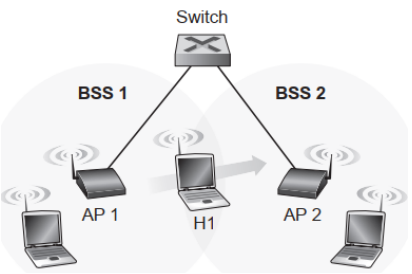
El router conoce la direccion IP de H1(direccion destino en el datagrama) y utiliza ARP para saber su direccion MAC. R1 encapsula en una trama con su direc origen mac del r1 y direc destino mac h1.
Cuando **la trama Ethernet** llega al punto de acceso, este la convierte en **trama WiFi** antes de transmitirla por el canal inalámbrico. El punto de acceso completa los campos de direccion 1 y 2 con las direcciones mac de h1 y del punto de acceso (su propia dir) y en la direccion **3 va la direccion mac del router** y asi **H1 sabe la direccion MAC de la interfaz del router que envía el datagrama**.

Ademas El campo Dirección 3 permite al punto de acceso determinar la dirección MAC de destino apropiada a la hora de construir la trama Ethernet.

- Campos número de secuencia, duracion y control del tema
  - Campo seq: permite al receptor distinguir entre una trama recien transmitrida y la retransmisión de una duracion: permite reservar el tiempo para transmitir la trama de datos y la trama de reconocimiento
  - Tipo y subtipo: sirven para distinguir las tramas: datos, RTS, CTS, ACK.
  - hacia y desde: sirven para definir los significados de los diferentes campos de direccion (si es modo ad hoc o modo infraestructura, y en este último caso dependiendo de si quien está enviando la trama es una estación inalámbrica o un punto de acceso)
  - el campo WEP indica si se está empleando cifrado o no

7.3.4 Movilidad dentro de la misma subred IP

¿cómo pueden moverse las estaciones inalámbricas de forma transparente de un BSS a otro, mientras mantienen una serie de sesiones TCP activas? Puede gestionarse de manera sencilla cuando los BSS forman parte de la misma subred. Cuando las estaciones se desplazan entre subredes contiguas, hacen falta protocolos más complejos de gestión de la movilidad.



Como todas las estaciones de los dos BSS, incluyendo los puntos de acceso pertenecen a la misma subred IP. Cuando un dispositivo se mueve de bss1 a un bss2 puede conservar su direccion IP y todas sus conexiones TCP activas.

¿Qué es lo que sucede?

A medida que el dispositivo se aleja del punto de acceso 1, el dispositivo detecta que la señal se empieza a debilitar y empieza a explorar otros puntos de acceso con una intensidad mayor. El dispositivo recibe tramas de baliza del punto de acceso 2. Entonces el dispositivo se deasocia de AP1 y se asociado a AP2 (**que tendrán el mismo identificador SSID que AP1)** al mismo tiempo que manteiene su direccion IP y sus sesiones TCP activas.

Desde el punto de vista del switch, estos disponen de la caracteristica de **autoaprendizaje que les permite** construir su tablas de reenvío automaticamente y así puede gestionar los desplazamientos de forma eficiente.

Un datagrama destinado a H1 tendrá que ser dirigido hacia H1 a través del punto de acceso AP1. Sin embargo, una vez que H1 se asocia con BSS2 sus tramas deben ser dirigidas hacia AP2. Una solución es que AP2 envíe al switch una trama Ethernet de difusión con la dirección de origen de H1 justo después de la nueva asociación.

7.3.5 Caracteristicas avanzadas de WiFi

- **Adaptacion de la velocidad**: algunas implementaciones tienen una capacidad de adaptación de la velocidad que permite seleccionar adaptativamente la técnica subyacente de modulación de la capa física que hay que utilizar, basándose en las características pasadas o recientes del canal.

- **Gestion de potencia**: Un nodo indica al punto de acceso que se va a ir a dormir. Se configura un temporizador en el nodo para despertarle justo antes del momento en el que el punto de acceso tiene programado enviar su trama baliza. Puesto que el punto de acceso sabe que el nodo se va a dormir, el punto de acceso sabrá que no debe enviar ninguna trama a dicho nodo y almacenará en un buffer todas las tramas destinadas a ese host dormido. Permite a los nodos WiFi minimizar la cantidad de tiempo que sus funciones de detección, transmisión y recepción.

7.3.6 Redes de área personal: Bluetooth y Zigbee

BLUETOOTH

Opera con un corto alcance, a baja potencia y con bajo coste. Son **redes ad hoc**: no hace falta ninguna infraestructura para interconectar los dispositivos. Por tanto, estos dispositivos deben organizarse por sí mismos. Se trata de una tecnología de “sustitución de cable” que permite la interconexión de una computadora con periféricos inalámbricos.
Estos dispositivos no pueden comunicarse hasta que su estado sea cambiado por el nodo maestro de aparcado a activo.

ZIGBEE

Está pensada para aplicaciones de menor consumo de potencia, menor velocidad de bits y menor ciclo de trabajo que bluetooth.

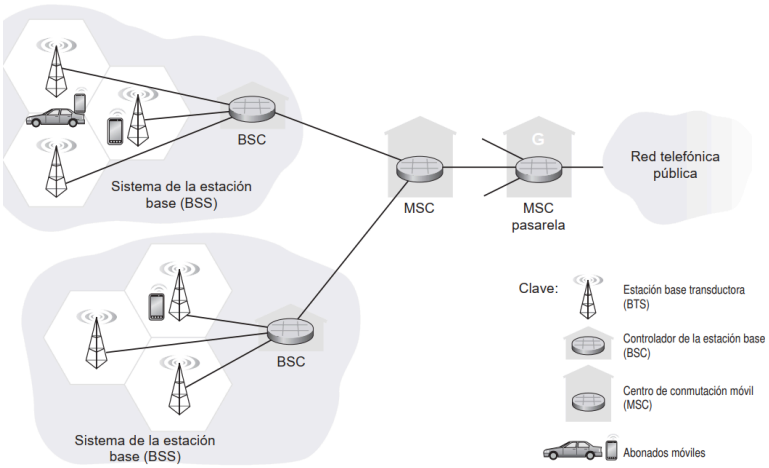
7.4 Acceso celular a Internet

7.4.1 Panorámica de la arquitectura de las redes celulares

Sistema global de comunicaciones móviles (GSM)
1G - tráfico de voz, analogico
2G - tráfico de voz, digitales
3G - tráfico de voz y datos (enfasis en los datos y los enlace de acceso)
4G - LTE. red principal completamente IP y proporciona servicio de datos y voz integrados a velocidades de varios MEGABITS

2G: conexiones de voz con la red telefonica

La región cubierta por una red de celular está divida en una serie de areas geograficas de coverturas llamadas celdas. Cada celda contiene una **estacion transductora base** (BTS, Base Transceiver Station) que transmite y recibe señales hacia y desde las estaciones móviles que se encuentran dentro de su celda.



El area de cobertura depende de factores como:

- potencia de transmision de la BTS
- potencia de transmisión de los depositos de usuarios
- Los edificios situados dentro de la celda que puedan obstruir las comunicaciones
- La altura de las antenas de la estacion base

Muchos sistemas actuales colocan las BTS en las esquinas donde intersectan tres celdas, de modo que una única BTS con antenas direccionales pueda dar servicio a las tres.

El estándar GSM para los sistemas celulares 2G utilizan una combinacion FDM/TDM (radio) para la interfaz area.

El controlador de la estacion base (BSC) da servicio a varias decenas de estaciones transductura base. Su funcion consiste en asignar los canales de radio de las BTS a los abonados móviles, determinar la celda en la que se encuentra un usuario movil (pagging) y llevar a cabo la transferencia(handoff) de los usuarios móviles.
BSC CONTROLA A LOS BTS
Controlador + Σestaciones transductoras = subsistema de estaciones base (BSS, Base Station Subsystem)

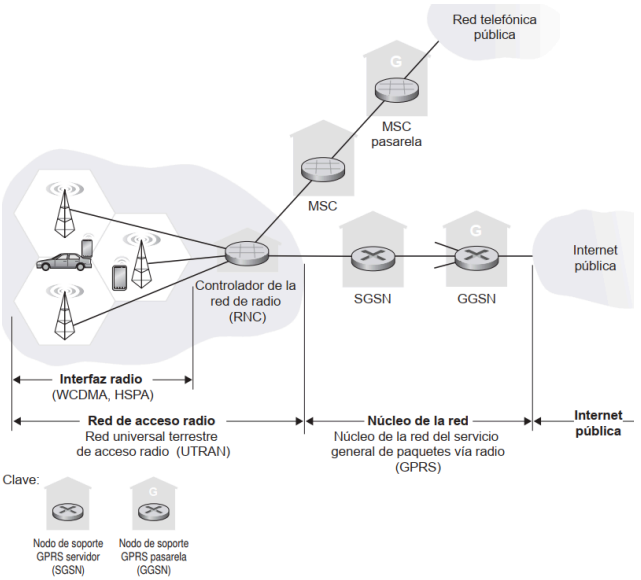
7.4.2 3G: llevando Internet a los abonados celulares

Nuestro teléfono inteligente necesitará ejecutar una pila de protocolos TCP/IP completa (que incluya las capas física, de enlace, de red, de transporte y de aplicación) y conectarse a Internet a través de la red de datos celular

Nucleo de la red 3G

conecta las redes de acceso de radio a la internet pública. Interopea con componentes de la red celular de voz existente.

La solución fue integrar los nuevos servicios de datos directamente en el nucleo de la red celular de voz existente.
hay dos tipos de nodos en el nucleo:



- **Nodos de soporte GPRS servidor** (**SGNS**): Es **responsables de entregar los datagrama**s que viajan hacia/desde los nodos móviles de la red de acceso vía radio a la que el SGSN está conectado. Interactua con el MSC de la red correspondiente a dicha area encargada de la autorizacion del usuario y la sesion de llamada, de mantener la informacionde ubicacion y de realizar en reenvio de los datagramas.
- **Nodos de soporte GPRS pasarela** (**GGNS**): Actua como pasarela conectando multiples SGSN con internet. Es el último elemento con el que se encuentra un datagrama antes de entrar a internet. Oculta al mundo exterior la movilidad de los nodos 3G existentes dentro de su red. GETAWAY hace la conexion de red con telefono

Red de acceso radio 3G: La frontera inalámbrica:

La red de acceso radio 3G es la red inalámbrica de primer salto que vemos como usuarios 3G. El controlador de red radio (RNC) suele controlar varias estaciones base celulares transceptoras.
El RNC conecta tanto a la red celular de voz de conmutacion de circuitos, como a la red internet de conmutacion de paquetes. Emplea una tecnica de CDMA de banda ancha de secuencias directas.

7.4.3 Hacia la tecnología 4G: LTE

Dos innovaciones importantes:

- Nucleo de la red completamente IP
- Una red mejorada de acceso vía radio

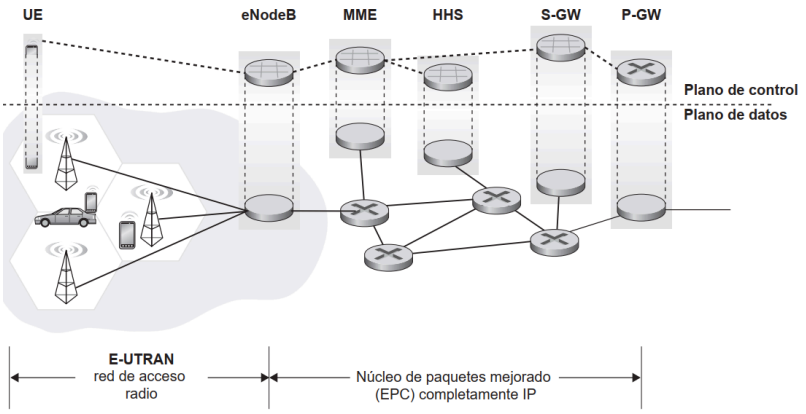


Figura 7.20 ♦ Arquitectura de red 4G.

Nucleo de la red IP

- **arquitectura de red unificada, complemante IP**: tanto la voz como los datos son transportados en datagramas IP hacía/desde el dispositivo inalámbrico(UE) hasta la pasarela de paquetes (P-GW) que conecta la red de fronterga 4G con el resto de la red
- **Separacion del plano de datos y el control 4G**
- **Separacion entre la red de acceso vía radio y el nucleo de la red completamente IP**: los datagramas son enviados a través de una red IP internat a 4G hasta la red internet externa

Componentes principales

- **eNodeB**: su mision consiste en r**eenviar los datagramas entre el UE y el P-GW**

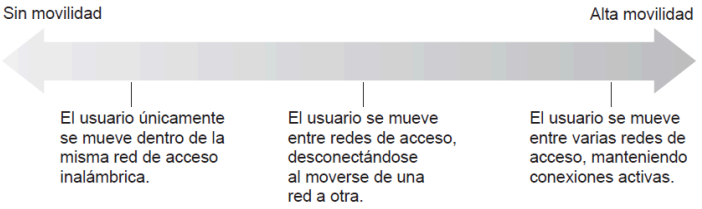
Los datagramas del UE se encapsulan en el nodo eNodeB y se tunelizan hacia el P-GW a traves del nucleo de paquetes mejorado completamente IP. Estos túneles pueden tener asociadas distintas ganarantias de calidad de servicios

- **Pasarela de la red de datos empaquetados** (P-GW) asigna **direcciones ip** a los equipos UE y se encarga de imponer las garantias QoS. Tambien lleva a cabo la encapsulacion/desencapsulacion de los datagramas al reenviarlos hacia/desde el UE
- **Pasarela de servicio** (S-GW): Es el punto de anclaje de movilidad del plano de datos: todo tráfico de UE pasará a traves de S-GW.
- **Entidad de gestion de la movilidad** (MME) se encarga de la **gestion de conexion** y de movilidad por cuenta de los UE residentes en la celda que controla.
- **Servidor de abonado doméstico** (HSS): Contiene **informacion** del UE.

7.5 Gestion de la movilidad Principios:

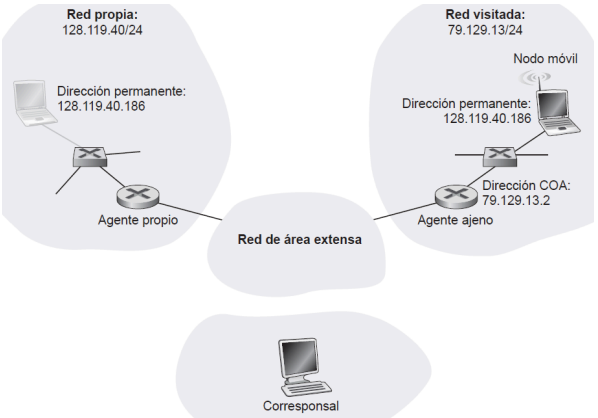
Un nodo movil es aquel que cambia su punto de conexion con la red a lo largo del tiempo.

Movilidad desde el punto de vista de la capa de red:
Hasta qué punto es importante que la direccion del nodo movil sea siempre la misma:



Depende de la situación: si se quiere mantener una conexion tcp en un auto en movimiento o si un usuario apaga su compu portatil de la oficina y la vuelve a prender en su casa.
En el segundo caso no tiene tanta importancia porque el usuario podría perfectamente funcionar con una dirección que el ISP que da servicio a su domicilio le asignara temporalmente a la computadora portátil.

Recordar que una aplicacion de internet necesita conocer la direccion IP y número de puerto de la entidad remota con la que se está comunicando. Si una entidad movil es capaz de mantener su direccion IP a medida que se desplaza, la movilidad se convertirá en algo transparente desde el punto de vista de la aplicacion. Esta transparencia es algo importante xq la aplicacion no debera preocuparse de si las direcciones IP cambian o no para un mismo dispositivo.



Elementos iniciales de una arquitectura de red móvil

- El domicilio permanente de un nodo movil se llama **red propia**
- **Agente propio** es la entidad dentro de la red propia que se encarga de llevar a cabo funcionalidades de gestion de la movilidad. (mi router)
- La red en la que reside actualmente el nodo movil se conoce como **red ajena o visitada.**
- **Agente ajeno**: entidad dentro de la red ajena que ayuda al nodo movil con las funciones de gestion de movilidad. (router del vecino)
- Un **corresponsal** es la entidad que se quiere comunicar con el nodo movil

7.5.1 Direccionamiento

Para que la movilidad de los usuarios sea transparente a los ojos de la aplicaciones de red es deseable que mantenat su direccion Ip mientras se mueven de una red a otra. Po rlo que cuando un nodo reside en una red ajena, todo el tráfico dirigido a la direccion permanente del nodo ahora tendrá que ser enrutado hacia la direccion ajena. ¿Cómo se puede hacer eso?

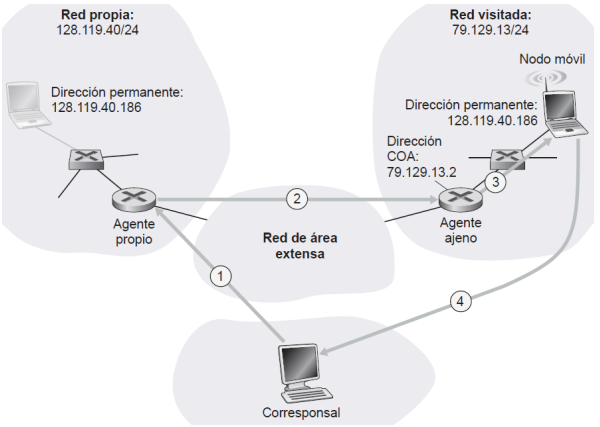
- Una opcion es que se encarguen los routers. La red ajena anuncia a otras redes que el nodo movil está en su red pero no es escalable. Si la gestion de movilidad tendria que estar en manos de los routers, estos tendrian que mantener entradas en sus tablas de ruteo para millones de nodos móviles y actualizar dichas entradas cuando se muevan.
- Otro enfoque es trasladar la funcionalidad de movilidad desde el nucleo de la red hasta la frontera de la misma. Esto se puede hacer mediante la red propia del nodo movil. El agente propio situado en la red propia del nodo movil puede controlar en qué red ajena reside el nodo movil.

Un papel del agente ajeno consiste en crear la denominada **direccion cedida**(**COA**, **Care-of Address**) para el nodo movil. Habra dos direcciones asociadas a un nodo movil: su direccion permanente y su direccion cedida COA (o Dirección ajena).

La COA **se utiliza para "re-enrutar" datagramas** hacia el nodo móvil a través de su agente ajeno.

También el nodo móvil podría obtener una COA en la red ajena (por ejemplo, utilizando un protocolo como DHCP) e informar él mismo al agente propio de cuál es su COA.

7.5.2 Enrutamiento hacia un nodo móvil



Hay dos tipos: enrutamiento indirecto y directo.

Enrutamiento indirecto

El corresponsal direcciona el datagrama con la **dirección permanente del nodo movil** y lo envía a la red (ignorando si el nodo está en su red propia o en una ajena por lo que la movilidad es completamente transparente para el corresponsal).

El agente propio ademas de ser el responsable de interactuar con el agente ajeno para saber en todo momento el COA del nodo movil, También debe estar atento para ver si llegan datagramas dirigidos a nodos cuya red propia sea la de ese agente propio pero que actualmente están residiendo en una red ajena. El agente propio intercepta estos datagramas y luego los reenvia hacia un nodo movil siguiendo un proceso de dos pasos:

- El agente propio encapsula el datagrama completo en un nuevo datagrama más grande y es reenviado hacia el agente ajeno usando la direccion COA del nodo movil.
- El agente ajeno recibe el datagrama grande, lo desencapsula y reenvia el datagrama original al nodo movil.

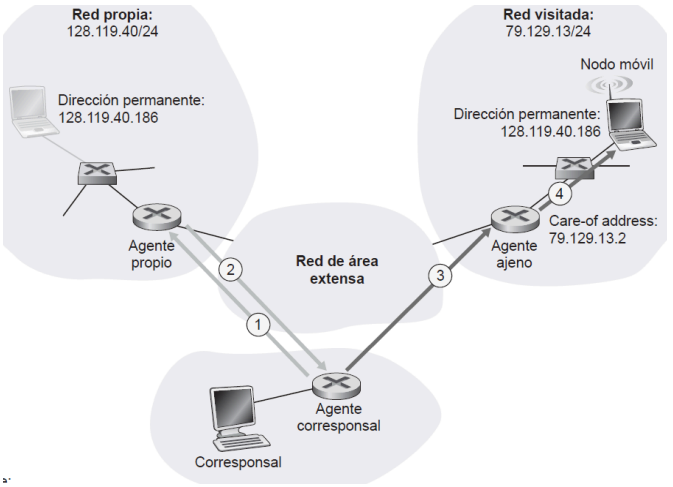
Resumiendo tenemos:

- **Un protocolo entre el nodo móvil y el agente ajeno**. El nodo móvil se registrará ante el agente ajeno cuando se conecte a la red ajena. De forma similar, el nodo móvil se desregistrará ante el agente ajeno cuando abandone la red ajena.

- **<u>Un protocolo de registro entre el agente ajeno y el agente propio</u>**. El agente ajeno **registrará la COA** del nodo móvil ante el agente propio. **El agente ajeno no necesita desregistrar explícitamente una COA cuando un nodo móvil abandona su red,** porque el subsiguiente registro de una nueva COA, cuando el nodo móvil se desplace a otra red, se encargará de ello.
- **<u>Un protocolo de encapsulación de datagramas para el agente propio</u>**. Este protocolo se encargará de la **encapsulación y del reenvío del datagrama** original del corresponsal dentro de un datagrama dirigido a la COA.
- **<u>Un protocolo de desencapsulación para el agente ajeno</u>**. Este protocolo se encargará de la extracción del datagrama original del corresponsal a partir del datagrama encapsulante y del reenvío del datagrama original al nodo móvil.

Problema del enrutamiento triangular:
Los datagramas dirigidos al nodo movil debe enrutar en primer lugar hacia el agente propio y luego hacia la red ajena, **aun cuando exista una ruta más eficiente entre el corresponsal y el nodo movil**.

Enrutamiento directo



Elimina la ineficiencia del enrutamiento triangular, pero a costa de un proceso mas complejo.

Un **agente corresponsal situado en la red de corresponsal determina el COA del nodo movil consultando al propio agente.** Entonces el agente corresponsal tuneliza directamente los datagramas hacia la COA del nodo movil.

2 problemas adicionales:

- falta un **protocolo de localización de usuarios** móviles para que el agente corresponsal consulte al agente propio con el fin de obtener la COA del nodo móvil
- **Cuando el nodo móvil se desplaza de una red ajena a otra. el agente corresponsal solo consulta la COA una vez al agente propio**, al inicio de la sesión. Por tanto, la actualización de la COA en el agente propio, aunque sigue siendo necesaria, no será suficiente para resolver el problema de cómo enrutar los datos hacia la nueva red ajena del nodo móvil.

Una solucion seria crear un nuevo protocolo para notificar al corresponsal el cambio de la COA. Otra alternativa adoptada en la redes GSM es la siguiente:

El agente ajeno de dicha red ajena en la que el nodo móvil se encontraba inicialmente con el nombre de **agente ajeno ancla**. Cuando el nodo móvil se desplaza a una nueva red ajena (paso 2) se registra ante el nuevo agente ajeno (paso 3) y el nuevo agente ajeno **proporciona al agente ajeno anclado la nueva COA del nodo móvil** (paso 4). Cuando el agente ajeno ancla recibe un datagrama encapsulado para un nodo móvil que ya ha salido de su red, puede entonces reencapsular el datagrama y reenviarlo al nodo móvil (paso 5) utilizando la nueva COA.

7.6 IP MOVIL

IP móvil es un estándar flexible, que soporta muchos modos distintos de operación (por ejemplo, operación con o sin un agente ajeno), múltiples formas de que los agentes y los nodos móviles se descubran entre sí, utilización de direcciones COA únicas o múltiples y diversas formas de encapsulación

El estandar IP movil consta de 3 elementos principales:

- **Descubrimiento de agentes**. IP móvil define los protocolos utilizados por un agente propio o ajeno para anunciar sus servicios a los nodos móviles, así como protocolos para que los nodos móviles soliciten los servicios de un agente ajeno o propio.
- **Registro ante el agente propio**. IP móvil define los protocolos utilizados por el nodo móvil y/o el agente ajeno para registrar y desregistrar direcciones COA ante el agente propio de un nodo móvil.
- **Enrutamiento indirecto de los datagramas**. El estándar también define la forma en que el agentepropio reenvía los datagramas hacia los nodos móviles, incluyendo reglas para el reenvío de datagramas, reglas para la gestión de las condiciones de error y diversas formas de encapsulación

Descubrimiento de agentes

Cuando un nodo de IP movil llega a una nueva red debe averiguar la identidad del agente ajeno o propio correspondiente. Este proceso de descubrimiento de agentes puede realizarse mediante anuncios de los agentes o mediante las solicitudes de agente.

- Con el **anuncio de agente** cada agente ajeno o propio anuncia sus servicios. Este agente difunde periódicamente un **mensaje ICMP** a traves de todos los enlaces en el que está conectado que **contiene la direccion IP del agente**.

- Con la **solicitud de agente**, un nodo móvil puede difundir un mensaje de solicitud de agente por medio de un **mensaje ICMP**. Un agente que reciba la solicitud enviará directamente al nodo móvil un anuncio de agente, mediante un **mensaje de unicast**, pudiendo entonces el nodo móvil proceder como si hubiera recibido un anuncio no solicitado.

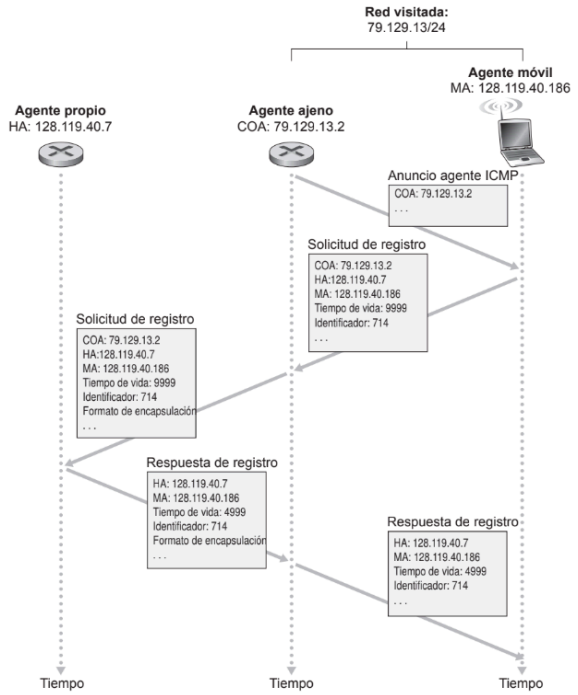


Figura 7.29 ♦ Anuncio de agente y registro de IP móvil.

Registro ante el agente propio

Una vez que un nodo IP ha recibido una direccion COA, **debe registrar dicha direccion** ante su **agente propio**. Esto lo puede hacer por medio del agente ajeno o lo puede hacer directamente el propio nodo de IP movil.

Por medio del agente ajeno:

1. Despues de recibir el anuncio de un agente ajeno, el **nodo movil envía** un mensaje de registro de IP movil a ese agente ajeno. Este mensaje se transporta en un datagrama UDP

que contiene la dirreccion COA, la direccion del agente propio (HA), la direccion permanente del nodo movil y el tiempo de vida para el registro
2. El agente ajeno recibe el mensaje de registro y anota la dirección IP permanente del nodo móvil.El agente ajeno envía a continuación un mensaje de registro de IP móvil (de nuevo dentro de un datagrama UDP) al agente propio con las direcciones COA, HA y MA.
3. El agente propio recibe la solicitud de registro y comprueba la autenticidad y la corrección de la misma. El agente propio establece una asociación entre la dirección IP permanente del nodo móvil y la dirección COA.
4. El agente propio envía una respuesta de registro de IP móvil que contiene las direcciones HA y MA, el tiempo de vida real del registro y el identificador de registro correspondiente a la solicitud que se esté satisfaciendo con esta respuesta.
5. El agente ajeno recibe la respuesta de registro y a continuación la reenvía hacia el nodo móvil.

Una vez realizado esto, el nodo movil ya puede empezar a recibir datagramas enviados a su direccion permanente.

7.7 Gestion de la movilidad en redes celulares

Arquitectura de las redes celulares GSM.

GSM adopta una tecnica basada en el enrutamiento indirecto, enrutando primero la llamada del corresponsal hacia la red propia del usuario movil y de alli a la red visitada.

La **red propia** es el proveedor de telefonia celular con el que está abonado el usuario movil.
Denominamos **red visitada** a la red en la que reside actualmente el usuario movil.

Ambas poseen responsabilidades distintas:

- La red propia mantiene una base de datos que se conoce con el nombre de **registro de ubicaciones propias (HLR),** que contiene el **número de teléfo**no celular permanente y la **información del perfil** de abonado para cada uno de sus abonados. También contiene informacion sobre **la ubicacion** de los abonados.
  Un **conmutador** especial dentro de la red propia, conocido como **centro de conmutación pasarela para servicios móviles** (GMSC) es contactado por el corresponsal cada vez que realiza una llamada a un usuario móvil.
- La red visitada mantiene una base de datos conocida con el nombre de **registro de ubicación de visitantes (VLR**). La base de datos VLR contiene una entrada para cada usuario móvil que se encuentra actualmente en la parte de la red a la que da servicio VLR. A medida que los usuarios móviles entran y salen de la red las entradas de VLR aparecen y desaparecen.

7.7.1 Enrutamiento de llamadas hacia un usuario movil

Veamos cómo se realiza una llamada a un usuario móvil GSM que se encuentra en una red ajena

1. El corresponsal marca el número telefónico del usuario móvil. Los primeros dígitos del número son suficientes para identificar globalmente la red propia a la que el móvil pertenece. La llamada será enrutada desde el corresponsal, a través de la red telefónica conmutada pública hasta el conmutador propio de la red propia del móvil

2. El MCS recibe la llamada y consulta a su base de datos para determinar la ubicación del usuario móvil. Puede devolver el número de itinerancia (distintos del numero permanente): es efimero (es asignado temporalmente al movil cuando entra dentro de una red visitada)
   Si la bdd no tiene el numero devuelve la direccion de la bdd de la red visitada y en ese caso el conmutador debera consultar a esa VLR(bdd red visitada) para obtener el número de itinerancia del nodo movil.
3. Conocido el número de itinerancia, el conmutador propio establece el segundo tramo de la llamada a través de la red hasta el conmutador de la red visitada. Con ello, la llamada se habrá completado.

7.8 Tecnología inalámbrica y movilidad: impacto sobre los protocolos de las capas superiores

Dadas las tasas de errores de bit en los enlaces inalámbricos y la posibilidad de que se produzcan pérdidas en la transferencia de llamadas, la respuesta del control de congestión de TCP podría ser problemática en una configuración inalámbrica.
Porque tcp lo que hace cuando hay errores es bajar la receive window pero esto soluciona la congestion, no errores de bit, que en las redes inalambricas predominan los errores de bits.

Para resolver este problema se pueden usar tres clases genéricas de técnicas:

Recuperación local: permiten recuperarse de los errores de bit en el lugar y en el momento en que esos errores se producen.

Conocimiento por parte del emisor TCP de enlaces inalámbricos: el emisor y el receptor TCP sean conscientes de la existencia de un enlace inalámbrico, para distinguir entre las pérdidas por congestión que tienen lugar en la red cableada y las pérdidas/corrupciones que se producen en el enlace inalámbrico, y para invocar los mecanismos de control de congestión solo en respuesta a las pérdidas debidas a que la red cableada está congestionada

Técnicas de conexión dividida: La conexión extremo a extremo se forma mediante la concatenación de una parte inalámbrica (host movil - Punto de Acceso inalambrico) y una parte cableada (AP inalámbrico - el otro extremo: host cabledo). La capa de transporte a través del segmento inalámbrico puede ser una conexión TCP estándar o un protocolo de recuperación de errores especialmente adaptado ejecutándose sobre UDP.