Capítulo 7
QoS y Seguridad en IMS

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

QoS en IMS

- Los equipos terminales pueden usar directamente
  - Protocolos de reservación de recursos a nivel de la capa de enlace, ejemplo: PDP Context Activation
  - RSVP
  - DiffSev
- La red puede usar
  - DiffSer
  - RSVP
- Cuando el terminal es un móvil celular lo más típico es que use protocolos a nivel de la capa de enlace, como PDP, y que la IPCAN transforme los flujos con reservación de recursos de la capa de enlace a códigos DiffServ
- La solicitud de recursos puede hacerse a través de la creación de un PDP Context o enviando un mensaje RSVP PATH.

PDP Context es una estructura de datos que contiene la información de sesión del usuario cuando el mismo tiene una sesión activa. Cuando un UE quiere registrarse a una red de datos, primero debe anexarse a la misma y luego crear un PDP Context. El PDP puede ser, IP, ATM,etc. Para el caso de IMS debe ser IP.

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

IMS: QoS Dinámica

En una red que tiene diferentes niveles de QoS en función del servicio, el UE debe solicitar el nivel de QoS necesario, y si los recursos están disponibles se les garantizarán.

La solicitud de la QoS es dinámica en el sentido que puede hacerse en distintos instantes de tiempo:

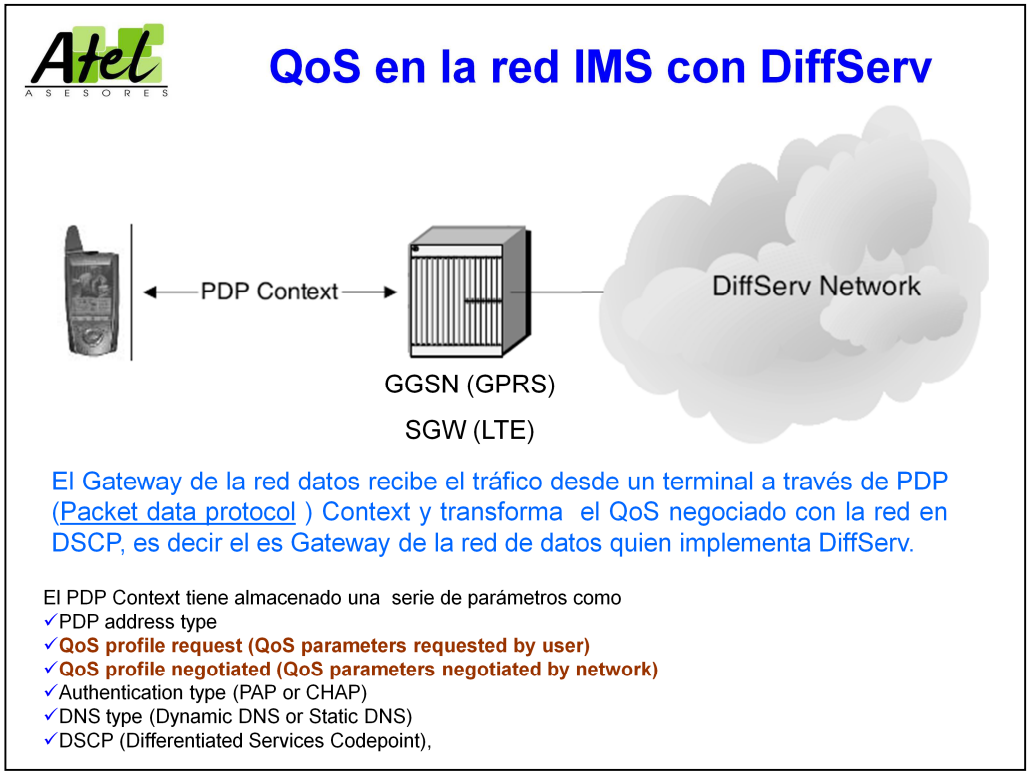
- Con Antelación: se establece un acuerdo previo sobre la clase de servicio del usuario
- Dinámicamente al establecer la llamada: la negociación para una sesión particular se realiza en forma dinámica justo al momento de establecer la sesión la misma es evaluada en forma individual para determinar los requisitos de QoS y los recursos disponibles
- En medio de una llamada, como respuesta a un evento: en servicios multimedia, durante una llamada pueden ocurrir eventos que requieran un cambio en el tipo de media (por ejemplo, agregar video en lugar de voz), agregar un flujo de datos (ej. la entrada de otro usuario a la sesión) o la liberación de un flujo, etc. Estos eventos producen una reevaluación de los requisitos de QoS

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

Instrucciones para Reservar Recursos

- Los terminales deben tener la capacidad de transformar los media streams de una sesión de comunicación en flujos de reservación
- Por ejemplo, un terminal que desee transmitir audio y video puede
  - Hacer una sola reservación de recursos para ambos flujos
  - O reservar recurso por separado para cada flujo: uno para audio y otro para video

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739



En este caso se muestra una red de datos que tiene implementado el mecanismo DiffServ para manejar la QoS. Vemos que a pesar de que entre el móvil y la red el perfil de QoS está basado en PDP Context, estos son transformados a DiffServ. En IMS el core de la red maneja DiffServ o RSVP.

Incluso si el móvil usa RSVP el Gateway puede usar dicha información para asignarle un DSCP correspondiente.

Packet data protocol (PDP): Se refiere a cualquier protocolo basado en paquetes, tal como IP.

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

QoS en Internet

Internet siempre ha sido tradicionalmente una red best-effort, sin embargo, para garantizar el despliegue de ciertas aplicaciones es indispensable garantizar un determinado nivel de QoS.

Por ejemplo, mientras que un usuario que esté bajando un archivo puede tolerar grandes retardos debido a congestionamiento en la red, un usuario que desea establecer una comunicación vocal no se siente a gusto si tiene que esperar mucho tiempo para que se establezca la comunicación; mas aún, una vez establecida la comunicación los retardos en la llegada de los paquetes degradan la calidad de la voz recibida.

Muchas veces pensamos que la QoS es cuestión de que el usuario pague una tarifa más alta, podría ser el caso, pero también podría suceder que la red sencillamente no puede garantizar cierta QoS.

Existen dos modelos para brindar QoS en Internet:

- Integrated Services (RFC 1633)
- Differentiated Services (DiffServ RFC 2472 y RFC 3260)

Internet fue originalmente concebida para aplicaciones best-effort donde no se requiere una QoS que le exigiera mucho a la red. Por esta razón las aplicaciones en tiempo real no se adaptan bien en Internet y su desempeño es muy bajo.

Con el fin de soportar aplicaciones multimedia en tiempo real que incluyan voz, video, juegos interactivos, etc., es necesario incluir algunos cambios en la red que permitan soportar aplicaciones en tiempo real con QoS.

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

Integrated Services
IS (RFC 1633)

- IS suministra QoS de extremo-a-extremo
- Los extremos solicitan un cierto nivel de QoS y si es aceptado por la red, los routers tratarán esos paquetes de acuerdo con lo establecido
- Existen 2 tipos de servicio en IS
  - Controlled load service: los paquetes son tratados como si la carga en la red fuese moderada, el servicio no se ve afectado por congestión, pero no se puede garantizar ni un ancho de banda ni un dealy específico, este servicio se conoce como better-than-best-effort.
  - Guaranteed service: garantiza un cierto ancho de banda o delay dentro de limites determinados. En la práctica este servicio no se usa mucho, ya que el Controlled Load Service es más adecuado y fácil de gestionar.
- IS usa RSVP (RFC 2205) como protocolo para reservar servicios

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

RSVP: Resource ReSerVation Protocol RFC 2205

- RSVP es un protocolo de la capa de transporte diseñado para reservar recursos a través de una red para flujos de datos Unicast o Multicast, se implementa en los host y en los routers a lo largo de una ruta de manera que el ancho de banda solicitado esté disponible cuando se envíen los paquetes
- RSVP es un protocolo SIMPLEX, para garantizar FULL DUPLEX se deben hacer reservaciones en ambas direcciones
- RSVP es usado por un host para solicitar a una red una QoS especifica para una aplicación particular. Ha sido diseñado para protocolos de enrutamiento unicast y multicast
- RSVP también se usa en los routers para entregar QoS a los nodos a través de una ruta de un flujo IP perteneciente a una aplicación con la cual se ha acordado una QoS
- La función de RSVP es reservar los recursos necesarios a lo largo de toda una ruta entre los extremos en una sola dirección. Es decir RSVP deferencia, desde el punto de vista lógico, al transmisor del receptor, a pesar de que la aplicación sea en ambas direcciones.
- RSVP se ubica en el tope de IPv4 o IPv6, ubicándose en el lugar de la capa de transporte, pero no transporta datos de las aplicaciones y se ejecuta en el plano de control, no en el de datos de usuarios.

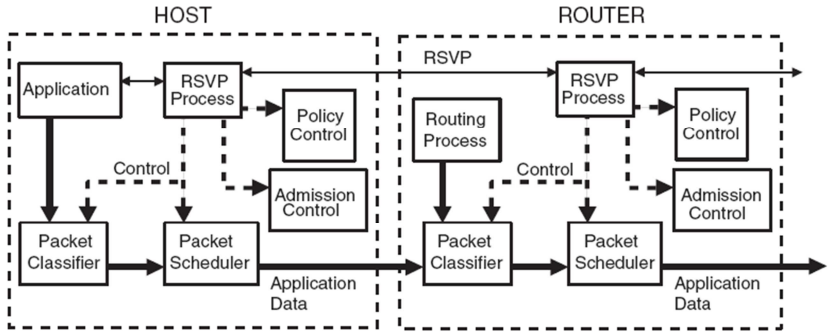
RSVP ofrece un buen mecanismo para garantiza QoS y es lo más cercano al concepto de circuitos, pero justamente debido a eso tiene un costo significante. RSVP exige que los router examinen en detalles el encabezado IP y que mantengan almacenado el estado de todas las reservaciones existentes. Si usáramos RSVP para cada sesión, por ejemplo de VoIP, podríamos tener millones de reservaciones simultáneas. Así, RSVP presenta problemas de escalamiento para sistemas muy grandes.

A parte del RFC 2205, existen otros estándares relacionados con RSVP

- RFC 2206, RSVP Management Information Base using SMIv2 (RFC 2206)
- RFC 2207, RSVP Extensions for IPSEC Data Flows
- RFC 2208, RSVP Version 1 Applicability Statement Some Guidelines on Deployment
- RFC 2209, RSVP Version 1 Message Processing Rules

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

RSVP en Hosts y Routers



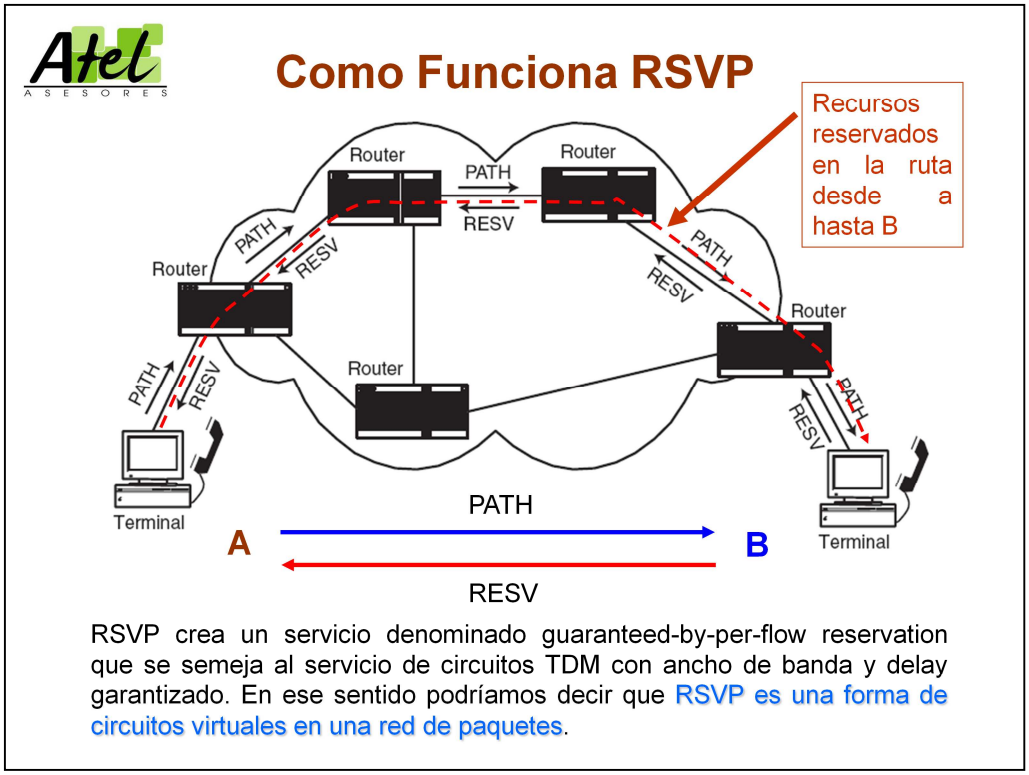
1. Admission Control: Determina si el nodo tiene suficientes recursos
2. Policy Control: Verifica si el usuario tiene privilegios para reservar recursos
3. Si se pasa 1 y 2, se notifica al Packet Clasiffier para que asigne la clase de QoS

RSVP se ejecuta en el plano de control no en el de usuarios, por lo tanto no lleva datos de las aplicaciones.

RSVP implementa la QoS a través de mecanismos llamados “Control de Tráfico” e incluyen un packet classifier, un admission control y un "packet scheduler“. Dichos mecanismos se implementan tanto los hosts como en los routers.

Durante el establecimiento de la reservación, se envía una solicitud de RSVP QoS a los módulos Admission Control y Policy Control. Admission Control determina si el nodo tiene suficientes recursos disponibles para satisfacer la QoS solicitada. Admission Policy verifica si el usuario tiene permiso para hacer reservación de recursos. Si ambos chequeos están bien se notifica al Packet Classifier, si alguno falla se genera un error.

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739



El terminal A desea comunicarse con el terminal B, A envía un mensaje PATH al terminal B el cual viaja a través de una cierta ruta determinada por los routers. El mensaje PATH lleva información relativa al tráfico denominada “Traffic Specification” (TSpec) que incluye detalles de los datos que A espera enviarle a B, básicamente ancho de banda y tamaño de los paquetes. Cada router que soporte RSVP establece un path state que incluye la dirección de donde le fue enviado el mensaje PATH, es decir la dirección del próximo salto en sentido inverso hacia el terminal A. Cuando el mensaje PATH llega a B, éste responde con el mensaje RESV (Reservation Request) que incluye un TSpec e información sobre el tipo de reservación solicitada; hay dos tipos de reservación: controlled-load y guaranteed service.

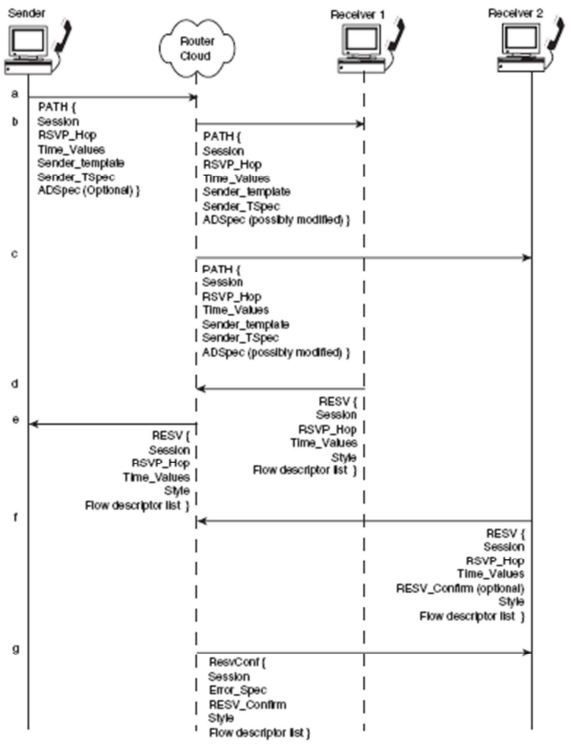
El mensaje RESV viaja de B hacia A siguiendo la misma ruta que siguió PATH pero en sentido inverso. En cada router se reservan los recursos solicitados, si hay y si B tiene autorización para ello. Finalmente, el mensaje RESV llega al terminal A con una confirmación que los recursos han sido reservados.

Es de resaltar que en RSVP la reservación es hecha por el receptor, el terminal B en nuestro caso, no por el que envía que es el terminal A. Este concepto es muy adecuado para multicast, donde hay muchos receptores y un sólo emisor. RSVP no lleva datos de usuarios, éstos son transportados por *Real-Time Transport Protocol* (RTP).

Las reservaciones hechas por RSVP son soft, lo que significa que hay que refrescarlas periódicamente.

RSVP y MULTICAST

Este es un ejemplo multicast, El Receptor1 envía un RESV antes que el Receptor2. En este ejemplo los requerimientos de QoS del Receptor1 son más fuertes que los del Receptor2, en este caso no es necesario modificar la reservación que previamente había enviado el Receptor1 dado que la misma es suficiente para satisfacer los requerimientos de ambos receptores.



Esto puede suceder por ejemplo, si el Receptor1 hace una reservación para audio y video, pero el receptor 2 sólo soporta audio., en cuyo caso el receptor 1 solicita muchos más recursos. Cuando llega la solicitud del receptor2 para el mismo servicio proveniente del mismo origen, los roueters no necesitan hacer ninguna reserva adicional ya que lo que solicita el receptor 2 está incluido en la reservación previamente hecha por el receptor 1.

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

An Architecture for Differentiated Services DiffServ RFC 2475

La idea de DiffServ es garantizar QoS a muchas aplicaciones sin la complejidad y el overhead de RSVP.

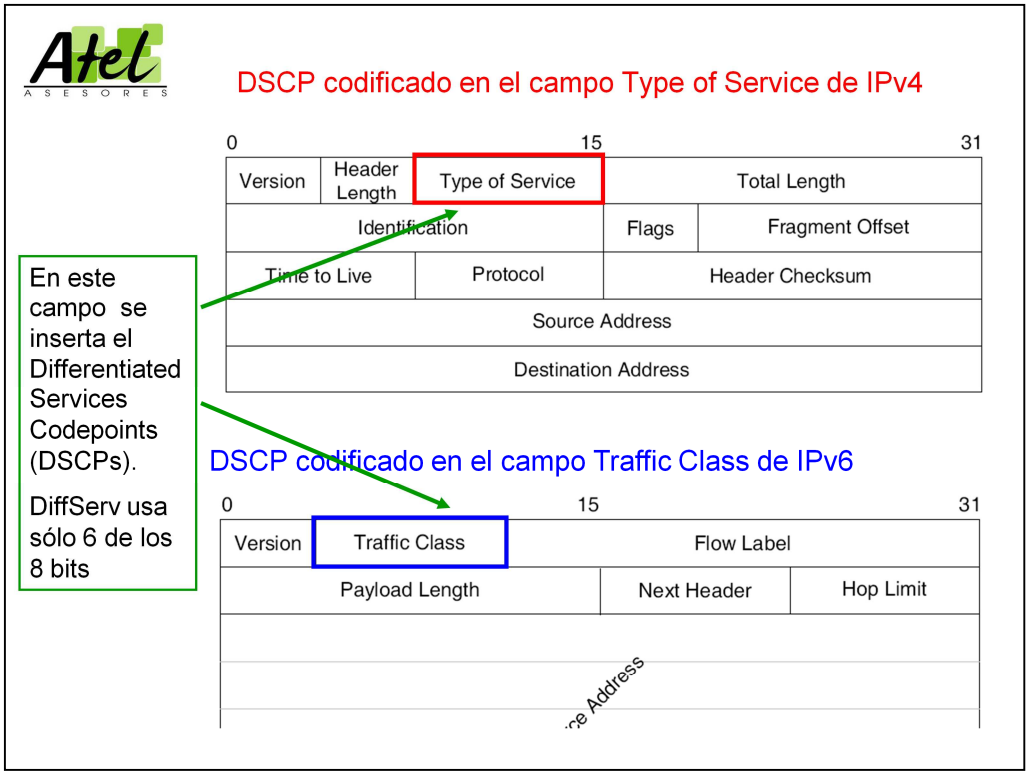
DiffServ está basado en marcar los paquetes IP y los router conocen el tipo de tratamiento que deben darle a un paquete IP de acuerdo a dicha marca, sea IPv4 o IPv6. Estos tratamientos se denominan Differentiated Services Codepoints (DSCPs). Existen dos procedimientos *Expedited Forwarding* definido *en* RFC 3246 y *Assured Forwarding* RFC 2597.
En los bordes de la red los paquetes son marcados con el DSCP correspondiente de manera que los router puedan establecer el comportamiento del paquete, esto se denomina Per-Hop Behaviors (PHBs) y se refiere al comportamiento del paquete en cada salto, de esta forma los router sólo necesitan leer la marca en el IP Header.

DiffServ parece ser el mecanismo más adecuado para garantizar QoS en Internet debido a su simplicidad y a su facilidad de escalabilidad. DiffServ introduce dos nuevos elementos funcionales “Edge Routers” y “Core Routers”.

Los Edge Routers miden el tráfico y lo clasifican en clase de servicio, y luego marca los paquetes en IN, si están de acuerdo al contrato entre el cliente y el operador, o en OUT si violan el contrato.

Los Core Routers, al recibir los paquetes marcados los envían al próximo router en función de la marca correspondiente que indica el tipo de tráfico.

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739



Cada uno de estos campos ocupa 8 bits tanto en Ipv4 como en IPv6, pero DiffServ usa únicamente 6 bits. En la red los valores de DSCP están en el encabezado IP y determinan en comportamiento del paquete, de esta forma lo único que se le exige a los routers es que examinen el DSCP y actúen en consecuencia.

Para evitar que todos los paquetes sean marcados con una alta prioridad, existen funciones en los extremos de la red para asegurar que sólo los paquetes que aplican para cada caso serán marcados con un cierto valor de DSCP. Esta funciones incluyen medición del packet rate, política para asegurarse que el tráfico cumple con ciertas condiciones, etc.

Seguridad en IMS

Los esquemas de seguridad de la red IMS son adicionales a los de la red IP de acceso (GPRS, LTE, WiMAX). De hecho IMS garantiza un nivel de seguridad de alto nivel, si la IP-CAN es objeto de intrusos no necesariamente debe ocurrir lo mismo con la red IMS.

Para acceder a una red IMS se requiere autorización, la cual está basada en realizar la autenticación de usuario conjuntamente con el registro del mismo en la red IMS.

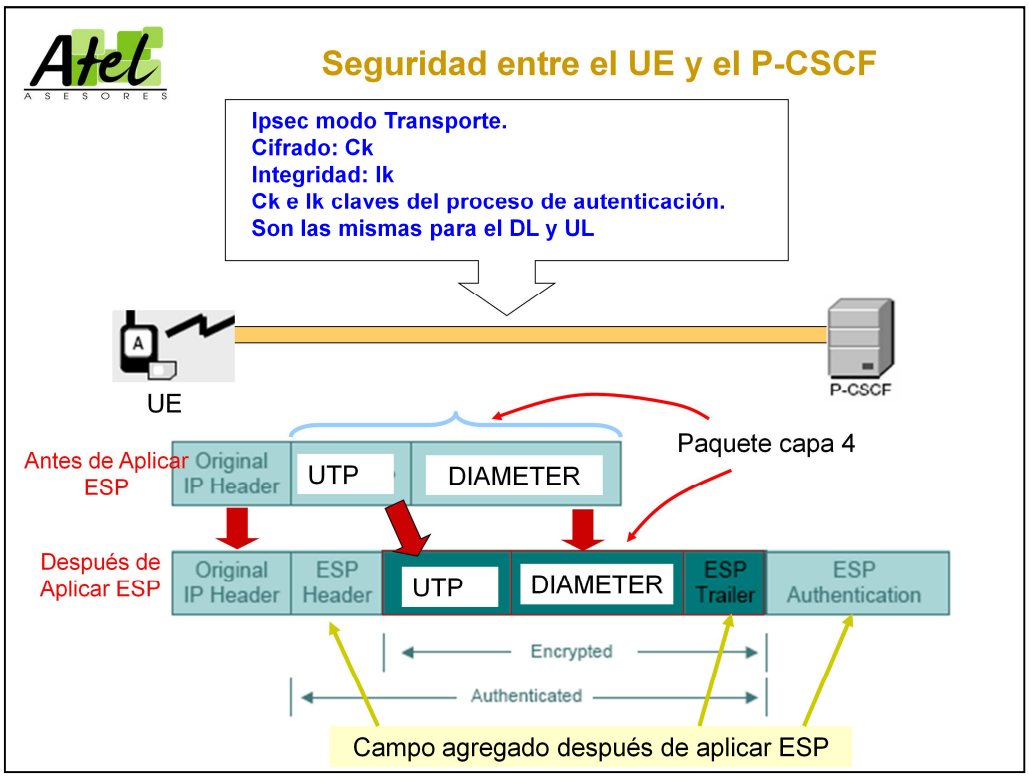
Los procesos de seguridad siempre son ejecutados por la Home Network incluso si usuario está en roaming; nunca los procedimientos de seguridad son ejecutados en la Visited Network.

El 3GPP ha definido dos grandes áreas de seguridad en IMS

- Access Security: seguridad entre la red IMS y el usuario final
- Network Security: seguridad entre redes IMS y entre los diferentes nodos dentro de una red IMS

El esquema de autenticación en IMS denominado Authentication and Key Agreement (AKA) es similar al usado en UMTS y permite hacer autenticación mutua.

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739



Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

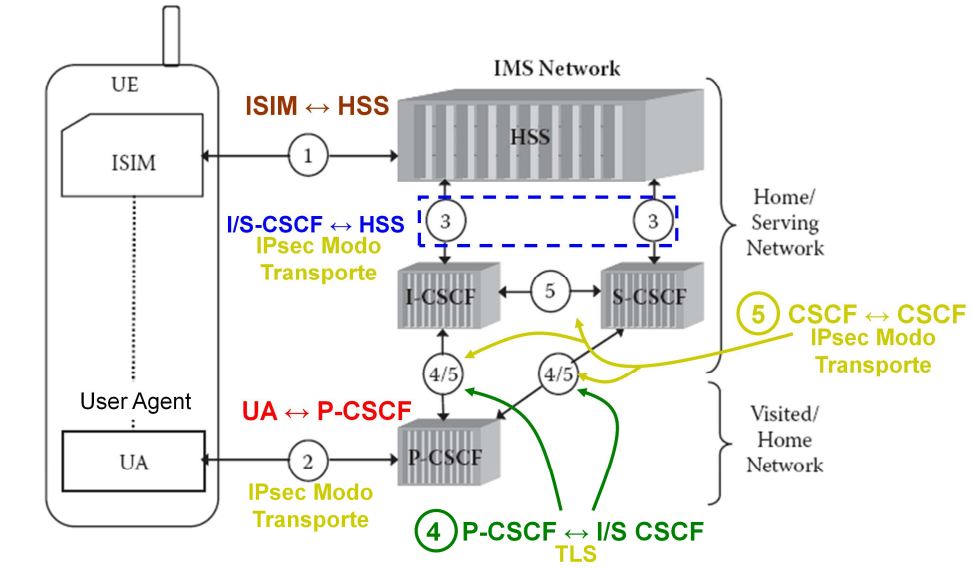
Authentication and Key Agreement (AKA)

La única información IMS que no es pública y que envía el equipo terminal a través de la red de acceso es la identificación privada IMPI. Esta información se encuentra guardada tanto en el terminal (típicamente en la UICC) como en el HSS. De igual forma en el UE y en el HSS se encuentra una clave secreta K.

En general el proceso consiste en que el UE debe enviar la IMPI al HSS, con lo cual este último ubica la clave secreta K correspondiente a la IMPI. Así, la clave secreta nunca viaja entre la ISIM y el HSS. Luego usando un algoritmo de criptografía conocido tanto por el UE como por la red IMS, se generan ciertas claves en ambos lados tanto en la red IMS como en el UE, finalmente comparando estas claves y verificando que coinciden se realiza la autenticación mutua

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

Arquitectura de la Seguridad en IMS



IMS tiene 5 Asociaciones de Seguridad definidas en 3GPP TS 33.203, Cuando el P-CSCF está en el Home Network aplica la asociación de seguridad #5, sino aplica la #4.

El UA es un SIP UA (SIP User Agent), es un software corriendo en un equipo terminal o un software corriendo en un SIP Server, en este caso se refiere al equipo terminal. Los equipos terminales pueden ser muy diversos: PCs, Laptops, teléfonos SIP, teléfonos celulares, PDAs, IPTV set top boxes, etc.

Aquellos equipos terminales que no tengan incorporada una UICC, debe usar el protocolo HTTP para la autenticación de acuerdo a lo establecido en el RFC 2617.

1. ISIM ↔ HSS: Necesario para la autenticación mutua. Tanto el HSS como el IMSI tienen almacenada una clave secreta así como la identificación privada asociada a dicha clave.

2. UA ↔ P-CSCF: Garantiza un enlace seguro entre el UE y la red IMS

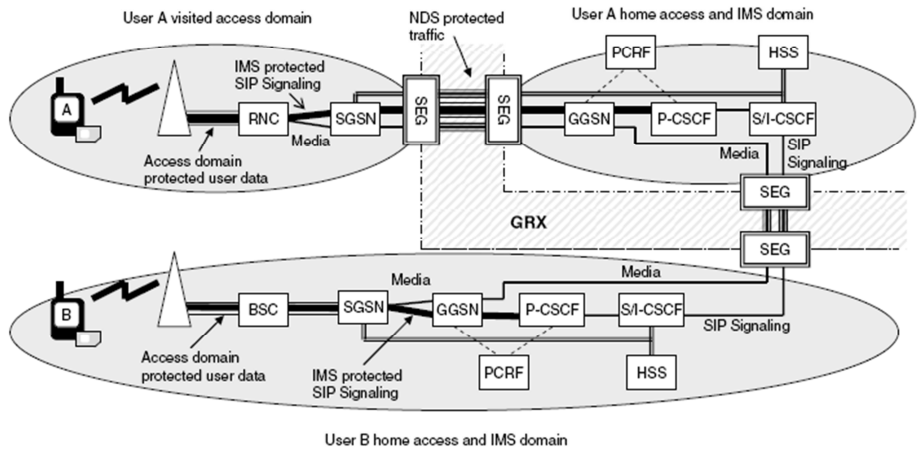
3. I/S-CSCF ↔ HSS: provee una asociación de seguridad para la transferencia de información entre el I/S-CSCF y el HSS

4. P-CSCF ↔ I/S-CSCF: Esta asociación de seguridad se aplica sólo cuando el P-CSCF no se encuentra en el Home Network, por ejemplo en el Visited Network. SI el P-CSCF está en el Home Network aplica la asociación de seguridad #5.

5. CSCF ↔ CSCF: Suministra la seguridad entre nodos SIP dentro de una misma red, ejemplo el Home Network.

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

Usuarios IMS con acceso en el Home y en Roaming



SEGs: SEcurity Gateways

NDS: Network Domain Security

GRX: GPRS Roaming eXchange

Las líneas gruesas indican enlaces protegidos mientras que las finas enlaces desprotegidos.

Los datos de usuario pueden estar protegidos a nivel de la red de acceso. pero en general en las redes móviles esta protección es opcional. Sin embargo, toda la señalización SIP en la red de acceso es vista como datos de usuario, por lo que pudiese estar desprotegida.

Por ejemplo, en LTE el cifrado y la Integridad son obligatorios para la señalización, pero para los datos el cifrado es opcional y no aplica la integridad.

Para mitigar esta situación en IMS es obligatorio la integridad, y opcional la confidencialidad, de todos los mensajes SIP que se envían entre el UE y el P-CSCF. La integridad y la confidencialidad se aseguran por medio de las claves IK y CK, respectivamente. De esta forma, aunque la señalización SIP no esté protegida por la red de acceso si lo está por ser de IMS.

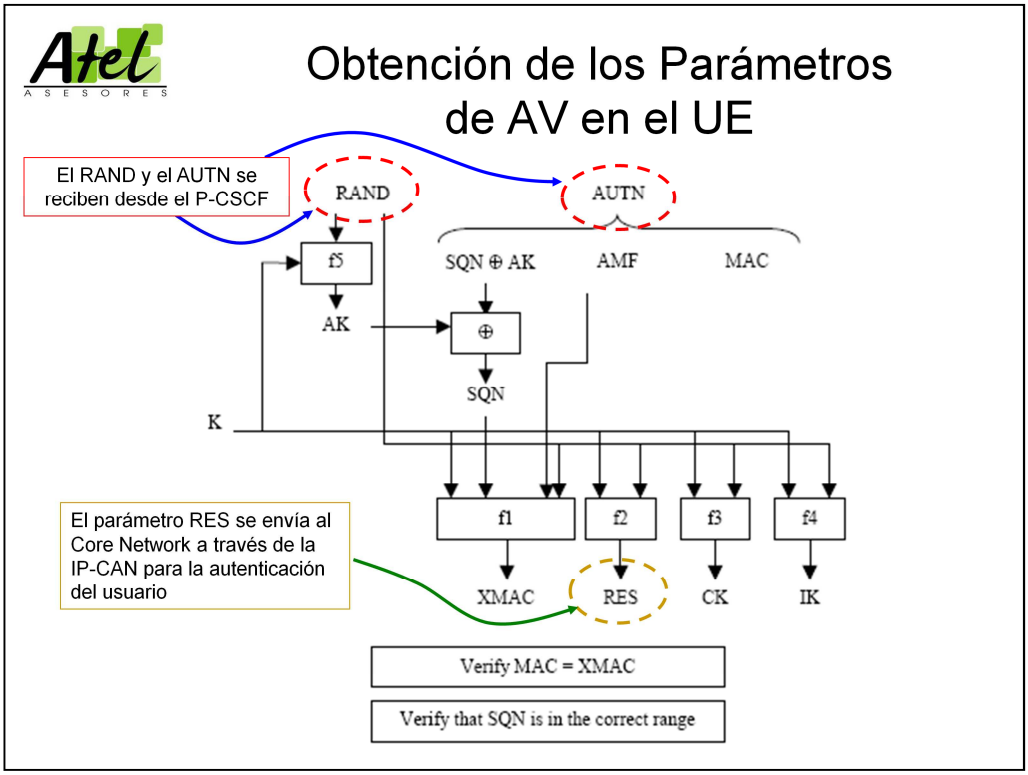
Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

Vector de Autenticación

Con la clave secreta y la IMPI se corren una serie de algoritmos de seguridad para justamente generar el Vector de Autenticación que consiste en una serie de parámetros de seguridad que se intercambian entre el UE y la red IMS.

- RAND: Randon Challenge
- RES/XRES: Response/Expected Reponse
- CK: Cipher Key
- IK: Integrity Key
- AUTN: Authentication Network

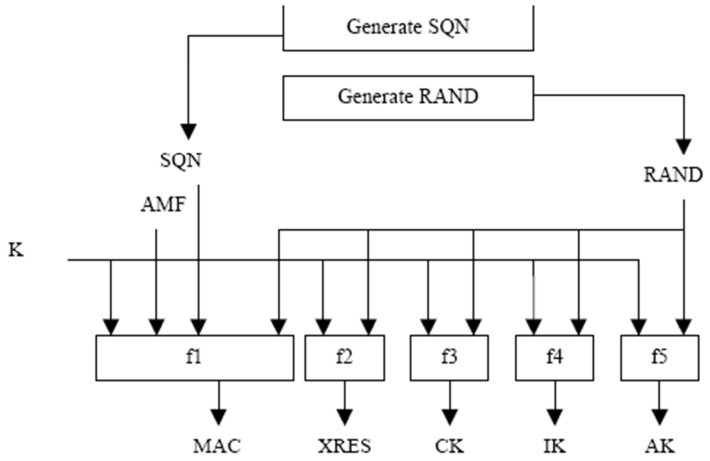
Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739



A partir del RAND y del AUTN, y de la clave secreta, el ISIM puede calcular los parámetros necesarios para autenticar la red IMS y enviar su respuesta RES a la red de manera que el ISIM sea autenticado por la misma.

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739

Generación del Vector de Autenticación en el core IMS



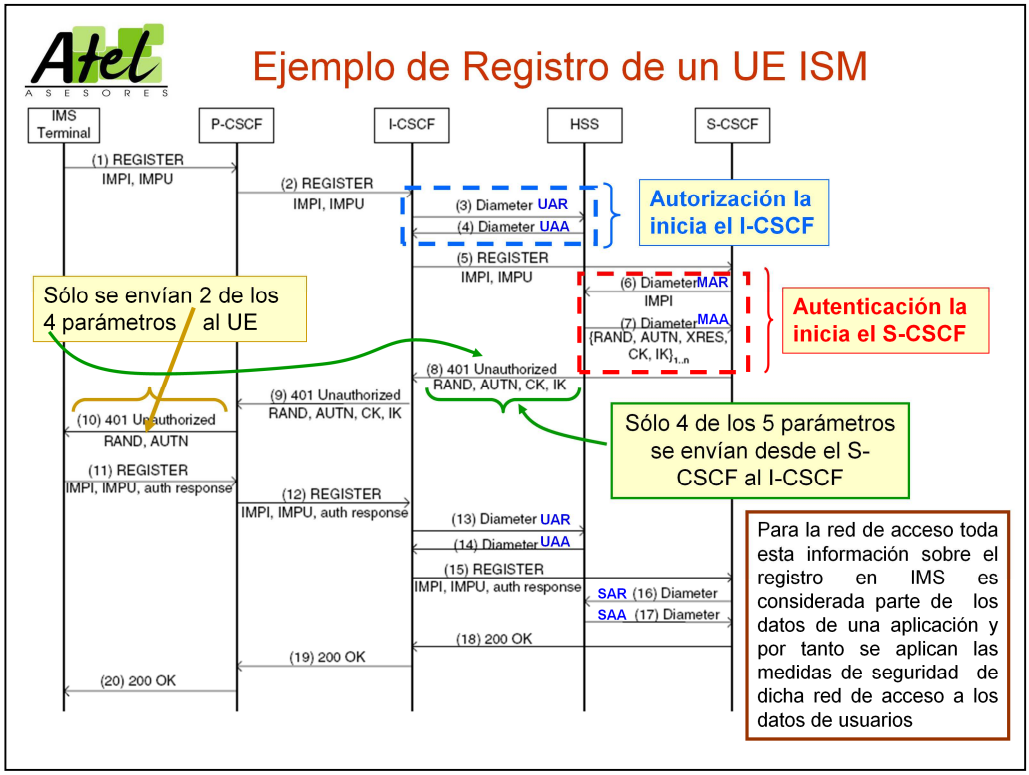
AMF: Authentication Management Field

|| ||: significa concatenación

AUTN := SQN ⊕ AK || AMF || MAC

AV := RAND || XRES || CK || IK || AUTN

Atel Asesores C.A atel.asesores@cantv.net www.atelasesores.com.ve +58 212-9417771 416-6306739



El proceso lo inicia el terminal IMS enviando un mensaje SIP REGISTER (1) dirigido al P-CSCF con su identidad privada y pública IMPI e IMPU, respectivamente. Dicho mensaje atraviesa la red IP-CAN antes de llegar al P-CSCF, el cual reenvía el mensaje al I-CSCF (2). El I-CSCF envía un mensaje DIAMETER de solicitud de autenticación del usuario que envío el mensaje REGISTER, DIAMETER UAR (3) al HSS, quien responde con otro mensaje DIAMETER URR (4) y simultáneamente informa al I-CSCF la dirección del S-CSCF asignado al usuario. Luego el I-CSCF reenvía el mensaje de REGISTRO al S-CSCF (5), el cual a su vez envía el mensaje DIAMETER MAR (6) que incluye el IMPI, con el IMPI el HSS calcula el vector de autenticación (AV) y genera la quíntupla <RAND, AUTN, XRES, CK, IK> y regresa la quíntupla al S-CSCF a través del mensaje DIAMETER MAA (7). Este mensaje es un indicativo de que la red está solicitando que el terminal corra sus algoritmos de seguridad a fin de hacer la autenticación. A continuación, el S-CSCF envía el mensaje SIP tipo respuesta 401 Unauthorized (8) acompañado de cuatro de los cinco parámetros que forman el AV <RAND, AUTN, CK, IK> dirigido al I-CSCF, quien retransmite el mensaje al P-CSCF (9). Nuevamente el P-CSCF retransmite el mensaje al UE pero dejando sólo dos parámetros en el AV (10), específicamente el RAND y el AUTN.

Dado que el terminal tiene almacenada la misma clave secreta que tiene el HSS correspondiente el usuario en cuestión, puede calcular el AUTN, si este coincide con el que recibió de la red se considera que la red es legítima. El UE también calcula su respuesta RES, la cual se envía en otro mensaje SIP REGISTER junto IMPI y el IMPU (11); dicho mensaje llega al P-CSCF el cual lo reenvía al I-CSCF (12). Después el I-CSCF envía un mensaje DIAMETER UAR (13) al HSS quien le responde con la dirección del S-CSCF a través de un mensaje DIAMETER UAA (14) que se ocupa del usuario, entonces el I-CSCF retransmite el mensaje de registro junto a RES al S-CSCF (15), éste último envía el mensaje DIAMETER SAR (16) al HSS quien responde con el mensaje DIAMETER SAA (17), si el parámetro RES enviado por el usuario es igual al XRES que había calculado el HSS en el primer intento de registro, entonces el HSS autentica al usuario lo cual se confirma por medio del mensaje (17), seguidamente el S-CSCF envía un mensaje SIP 200 OK (18) al P-CSCF y finalmente dicho mensaje llega al usuario.