Senyalització per a veu IP (VoIP)

Ferran Adelantado i Freixer

PID_00201819

Temps de lectura i comprensió: **4 hores**

Universitat Oberta de Catalunya

Índex

Introducció

La millora de les xarxes de telecomunicació –en termes d'amplada de banda, retard, fiabilitat, extensió, etc.– ha permès arreu del món, però particularment en els països més desenvolupats, l'aparició i oferta de serveis de banda ampla. En aquest context, les comunicacions de veu no n'han quedat al marge i la veu sobre IP (en anglès *voice over IP*, VoIP) pren força en el present i amb vista al futur.

Tot i l'augment imparable de la demanda de serveis de banda ampla, així com el desplegament constant de noves xarxes de paquets, no es pot oblidar que les xarxes de commutació de circuits existents (XTC o XDSI) són una part molt important del total de xarxes d'accés i de transport actuals. En el futur sembla evident que les xarxes de commutació de circuits perdran importància i seran substituïdes progressivament per xarxes de commutació de paquets (xarxes IP). Malgrat aquesta certesa, una de les necessitats principals d'avui en dia és aconseguir la interoperabilitat de les noves xarxes de paquets i les velles xarxes de commutació de circuits.

És en el marc d'aquesta interoperabilitat que aquest mòdul presenta dues parts ben diferenciades. La primera part adreça el conjunt de protocols SIGTRAN, la solució definida per la ITU-T per a interconnectar la XTC o la XDSI amb la xarxa IP. L'objectiu final d'aquest conjunt de protocols és definir una capa de transport que permeti complir amb els estrictes requisits de la senyalització SS7, així com establir un grup de capes d'adaptació d'usuari que permetin l'intercanvi de senyalització entre punts de senyalització de la xarxa SS7 i nodes de la xarxa IP.

La segona part del mòdul, en canvi, se centra en un dels protocols de senyalització de les xarxes IP més estesos i prometedors: el *Session Initiation Protocol* (SIP).

Objectius

Els objectius que ha d'assolir l'estudiant un cop estudiats els materials didàctics d'aquest mòdul són:

1. Entendre el canvi de paradigma en les comunicacions de veu i què l'ha motivat.
2. Conèixer el conjunt de protocols que permeten la interconnexió de la xarxa commutada de telefonia i la xarxa IP.
3. Entendre els fonaments de les capes d'adaptació d'usuari definides a SIGTRAN.
4. Saber quines són les característiques que fan del protocol SCTP un bon candidat per al transport de senyalització.
5. Entendre, de manera introductòria, el protocol SIP i la seva importància a les xarxes IP.

1. Veu IP: els fonaments

Fins fa relativament pocs anys el concepte de veu sobre IP (més conegut per l'acrònim anglès VoIP, és a dir, *voice over IP*) era desconegut. S'associava el protocol IP, de la capa de xarxa, a la transmissió de dades més que no pas a la transmissió de veu. Ara, però, no només es coneix el concepte sinó que la veu IP és una realitat.

Hi ha dos motius bàsics pels quals la veu IP, una tecnologia que inicialment presentava dubtes seriosos, ha acabat tenint èxit:

- **La disminució dels costos**. El pas de la telefonia basada en commutació de circuits cap a a una telefonia basada en commutació de paquets (telefonia IP) aconsegueix un increment de l'eficiència. Ja no és necessari reservar circuits per a una única trucada, sinó que la transmissió per commutació de paquets permet maximitzar la utilització de cada enllaç (multiplexant diversos fluxos de dades o veu). En termes de senyalització, a més, la implantació de la veu IP suposa no haver de mantenir una xarxa paral·lela de senyalització*, amb el conseqüent estalvi. Fixem-nos, en termes d'eficiència, que els sistemes de compressió que permeten la veu digitalitzada (com per exemple la detecció d'activitat per a disminuir els bits transmesos en períodes de silenci) minimitzen el trànsit transportat a través de les xarxes de comunicació. En qualsevol cas, la reducció de costos es tradueix en una disminució del preu del servei.

  *** Recordem que la xarxa de senyalització SS7 era paral·lela a la xarxa XTC.**

- **Independència de la distància**. La tarifació i la senyalització de trucades internacionals mitjançant VoIP no afegeix dificultats addicionals respecte de les trucades nacionals, com sí que succeeix en el cas de les trucades a través de la XTC (Xarxa Telefònica Commutada).

- **La convergència de les xarxes**. L'augment de les comunicacions de dades durant les darreres dècades ha estat enorme. Aquest fet, tenint en compte que la majoria d'aquestes transmissions de dades es basen en el protocol de xarxa IP, ha produït un augment de l'extensió de les xarxes de comunicacions arreu del món. En aquest context, les xarxes de telefonia no podien quedar al marge de la tendència a convergir envers les anomenades xarxes *All-IP* que han experimentat totes les xarxes de telecomunicacions.

- **Nous serveis**. La telefonia IP, per definició, permet oferir tant el servei de dades com de vídeo i dades a través d'una xarxa IP.

Tot i així, també és bo destacar els desavantatges de la implementació de la VoIP:

- **Necessitat d'amplada de banda al bucle local**. La utilització de telefonia IP obliga a tenir connexió de dades amb una mínima amplada de banda al bucle local. Malgrat que aquest era un problema greu en el moment de l'aparició de la VoIP, es tracta d'un problema que ha anat disminuint gràcies a l'extensió de les xarxes d'accés de banda ampla.

- **Trucades d'emergència**. Les trucades d'emergència a la XTC permeten determinar la localització de l'abonat, un fet determinant per a la redirecció necessària de la trucada. Aquesta localització de l'abonat no és immediata en el cas de la VoIP, ja que l'adreça IP no està necessàriament lligada a una adreça física.

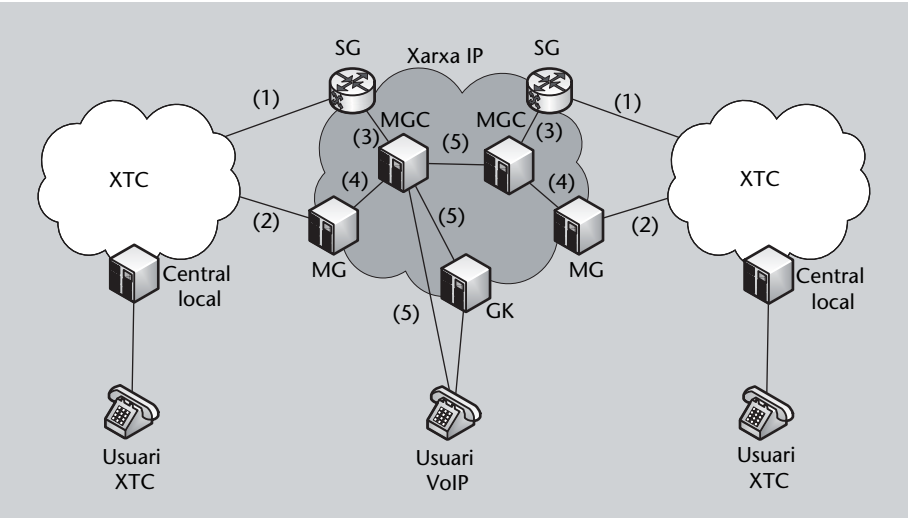
- **Talls de llum**. Quan hi ha un tall del servei elèctric el terminal de VoIP resta fora de servei.

- **Qualitat de servei**. Garantir qualitat de servei (en anglès, *Quality of Service*, QoS) mitjançant l'accés a Internet no és senzill. Per a la veu IP, és necessari garantir, entre d'altres coses, un retard màxim per als paquets IP.

La tecnologia associada a la VoIP i el seu desplegament, però, no pot obviar l'existència –i l'extensió– de la xarxa telefònica *convencional* existent, l'anomenada XTC. És per aquest motiu que, malgrat el prometedor futur de la VoIP, cal afrontar el repte d'interconnectar les xarxes IP i les xarxes XTC.

La figura 1 mostra de manera esquemàtica la interconnexó de les dues xarxes i els nodes principals que ho permeten. A la figura s'hi representen dues xarxes XTC i una xarxa IP.

Figura 1. Connexió de les xarxes XTC i IP



Per mirar de facilitar-ne la comprensió, s'ha afegit un usuari final (també anomenat *User Agent*, UA) a cadascuna de les xarxes i els nodes fonamentals, entre els quals cal destacar els següents:

- **Signalling Gateway (SG)**. Es tracta d'un node fonamental que connecta la xarxa de senyalització de la XTC amb el *Media Gateway Controller* (MGC) de la xarxa IP. Aquest node està íntimament relacionat amb la senyalització SS7 que hem detallat al mòdul anterior, ja que permet adaptar la senyalització de la XTC perquè es pugui transportar a través de la xarxa IP. Convé adonar-se, d'acord amb aquesta descripció, que els enllaços marcats amb un (1) a la figura 1 són enllaços SS7. A la sortida de l'SG el conjunt de protocols utilitzats, ja a la xarxa IP, és l'anomenat SIGTRAN, marcat amb un (3) a la figura. Aquest conjunt de protocols són objecte d'estudi en els apartats propers.

SIGTRAN

Aquesta és la denominació del conjunt de protocols definits amb l'objectiu d'adaptar els missatges rebuts en un format SS7 per a transportar-los a través d'una xarxa IP. El marc general per a aquest protocol es pot consultar a l'RFC 2719 de la IETF.

- **Media Gateway (MG)**. És el node que converteix la informació que li arriba dels circuits de veu de la XTC a un format adequat per a la xarxa IP. Per tant, i d'acord amb la nomenclatura de la figura, els enllaços marcats amb un (2) són enllaços de veu de la XTC. El node converteix les connexions de veu per tal de transferir la informació en formats adequats per a la xarxa IP, com per exemple l'RTP (*Real Time Transport Protocol*). Aquest protocol, malgrat la seva importància, queda fora de l'abast d'aquesta assignatura, i es treballa en altres assignatures del pla d'estudis. La relació entre l'MG i l'MGC es fa a través del protocol definit per la ITU-T, l'H.248.1* (amb un (4) a la figura).

Protocol H.248.1

L'H.248.1 és una Recomanació de la ITU-T. Es tracta d'una nova versió d'un protocol inicialment definit per la IETF amb el nom de MEGACO i inclòs a l'RFC 3525.

- **Media Gateway Controller (MGC)**. Aquest node controla tant l'SG com l'MG. Així, estableix comunicació entre tots dos nodes per tal de processar la informació de la trucada. Tindria funcions similars a les d'un commutador en una XTC. També es coneix amb el nom de *Call agent*. Per l'altra banda, també es comunica i controla un conjunt de *gatekeepers* (GK).

- **Gatekeeper (GK)**. Les funcions bàsiques d'aquest node són el control d'accés a la xarxa i la traducció d'adreces IP. La VoIP basa el seu adreçament, com qualsevol servei sobre IP, en l'adreça IP. Tot i així, el servei de telefonia es basa en un sistema de numeració diferent (definit a la Recomanació E.164 de la ITU-T). La traducció d'un sistema a l'altre, o la decisió sobre l'encaminament dels paquets la du a terme el GK. Com que els *gatekeepers* habitualment realitzen les seves funcions per a un conjunt de terminals/usuaris d'una zona, poden establir comunicació amb altres *gatekeepers* per a fer la traducció de l'adreça i l'encaminament. La comunicació entre dos GK, amb l'MGC o amb l'usuari es fa d'acord amb protocols com ara el *Session Initiation Protocol* (SIP) o l'H.323. A la figura s'assenyala amb el (5).

SIP i H.323

Són dos dels protocols de senyalització més importants per a VoIP. En el cas del SIP, es tracta d'un protocol definit per la IETF, mentre que l'H.323 ha estat definit per la ITU-T.

Per tal de fer una mica més entenedora l'estructura de la figura 1, proposem dos exemples senzills que han de permetre visualitzar els processos que s'esdevenen a la xarxa.

Exemple 1

Imaginem una trucada generada per un usuari connectat a la XTC cap a un usuari connectat, directament, a la xarxa IP. La senyalització arriba a l'SG des de la xarxa SS7. S'estableix una connexió entre l'SG i l'MGC (amb els protocols SIGTRAN). A partir d'aquest moment l'MGC estableix una connexió de senyalització entre l'MGC i l'MG, utilitzant el protocol H.248, per tal que s'estableixi una connexió de dades entre l'usuari final i l'MG. Aquesta connexió de dades seria una connexió RTP sobre IP.

Exemple 2

El segon exemple és el cas contrari; és a dir, la trucada és generada per un usuari connectat a la xarxa IP i l'usuari final està connectat a la XTC. En aquest cas, en primer lloc l'usuari es comunica amb el GK tant perquè tradueixi el número de telèfon de l'usuari final en una adreça IP, com perquè determini l'adreçament apropiat per a arribar a l'usuari final (connectat a la XTC). Un cop obtinguda aquesta informació del GK, l'usuari inicial estableix un canal de senyalització amb l'MGC que, alhora, estableix un canal de senyalització entre l'MGC i l'MG, i entre l'MGC i l'SG. En acabat, l'MG estableix la connexió de dades entre l'usuari i l'MG.

Del que hem vist fins ara cal que tinguem presents les conclusions següents:

- La senyalització i el circuit de veu, en una XTC, utilitzen xarxes diferents i, per tant, arriben a la xarxa IP a través de diferents nodes (la senyalització a través de l'SG i la veu a través de l'MG).

- Com que tant la veu com la senyalització tenen formats diferents a la XTC (o XDSI) i a la xarxa IP, calen protocols que en permetin l'adaptació.

Aquest mòdul té un doble objectiu. Per una banda aprofundir en l'adaptació de la senyalització de la xarxa SS7 perquè pugui ser transportada a través de la xarxa IP. Per altra banda, introduir el protocol de senyalització més utilitzat per a connexions de veu en una xarxa IP, el SIP.

2. El conjunt de protocols *Signaling Transport* (SIGTRAN)

El conjunt de protocols de l'SS7 presenta diverses característiques que en dificulten l'adaptació a les xarxes IP. En concret, la pila de protocols SS7 defineix nivells/capes equivalents a les tres capes baixes del model OSI (des de la capa MTP1, considerada la capa física, fins a la capa MTP3, que seria la capa de xarxa). Convé recordar, addicionalment, que el protocol IP és un protocol de la capa de xarxa (capa 3), i que per aquest motiu és difícil adaptar les dues piles de protocols.

El conjunt de protocols denominats amb el nom de SIGTRAN té la intenció de permetre el transport, a través de la xarxa IP, de la senyalització SS7.

Els protocols de transports més habituals per a IP són el protocol TCP (*Transmission Control protocol*) i el protocol UDP (*User Datagram Protocol*). Pel que fa a la connexió de veu en temps real, les xarxes IP utilitzen el protocol de transport RTP (*Real Time Transport Protocol*). Ara bé, per a la connexió de senyalització SS7, la IETF, durant la definició del conjunt de protocols SIGTRAN, va haver de decidir quin protocol de transport s'utilitzava. Els requisits que havia de complir qualsevol protocol de transport eren els següents:

- **Transport fiable de la informació de senyalització**. Tal com s'ha estudiat al mòdul anterior, la informació de senyalització és molt sensible i és per aquest motiu que la capa MTP implementa mecanismes de correcció d'errors.

- **Retards baixos**. El retard màxim permès per a la informació de senyalització està limitat a la xarxa SS7 pels requisits que imposa el servei de telefonia ofert per la XTC i/o la XDSI.

- **Redundància**. La xarxa SS7 està definida de manera que garanteix redundància gràcies als múltiples camins possibles. És per aquest motiu que els nodes STP estan desplegats per parelles i amb enllaços redundants.

Per a fer front a aquests requisits, el protocol de transport emprat per a la senyalització SS7 no pot ser l'UDP. Com és sabut, el protocol de transport UDP no implementa control de flux ni correcció d'errors. Així doncs, la utilització d'UDP com a protocol de transport no permetria garantir ni el transport fiable de la informació ni la redundància. Per contra, sí que permetria tenir retards baixos.

Vegeu també

Al mòdul "Un sistema universal de senyalització: *Signalling System No. 7 (SS7)*" d'aquesta assignatura s'explica que la capa MTP implementa mecanismes per a una transmissió/recepció fiable i mantenint l'ordre dels missatges.

Lectura complementària

En cas que vulgueu aprofundir en el coneixement dels protocols TCP i UDP, podeu llegir el llibre *The TCP/IP guide: A comprehensive, illustrated Internet Protocol Reference*.

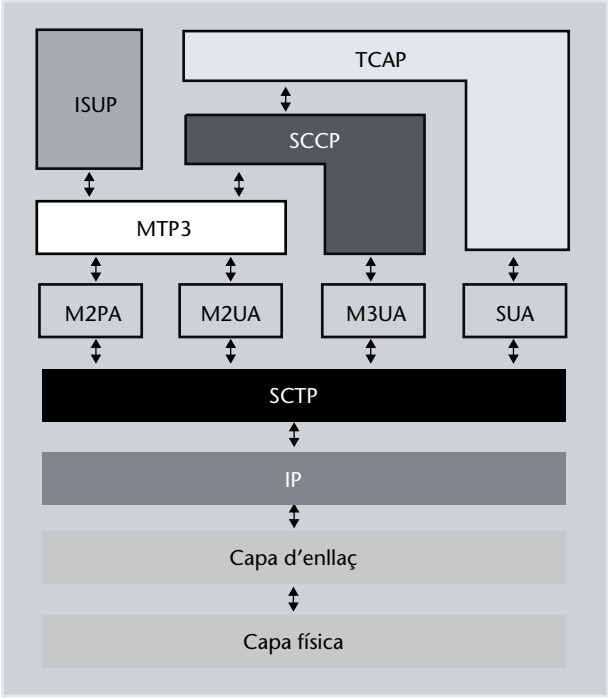
Pel que fa al protocol TCP, ofereix un servei de transport fiable i ordenat de la informació, però en canvi no és apropiat per a garantir retards baixos. El protocol, per definició, implementa un mecanisme de control de flux amb una finestra lliscant i requereix la notificació positiva de recepció dels paquets transmesos. El problema de TCP és que els errors de transmissió d'un paquet endarrereixen la transmissió dels paquets següents i, per tant, n'afecten negativament el retard. A més, TCP presenta problemes davant dels anomenats atacs DoS (*Denial of Service*).

Els protocols de la capa de transport TCP i UDP no són l'objecte d'estudi d'aquesta assignatura. Malgrat tot, hi ha nombroses referències que permeten aprofundir-hi en cas que es vulguin conèixer millor.

Així doncs, el conjunt de protocols SIGTRAN defineix un nou protocol de transport sobre IP que permet garantir els requisits exigits per a la senyalització SS7: l'*Stream Control Transmission Protocol* (SCTP). Un cop definit el protocol de la capa de transport, SIGTRAN defineix un conjunt de capes d'adaptació d'usuari entre els protocols definits a l'SS7 i el protocol de transport SCTP. Aquestes capes d'adaptació d'usuari (en anglès *User Adaptation layer*, UA) són les quatre que es mostren a la figura 2: *MTP2-user Peer-to-peer Adaptation* (M2PA), *MTP2-User Adaptation* (M2UA), *MTP3-User Adaptation* (M3UA), i *SCCP User Adaptation* (SUA)*.

*** SIGTRAN també defineix capes d'adaptació d'usuari per a la senyalització d'accés, com per exemple V5UA i IUA, però el seu estudi no és l'objectiu d'aquesta assignatura.**

Figura 2. Protocols definits per SIGTRAN



Tal com es pot observar a la figura 2, tenim una capa de xarxa basada en IP i una xarxa de transport basada en el protocol SCTP. Per sobre, una capa d'adaptació d'usuari composta de quatre protocols. Cadascun té la funció d'adaptar un tipus diferent d'usuari fent transparent als usuaris de capes superiors quines capes hi ha per sota (en aquest cas SCTP i IP). És a dir, les capes M2UA i

M2PA han d'aconseguir que, per a la capa MTP3, no hi hagi diferència entre transportar els missatges amb SCTP o fer-ho amb MTP2. El mateix es pot dir de l'M3UA, que ha de permetre a l'SCCP funcionar correctament, o de l'SUA, que ha de fer el mateix amb la TCAP.

En aquest apartat ens centrarem en aquells protocols que componen el SIGTRAN: SCTP, M2UA, M2PA, M3UA i SUA.

2.1. *Stream Control Transmission Protocol* (SCTP)

El protocol SCTP té l'objectiu de fer front als requisits que planteja la senyalització SS7 i que ja hem assenyalat. En general el protocol SCTP presenta moltes semblances amb el protocol TCP i introdueix algunes millores. Es tracta, doncs, d'un protocol de transport fiable (hi ha notificacions i retransmissions), en totes dues direccions (és a dir, *full-duplex*), i que implementa un control de congestió i de flux molt semblant a l'implementat al TCP i basat en el concepte d'*Additive-Increase Multiplicative-Decrease* (AIMD)*.

*** Aquest és un dels punts clau al protocol i s'implementa mitjançant els mecanismes de *slow start* i *congestion avoidance*.**

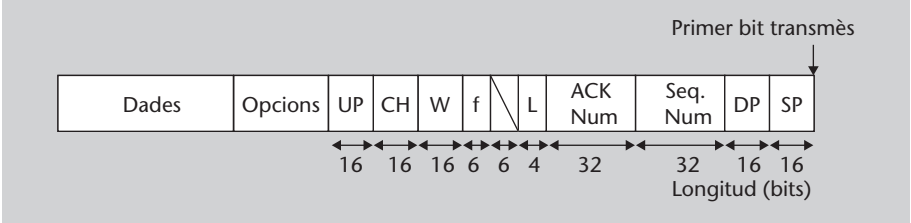
Tal com és sabut, el control de congestió i de flux a TCP (de la mateixa manera que passa a SCTP) es basa en la recepció de confirmacions positives de recepció de paquets i en l'anomenada finestra lliscant *sliding window*. El receptor no necessàriament ha de notificar la recepció correcta de cadascun dels missatges enviats per TCP, sinó que pot reconèixer un conjunt de missatges per a disminuir el nombre de missatges de notificació que cal enviar**.

**** Aquest mecanisme de notificació és molt similar al mecanisme anomenat *go-back N* però permet descartar missatges que arriben fora de seqüència.**

Una altra de les característiques del protocol SCTP que el diferencia del protocol TCP és que està orientat a missatge i no pas a byte. De fet, aquest és un aspecte que es pot observar fàcilment si mirem el format d'un segment TCP a la figura 3 i d'una *Protocol Data Unit* (PDU) d'SCTP, que es mostra a la figura 4.

És convenient constatar que, en essència, els segments de TCP i les PDU d'SCTP tenen estructures similars. Ara bé, la PDU transporta la informació dividida en *chunks*, mentre que el segment TCP no divideix les dades en unitats més petites. Aquest és un punt clau per a superar el problema del retard excessiu, tal com s'explicarà a continuació.

Figura 3. Segment del protocol TCP



Els paràmetres del segment TCP són els següents:

Protocol TCP

Si voleu consultar amb més detall l'estructura del segment TCP, podeu adreçar-vos a l'RFC 793.

- **Port d'origen (*Source Port*, SP) i Port de destinació (*Destination Port*, DP)**. Els ports de destinació i d'origen permeten determinar les aplicacions d'origen i de destinació. Cadascun té una longitud de 16 bits.

- **Número de seqüència (*Sequence Number*)**. Camp que permet identificar el primer byte del camp de dades. És a partir d'aquest valor que es realitza la notificació de recepció correcta. Té una longitud de 32 bits.

- **Número de notificació (*Acknowledgement number*)**. Aquest camp de 32 bits és utilitzat per a notificar la recepció correcta d'un segment anterior. El valor d'aquest camp notifica la recepció correcta de tots els bytes que tenen un número de seqüència inferior.

- **Longitud de la capçalera (*Header length*, L)**. El valor de la longitud s'expressa en múltiples de 32 bits (és a dir 4 bytes).

- ***Flags* (f)**. Sis camps, d'un bit de longitud cadascun, que determinen si el segment conté el punter a dades urgents (UP), si el camp d'*acknowledgement number* té informació vàlida, el tipus de gestió de la memòria interna del receptor, l'avortament de la connexió, si es tracta d'un missatge *Synchronize* (inici de connexió) o *Finalize* (final de la connexió). Tots junts tenen una longitud de 6 bits.

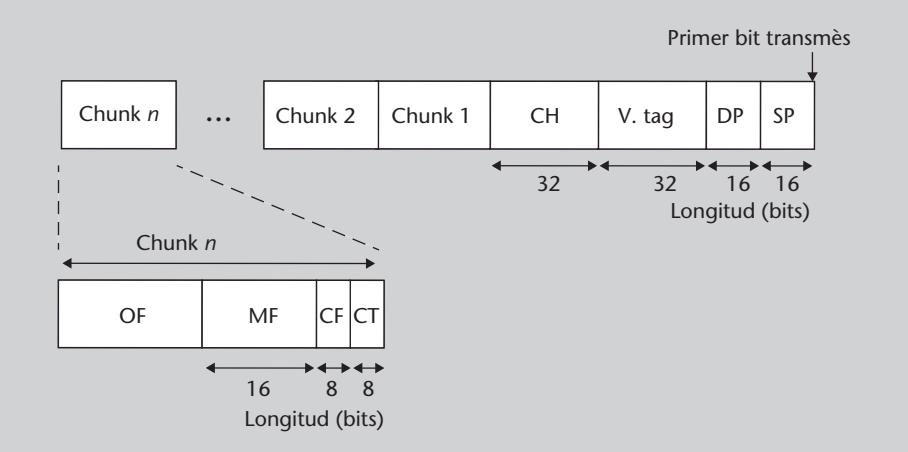
- **Finestra de recepció (*Receive window*, W)**. Mida de la finestra que el receptor comunica al transmissor. Té una longitud de 16 bits.

- **Detector d'errors (*Checksum*, CH)**. Té una longitud de 12 bits.

- **Punter a dades urgents (*urgent data pointer*, UP)**. Camp de 16 bits que permet indicar la localització, dins de les dades del segment, de les dades urgents (en cas que n'hi hagi).

- **Opcions**. Conjunt de camps opcionals.

Figura 4. PDU del protocol SCTP



Per la seva banda, els paràmetres de les PDU d'SCTP són els que es detallen a continuació:

Protocol SCTP

Si voleu consultar amb més detall l'estructura de la PDU de l'SCTP, podeu adreçar-vos a l'RFC 4960.

- **Port d'origen (*Source Port*, SP) i Port de destinació (*Destination Port*, DP)**. Aquests camps tenen la mateixa funció que als segments TCP. Cadascun té una longitud de 16 bits.
- **Verificació (*Verification tag*, V. tag)**. Camp de 32 bits que s'utilitza per a verificar la identitat del transmissor.
- **Detector d'errors (*Checksum*, CH)**. Té una longitud de 32 bits i du a terme la mateixa funció que als segments TCP.
- ***Chunk***. El *chunk* és la unitat de transport de dades o de senyalització. El *chunk* té una longitud variable, en funció del tipus de *chunk*. Pel que fa a l'estructura interna de cadascun dels *chunks*, la figura 4 mostra que consta del tipus de *chunks*, els *flags* (no definits a l'estàndard i, per tant, no s'utilitzen), la longitud del *chunks*, i, finalment, les dades.
- **Tipus de *chunk* (*Chunk Type*, CT)**. Camp de 8 bits de longitud. Els valors més destacats que pot prendre són DATA (*payload data*), INIT (*initiation*), INIT ACK (*initiation acknowledgement*), SACK (*selective acknowledgement*), ABORT, SHUTDOWN, SHUTDOWN ACK, o SHUTDOWN COMPLETE.
- ***Flags* del *chunk* (*Chunk flags*, CF)**. Camp de 8 bits no utilitzat actualment.
- **Camps obligatoris (*Mandatory Fields*, MF)**. El nombre de camps obligatoris i la seva longitud depèn del tipus de *chunk*.
- **Camps opcionals (*Optional Fields*, OF)**. El nombre de camps opcionals és variable.

Un cop descrita l'estructura dels segments TCP i de les PDU d'SCTP, passem a descriure com el nou protocol de transport fa front a les necessitats de la senyalització SS7. Per a fer-ho, descriurem a continuació els problemes que presenta TCP i la solució que presenta la proposta d'SCTP.

Terminologia

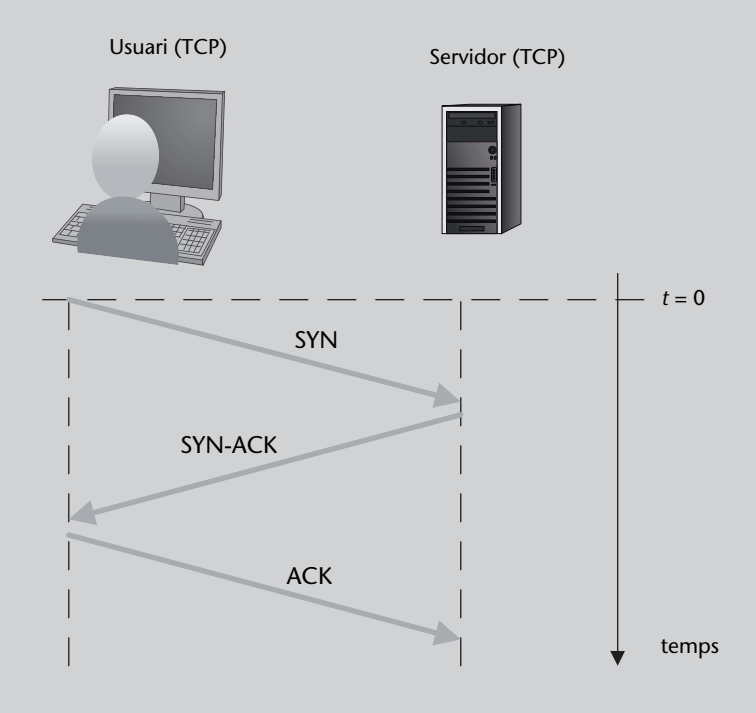
La nomenclatura utilitzada per l'SCTP varia lleugerament respecte de la utilitzada pel TCP. Mentre que la relació establerta entre dos *endpoints* TCP s'anomena **connexió**, els dos *endpoints* SCTP estableixen una **associació**.

2.1.1. Protecció contra atacs

El protocol TCP és vulnerable a l'atac anomenat *Denial of Service* (DoS). Per a entendre aquest atac cal tenir present quin és el procediment d'establiment d'una connexió TCP. La connexió entre dos nodes TCP es fa mitjançant l'anomenat *three-way handshake*. Aquest procediment consisteix, com mostra la figura 5, en el procés següent:

1) Inicialment el node que inicia l'establiment de la connexió transmet un segment amb un dels bits del camp de *flags* igual a 1. Aquest bit és el que anomenem bit de *synchronize* o d'inici de connexió i s'acostuma a denominar amb SYN. Un altre dels bits del camp de *flags*, el bit d'*acknowledgement* (ACK),

Figura 5. Establiment d'una connexió TCP



es col·loca a 0. Malgrat que durant aquest procés d'establiment es poden negociar diversos paràmetres de la connexió, els camps que cal incloure obligatòriament són el port de destinació (que és conegut), el port d'origen (que és seleccionat pel transmissor) i el número de seqüència. Com que es tracta del primer segment de la connexió, el valor es pot escollir aleatòriament.

2) En rebre el segment SYN, el receptor respon amb un segment amb els bits del camp de *flags* de *synchronize* i d'*acknowledgement* (SYN+ACK) iguals a 1. Pel que fa al número de seqüència, s'utilitza un número aleatori seleccionat pel receptor. Com que l'objectiu d'aquest segment és confirmar la correcta recepció del segment previ, el camp *acknowledgement number* ha de ser igual al número de seqüència del missatge SYN més 1*.

*** El valor de l'*acknowledgement number* sempre ha de ser igual al valor del primer segment que encara no ha estat confirmat. És per aquest motiu que se suma 1 al valor del número de seqüència del segment que es vol confirmar.**

3) Un cop rebut el segment (SYN+ACK), el transmissor respon amb un segment de confirmació (*acknowledgement*, ACK). El número de notificació que cal enviar en aquesta ocasió és igual al número de seqüència enviat pel receptor en el segment (SYN+ACK) més 1.

El node receptor (aquell que no inicia l'establiment) pot patir un atac DoS si rep una gran quantitat de segments SYN i, posteriorment, després de respondre'ls amb un segment (SYN+ACK) per a cada segment rebut, no rep el segment ACK que finalitzi el procés d'establiment. Amb un nombre suficientment gran d'intents d'establiment sense finalitzar, el node receptor pot tenir problemes de memòria.

El protocol SCTP soluciona aquest problema mitjançant un mecanisme d'establiment d'associació en quatre etapes (*four-way handshake*), sovint també conegut com a *cookie mechanism*.

L'establiment d'associació d'SCTP segueix els passos següents (figura 6):

1) L'SCTP que inicia l'establiment envia una PDU amb el camp *Chunk Type* igual a INIT*****. El camp *verification tag* permet identificar la identitat dels altres nodes. Abans d'enviar la PDU, el transmissor entra en un estat anomenat *cookie wait*. Aquest estat es manté durant un temps màxim. En cas de no haver rebut una resposta amb la *cookie*, el transmissor abandona aquest estat i l'establiment d'associació queda avortat.

*** Les PDU que continguin un *chunk* igual a INIT o INIT ACK només poden tenir aquest *chunk*. No és possible utilitzar una mateixa PDU per a transmetre un INIT o INIT ACK amb qualsevol altre *chunk*.**

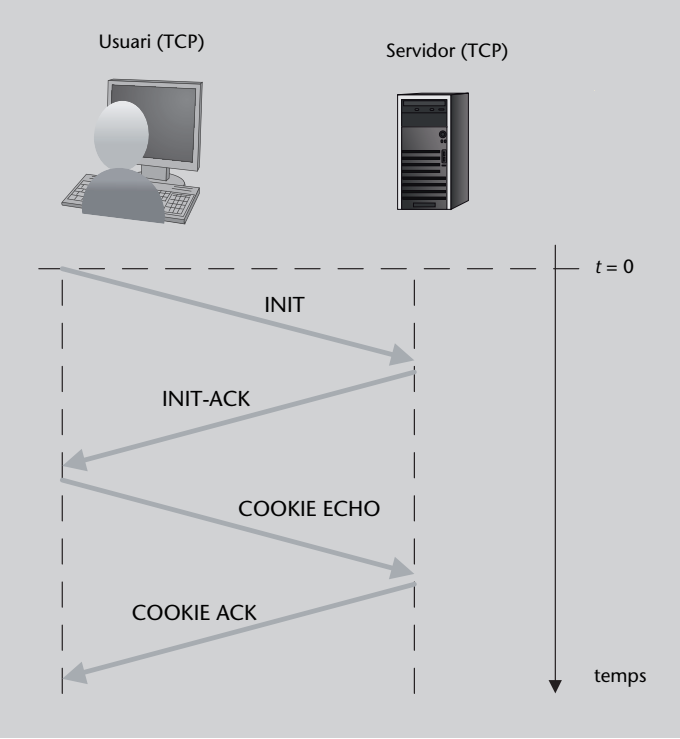
2) El receptor, en rebre la PDU d'inici d'associació, respon amb una PDU de notificació d'inici d'associació correcta (amb un *chunk type* igual a INIT ACK*****). El receptor cal que inclogui a la PDU el paràmetre anomenat *state cookie*******.

**** Podeu trobar la descripció de com es genera la *state cookie* a l'RFC 4960 de la IETF.**

3) La recepció per part del transmissor de la *state cookie* fa que abandoni l'estat *cookie wait*. En aquest instant, el transmissor envia cap al receptor una PDU amb un *chunk type* igual a COOKIE ECHO i que conté el *cookie state* rebut. Seguidament entra a l'estat anomenat *cookie echoed* i inicialitza el temps màxim que l'*endpoint* pot romandre en aquest estat.

4) El receptor, finalment, passa a l'estat *established* i transmet la darrera PDU de l'establiment: una PDU amb un *chunk type* igual a COOKIE ACK. El transmissor, en rebre aquesta PDU també passa a l'estat *established* i l'associació es dóna per establerta.

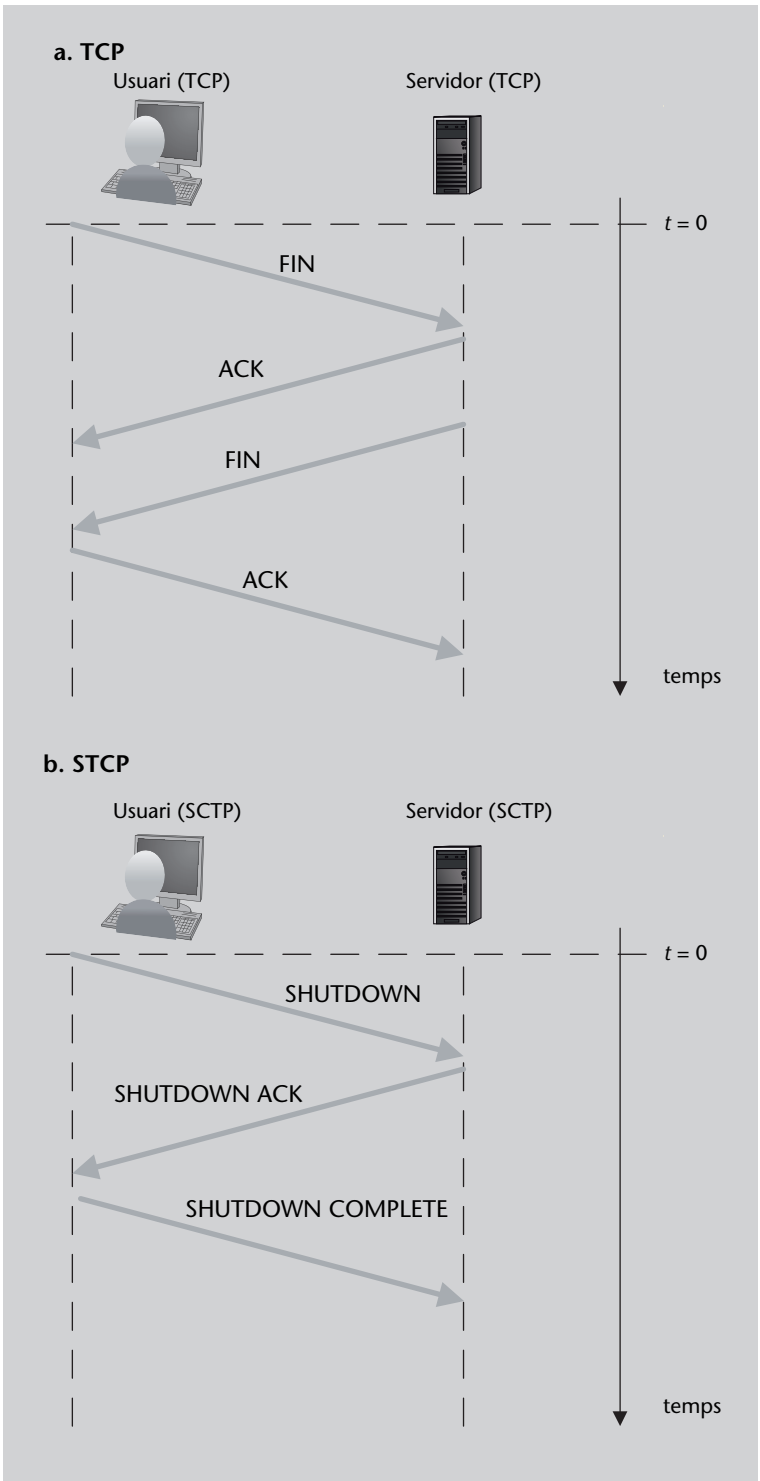
Figura 6. Establiment d'una associació SCTP



Tal com s'ha pogut comprovar, gràcies a l'existència de temporitzadors i d'un establiment d'associació estructurat en quatre fases, el protocol SCTP és capaç de fer front als atacs DoS.

L'intercanvi de dades segueix el mateix procediment (amb lleugeres diferències, ja que la notificació de recepció en SCTP es fa mitjançant un *chunk* igual a *selective acknowledgement*, SACK) tant per a TCP com per a SCTP, però la finalització presenta certes diferències. La diferència bàsica és que al protocol TCP cadascun dels *endpoints* allibera la connexió enviant un segment de *Finalize* (FIN) i rebent un segment d'*acknowledgement* (ACK), com mostra la figura 7 (a). En canvi, el protocol SCTP fa un alliberament de l'associació mitjançant un procediment en tres etapes, tal com mostra la figura 7 (b).

Figura 7. Alliberament d'una (a) connexió TCP i d'una (b) associació SCTP



L'alliberament de l'associació SCTP en tres fases assegura que l'associació queda definitivament tancada. En el cas de TCP, en canvi, com que la finalització s'ha de fer des dels dos extrems de la connexió, si un dels extrems no transmet el segment FIN, es diu que la connexió queda mig tancada (en anglès, *half closed connection*).

2.1.2. Transmissió fiable

La transmissió fiable de la informació (en aquest cas, i per a aquesta aplicació en concret, la senyalització SS7) fa referència tant a la detecció d'errors i la posterior retransmissió de la informació errònia, com al lliurament ordenat de les PDU.

Tal com ja s'ha fet notar, el control de flux i de congestió d'SCTP està completament basat en els mateixos mecanismes definits per al protocol TCP. Aquest fet garanteix que l'SCTP ofereixi un transport d'informació fiable.

2.1.3. Redundància

La redundància, en el context en el qual ens trobem, es pot definir com la capacitat d'una xarxa de tenir camins alternatius a través dels quals encaminar els paquets IP en cas de fallada d'algun dels camins. Si recordem l'estructura de la xarxa SS7, un dels punts clau és aconseguir redundància. Per a aconseguir-ho, la xarxa SS7 duplica tant els nodes (per exemple, les parelles d'STP) com els enllaços.

L'objectiu, doncs, del protocol SCTP és aconseguir redundància entre dos *endpoints* SCTP, i ho aconsegueix incorporant una de les característiques més destacades respecte al protocol TCP: **el *multi-homing*.**

Per a entendre el concepte del *multi-homing* convé recordar que l'adreça de transport de TCP és el resultat d'una adreça de xarxa (en aquest cas una adreça IP) i un port. Per tant, una connexió TCP s'estableix entre una adreça IP més un port, i una altra adreça IP més un port. En el moment en el qual una de les adreces IP esdevé inaccessible, la connexió no és possible. **No hi ha redundància**.

Per tal de fer front a la manca de redundància del protocol de transport TCP, el protocol SCTP defineix el *multi-homing*. En aquest protocol de transport, l'adreça de transport de cadascun dels *hosts* s'expressa com un conjunt d'adreces IP i un únic port. Així doncs, un *host/endpoint* SCTP es pot adreçar mitjançant un únic port però mitjançant diverses adreces IP (tantes adreces IP com interfícies tingui el node).

Malgrat el fet de poder establir una associació SCTP a través de diverses adreces IP, una de les adreces IP és considerada la principal/primària, i la resta són considerades adreces alternatives. És en cas que l'adreça IP principal sigui inaccessible que s'utilitzen les adreces alternatives. Les adreces alternatives també són utilitzades per a les retransmissions en cas d'error.

Tot i que es podria pensar que el *multi-homing* permet distribuir el trànsit entre les diverses interfícies del node SCTP, tal com succeeix amb el mecanisme basat en l'SLS definit a la capa MTP3, el *multi-homing* ha estat definit amb l'únic propòsit d'aconseguir tenir redundància, i no pas per a distribuir la càrrega de trànsit.

Els dos nodes d'una associació SCTP intercanvien la llista d'adreces IP alternatives de cadascun durant el procés d'establiment.

El funcionament correcte del *multi-homing* requereix la detecció de les fallades. Hi ha dos tipus de fallades possibles: o bé que l'*endpoint* sigui inaccessible (fallada de la xarxa), o bé que l'*endpoint* falli. En qualsevol dels dos casos l'efecte és el mateix per al mecanisme de *multi-homing*, i per tant, és necessari que l'SCTP estableixi un mecanisme de monitoratge de les adreces de l'associació. Aquest mecanisme rep el nom de *heartbeat mechanism*.

El mecanisme de *heartbeat* consisteix a enviar PDU amb un *chunk type* igual a HEARTBEAT cap a aquelles adreces que han restat inactives* durant un cert període. Un cop transmès un HEARTBEAT, el transmissor estableix un temps màxim per a rebre una notificació des de l'altre extrem de l'associació (HEARTBEAT ACK). En cas de no rebre la notificació de recepció, l'SCTP considera que l'adreça en qüestió és inaccessible.

*** Una adreça es considera inactiva si no es reben o bé dades o bé un *heartbeat* durant un període determinat.**

Malgrat considerar que una adreça és inaccessible, SCTP continua enviant periòdicament *chunks* HEARTBEAT per tal de detectar si, en algun moment, l'adreça torna a ser accessible.

2.1.4. Baix retard

La senyalització SS7 és molt sensible al retard. És per aquest motiu que el protocol de transport definit per SIGTRAN, l'SCTP, ha de garantir retards baixos. El protocol TCP presenta un problema denominat *head-of-line blocking**. Quan un segment TCP no es rep correctament, la recepció de qualsevol segment transmès posteriorment no es pot notificar fins que el segment perdut/erroni no es retransmet. Malgrat que aquesta situació no és un problema per a moltes aplicacions, en el cas de la senyalització pot causar retards superiors als seus restrictius límits de retard.

*** El terme anglès *head-of-line blocking* podria ser traduït com a *bloqueig del primer de la fila.***

SCTP fa front a aquest problema definint *streams* (o fluxos). El nombre de fluxos és determinat durant l'establiment de l'associació i es manté durant el

temps que es perllongui a aquesta associació. A cadascun dels fluxos se li assigna un identificador (*Stream Identifier*, SI), i per tant, tots els *chunks* transmesos contenen l'identificador de flux i un número de seqüència de flux (*Stream Sequence Number*, SSN), i això fa que el lliurament ordenat de *chunks* es faci a nivell de flux. Per exemple, quan un *chunk* és rebut amb errors, només la informació que pertany al mateix flux que la informació perduda/errònia pateix un retard addicional pel fet d'haver d'esperar la seva retransmissió. Així doncs, SCTP només garanteix el lliurament ordenat dins de cada flux, però no entre fluxos.

Aquest mecanisme s'anomena multi-streaming i redueix el retard global de l'associació, ja que el retard degut a les retransmissions només afecta aquells fluxos en els quals hi ha hagut errors, però no tota la informació, com succeeix a les connexions TCP.

2.1.5. Resum de les característiques de l'SCTP

Les principals característiques del protocol SCTP, algunes de les quals són comunes a TCP, són les següents:

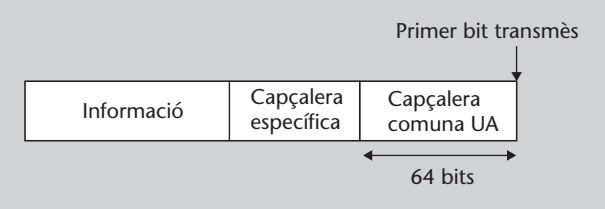
- **Conserva l'estructura dels missatges de capes superiors**. SCTP permet la segmentació de les dades de capes superiors i, per tant, un missatge es pot segmentar en diverses PDU o bé diversos missatges es poden incloure en diferents *chunks* d'una única PDU.
- **Evita el problema de l'anomenat bloqueig *head-of-line***. Aquesta és una característica bàsica perquè el protocol SCTP pugui ser el protocol de transport per a la senyalització SS7.
- **Diferents modes de lliurament de la informació**. Malgrat que en el cas de la senyalització estem interessats en un lliurament seqüencial i ordenat de la informació (com a TCP), el protocol SCTP també pot implementar modes similars a UDP.
- **Multi-homing**. Tal com s'ha explicat, SCTP permet redireccionar les PDU cap a adreces IP alternatives quan l'adreça principal falla.
- **Control de flux com el de TCP**. L'SCTP implementa mecanismes de control de flux basats en TCP, com per exemple *slow-start* i *congestion avoidance*.
- **Notificació de recepció correcta**. Tal com fa TCP, es notifica la recepció correcta de les PDU mitjançant un *chunk* anomenat *Selective acknowledgement* (SACK).
- **Mecanisme *heartbeat***. Gràcies a aquest mecanisme, el protocol SCTP és capaç de detectar la fallada d'una adreça IP.
- **Ofereix protecció contra l'atac DoS**. Gràcies al *cookie mechanism* és possible evitar aquesta mena d'atacs.

2.2. *User Adaptation Layers* (UA)

Les capes d'adaptació d'usuari tenen, en el context de SIGTRAN, la funció d'adaptar la senyalització provinent d'algun dels nivells de l'SS7 i la transmissió de paquets en una xarxa IP. Un cop definit el protocol de transport que compleix amb els requisits exigibles en termes de fiabilitat, redundància i de retard, les diverses UA acomoden la informació en format SS7 al format imposat per l'SCTP.

La informació SS7 és encapsulada/desencapsulada en el missatge propi de cadascuna de les capes d'adaptació específiques. El format dels missatges d'aquestes capes d'adaptació segueix un mateix format genèric (figura 8). Així, com es pot veure, en primer lloc hi ha una capçalera comuna, seguida d'una capçalera particular per a cada capa d'adaptació, i finalment la informació.

Figura 8. Format general d'un missatge de les capes UA



Quant a la capçalera comuna, aquesta consta d'un camp de versió del protocol, 8 bits no utilitzats, el camp de la classe del missatge, el tipus de missatge, i, finalment, la longitud de tot el missatge.

- **Versió del protocol**. Especifica la versió del protocol de la capa d'adaptació que s'executa al node que genera el missatge (8 bits).

- **Camp no utilitzat**. Té una longitud de 8 bits i es reserva per a possibles extensions dels protocols en el futur (8 bits).

- **Classe**. Aquest camp especifica quin dels protocols d'adaptació d'usuari (M2UA, M2PA, M3UA, etc.) ha generat el missatge (8 bits).

- **Tipus de missatge**. Dins de cada classe de missatge, la IETF defineix un conjunt de tipus de missatge, com per exemple els missatges d'establiment, de finalització, de dades, etc. (8 bits).

- **Longitud del missatge**. Conté la longitud total del missatge (dades més capçaleres) expressada en octets/bytes (32 bits).

Tal com es veurà a continuació, els missatges de mida variable emprats a totes les capes d'adaptació tenen la mateixa estructura: una etiqueta de 16 bits, un camp de longitud de 16 bits, i per acabar el valor del paràmetre, que té una longitud variable.

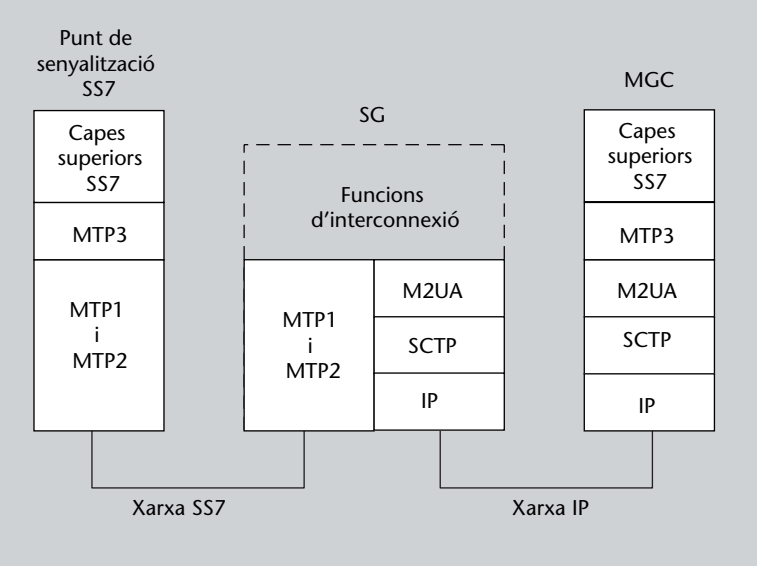
2.2.1. *MTP2-User Adaptation* (M2UA)

M2UA

La capa M2UA està descrita a l'RFC 3331 de la IETF.

Tal com s'ha explicat fins ara, la interconnexió de les xarxes de commutació de circuits i de les xarxes IP requereix, en termes de senyalització, la inclusió d'un node intermedi anomenat *Service Gateway* (SG). Aquest node, l'SG, té, per una banda, una connexió a la xarxa SS7 a través de les capes MTP1 i MTP2. Per l'altra, una connexió a la xarxa IP a través d'SCTP/IP. L'esquema de la figura 9 mostra la situació descrita a l'RFC 3331 per a l'ús de l'M2UA.

Figura 9. Arquitectura de referència per a M2UA



Font: RFC 3331. SS7 MTP2 User Adaptation Layer.

En aquesta arquitectura hi ha un seguit d'aspectes que tenen especial rellevància:

- El codi de punt, adreça mitjançant la qual s'encaminen els missatges a través de la xarxa SS7, és necessari per a tots aquells nodes que implementen la capa MTP3. Com es pot veure a la figura, l'SG no implementa la capa MTP3 i, per tant, no té un codi de punt (sí que té una adreça IP a la xarxa IP). Pel que fa a l'MGC, en canvi, sí que disposa tant d'adreça IP com de codi de punt, ja que estableix una associació amb l'SG mitjançant SCTP/IP i una connexió amb el punt de senyalització SS7 a la capa MTP3.
- Per a la capa MTP3 de l'MGC i del punt de senyalització SS7, l'SG és transparent.

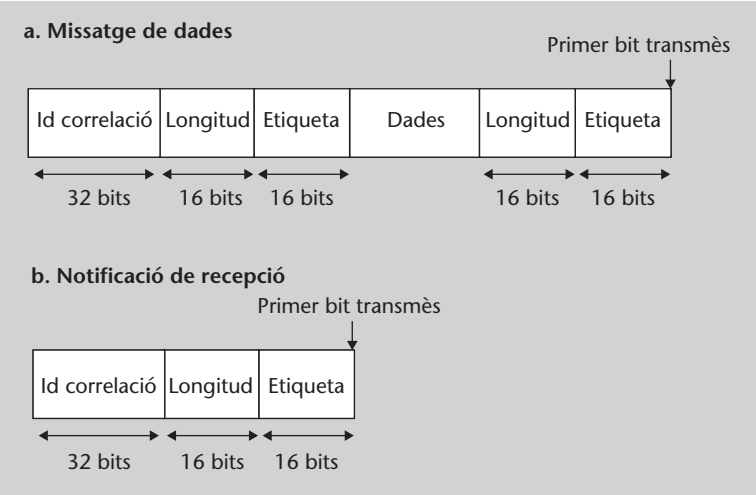
Els missatges utilitzats pel protocol M2UA tenen el format descrit a la figura 8, i per tant contenen una capçalera genèrica, una capçalera específica de l'M2UA i les dades per transmetre. Pel que fa a la capçalera específica, consta de tres camps: l'etiqueta o *tag* (16 bits), la longitud (16 bits), i l'identificador d'interfície.

- **Etiqueta**. Indica quina informació transporta el missatge; és dir, si conté dades, una notificació (ACK), una petició d'establiment, una sol·licitud, etc.

- **Longitud**. Per tal de preservar l'estructura general dels paràmetres, la capçalera inclou el camp de longitud. Malgrat això, no desenvolupa cap funció específica i el seu valor sempre és igual a 8.
- **Identificador d'interfície**. Les xarxes IP poden tenir capes física i d'enllaç diverses. Aquest camp descriu quina és la interfície a la qual està connectat el node.

Els missatges, a més de les capçaleres comuna i específica, inclouen el camp d'informació. En el cas de l'M2UA, el camp d'informació pot contenir dades, notificacions de recepció de dades, peticions i confirmacions d'establiment, peticions i confirmacions d'alliberament, notificacions d'estat i de congestió, etc. En general els missatges transportats al camp d'informació mantenen l'estructura d'etiqueta, longitud i valor. Tot i així, convé destacar el format i el funcionament de l'intercanvi de dades (figura 10).

Figura 10. Format de la part d'informació dels missatges utilitzats per l'M2UA en l'intercanvi de dades



Quan les capes M2UA de dos nodes s'intercanvien dades, és necessari que hi hagi una confirmació de recepció. Per a fer-ho, l'estructura del missatge de dades és la que mostra la figura 10 (a). El primer dels paràmetres és el que conté les dades. Així, el primer camp d'etiqueta i de longitud permet que la capa M2UA reconegui les dades i la seva longitud. Aquestes dades, però, van acompanyades d'un segon paràmetre (també amb l'estructura etiqueta-longitud*-valor): l'identificador de correlació. Aquest paràmetre permet que la notificació de recepció del missatge es dugui a terme. El receptor, en rebre el missatge de dades, respon amb un missatge de notificació com el de la figura 10 (b), amb el mateix identificador de correlació.

*** El camp de longitud associat a l'identificador de correlació pren sempre un valor igual a 8 perquè la longitud del camp és coneguda a priori.**

És important fer notar que la recepció correcta dels missatges de dades de l'M2UA ha de ser notificada perquè, en cas de no fer-ho, per a l'enllaç SS7 equivaldria a la manca de notificació de les MSU transmeses.

2.2.2. *MTP2-user Peer-to-peer Adaptation* (M2PA)

M2PA

La capa M2PA està descrita a l'RFC 4165 de la IETF.

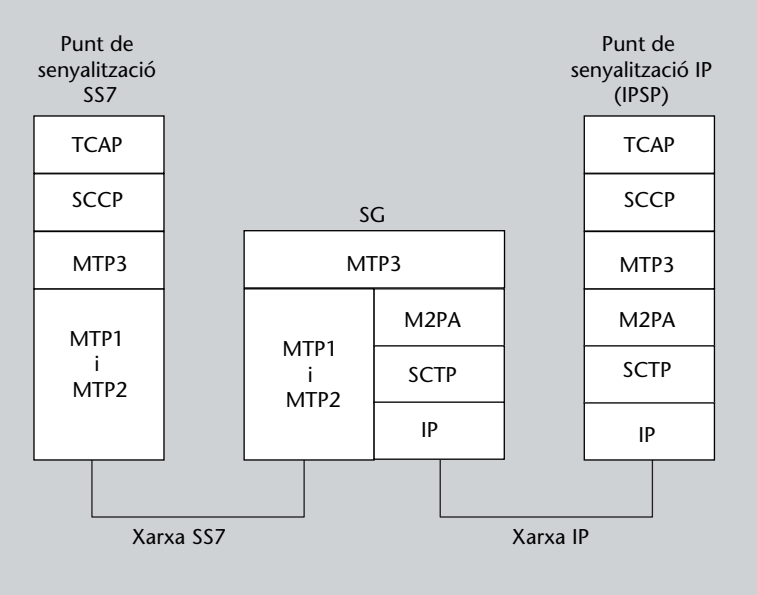
L'objectiu principal de la capa M2PA és aconseguir una veritable convergència entre les xarxes de senyalització SS7 i les xarxes IP. Per a fer-ho és necessari que els punts de senyalització, sigui quina sigui la xarxa a la qual es troben connectats, puguin comunicar-se entre ells de manera transparent.

IPSP

Els punts de senyalització IP (denominats com a *IP Signalling Point*, IPSP) són punts de senyalització connectats a la xarxa IP que implementen les capes altes de l'SS7, a partir de l'MTP3.

L'RFC 4165, que defineix aquesta capa d'adaptació d'usuari, proposa dues arquitectures en les quals es pot utilitzar l'M2PA (figura 11 i figura 12). La primera de les arquitectures és la connexió de dos punts de senyalització, l'un connectat a la xarxa SS7 i l'altre connectat a la xarxa IP (figura 11). De la mateixa manera que succeix a l'M2UA, l'intercanvi de senyalització es realitza a través d'un SG, però aquesta vegada l'SG implementa la capa MTP3. Per tant, en aquesta arquitectura l'SG sí que té una adreça IP i un Codi de Punt SS7.

Figura 11. Primera arquitectura de referència per a M2PA

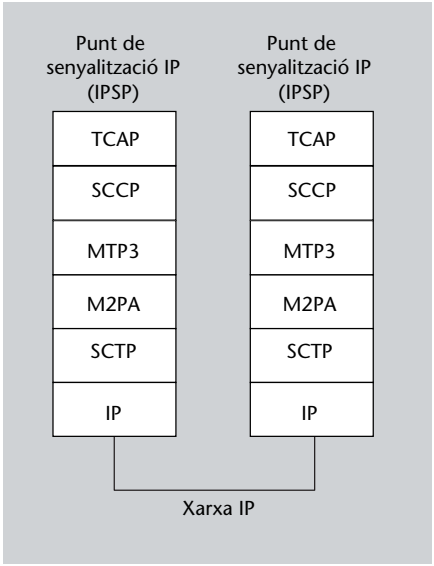


Font: RFC 4165. SS7 MTP2 User Peer-to-Peer Adaptation Layer.

Des del punt de vista del punt de senyalització SS7, l'SG és vist com un punt de senyalització STP. Gràcies a l'M2PA i la primera arquitectura presentada, és possible que els punts de senyalització de la xarxa SS7 puguin accedir a nodes de la xarxa IP (com, per exemple, bases de dades) i que els nodes de la xarxa IP puguin utilitzar els serveis oferts per la xarxa SS7.

La segona arquitectura especificada a l'RFC 4165 és la que es mostra a la figura 12. Es tracta, tal com es pot observar, d'una situació de convergència de les dues xarxes, en les quals els punts de senyalització SS7 poden estar connectats directament a la xarxa IP.

Figura 12. Segona arquitectura de referència per a M2PA



Font: RFC 4165. SS7 MTP2 User Peer-to-Peer Adaptation Layer.

Les arquitectures proposades per a l'M2PA permeten observar que a tots els punts de senyalització hi ha, per sobre de l'M2PA, la capa MTP3. Per tant, l'M2PA ha de ser vista per l'MTP3 de la mateixa manera que seria vista l'MTP2 (l'intercanvi de missatges entre MTP3 i M2PA ha de ser el mateix que l'intercanvi de missatges entre MTP3 i MTP2). Si recordem el funcionament de la capa MTP de l'estàndard SS7, MTP2 transmet/rep tres tipus d'unitats de senyalització: les MSU, les LSSU i les FISU. Dels tres tipus d'unitats de senyalització només les MSU són generades per la capa MTP3. Així doncs, les capes MTP3 i M2PA intercanvien MSU.

Els altres dos tipus d'unitats de senyalització són intercanviats entre les capes MTP2 dels dos punts de senyalització però no són transferits cap a la capa MTP3. Pel que fa a les LSSU, l'estàndard SS7 les utilitza per a intercanviar informació de l'estat de l'enllaç. Per tant, malgrat que la capa M2PA no transmet/rep LSSU, sí que defineix missatges amb una funció anàloga (intercanvi d'informació d'estat).

El cas de les FISU és diferent. A la capa MTP2 aquestes unitats de senyalització són transmeses sempre que no hi ha MSU i/o LSSU disponibles. Aquesta funció, que té sentit en la xarxa SS7, no té sentit en una xarxa IP. Per tant, la capa M2PA no defineix cap missatge que faci aquesta funció.

Les capes M2UA i M2PA poden semblar similars, però presenten diferències importants. Les semblances principals entre totes dues capes són les següents:

Semblances:

- Totes dues capes transporten missatges amb dades de l'MTP3.
- Totes dues capes tenen la capa MTP3 per sobre i l'SCTP per sota.

Diferències:

- Quan hi ha la capa M2PA, la connexió establerta entre l'SG i el punt de senyalització IP és una connexió SS7*. En canvi, amb la capa M2UA no s'estableix una connexió SS7 entre l'SG i l'MGC. De fet, en aquest darrer cas, l'SG és transparent a la connexió SS7.

- L'SG amb l'M2PA també implementa l'MTP3, mentre que amb l'M2UA no. Com a conseqüència d'aquest fet, l'SG té assignat un codi de punt en el primer cas i no en té en el segon cas.

- La capa M2PA no defineix funcions de gestió de la xarxa, ja que confia aquestes funcions a la capa MTP3. L'M2UA, en canvi, defineix funcions de gestió*.

- La capa M2UA sempre té la capa MTP3 per sobre, mentre que no succeeix el mateix en el cas de l'M2UA*.

*** Recordem que un node amb l'M2UA, com per exemple un SG, no necessàriament té la capa MTP3 per sobre.**

El format dels missatges M2PA segueix l'estructura de tots els missatges de les capes UA: capçalera comuna, capçalera específica per a M2PA, i camp d'informació. Ja s'ha explicat que l'M2PA du a terme les funcions de l'MTP2 i que per sobre sempre hi té l'MTP3. Per tant, la capçalera específica està molt relacionada amb les unitats de senyalització que a l'estàndard SS7 transmet/rep l'MTP2. En concret, la capçalera específica consta dels camps següents (ordenats):

- **Buit**. Camp de 8 bits de longitud reservat per a futurs usos.
- ***Backward Sequence Number* (BSN)**. Camp que conté el BSN, que, a l'estàndard SS7, incorpora la capçalera de les unitats de senyalització (24 bits). El valor d'aquest camp s'extreu de la capçalera de la unitat de senyalització.
- **Buit**. Camp de 8 bits de longitud reservat per a usos futurs.
- ***Forward Sequence Number* (FSN)**. Camp que conté l'FSN que, a l'estàndard SS7, incorpora la capçalera de les unitats de senyalització (24 bits). El valor d'aquest camp s'extreu de la capçalera de la unitat de senyalització.

Els missatges de l'M2PA, tal com ja s'ha apuntat anteriorment, poden ser de dos tipus: de dades o d'estat. El camp d'informació dels missatges de dades és, directament, els missatges generats per l'MTP3. Es tracta simplement d'encapsular la informació generada a l'MTP3 tal com ho faria la capa MTP2 però en un format diferent.

El protocol M2PA defineix dos tipus de missatges relacionats amb l'estat de l'enllaç: el missatge de prova d'estat (*Link Status Proving*) i el missatge d'estat (*Link Status*). La funció que tenen aquests missatges és anàloga a la que fan les LSSU; és a dir, comprovar l'estat de l'enllaç i comunicar-ne el resultat. En tots dos casos, el camp d'informació conté exclusivament l'estat de l'enllaç, que pot prendre valors com *Alignment*, *Proving Normal*, *Proving Emergency*, *Ready*, *Processor Outage*, *Processor Recovered*, *Busy*, *Busy Ended* o *Out of Service*.

2.2.3. *MTP3-User Adaptation* (M3UA)

M3UA

La capa M3UA està descrita a l'RFC 4666 de la IETF.

La capa M3UA és anàloga a l'M2UA, però en aquest cas té la funció de donar servei als usuaris MTP3; és a dir, té la funció de fer l'adaptació entre l'SCCP i el protocol de transport de la xarxa IP, l'SCTP.

El protocol M3UA està definit per a utilitzar-lo en tres situacions diferents:

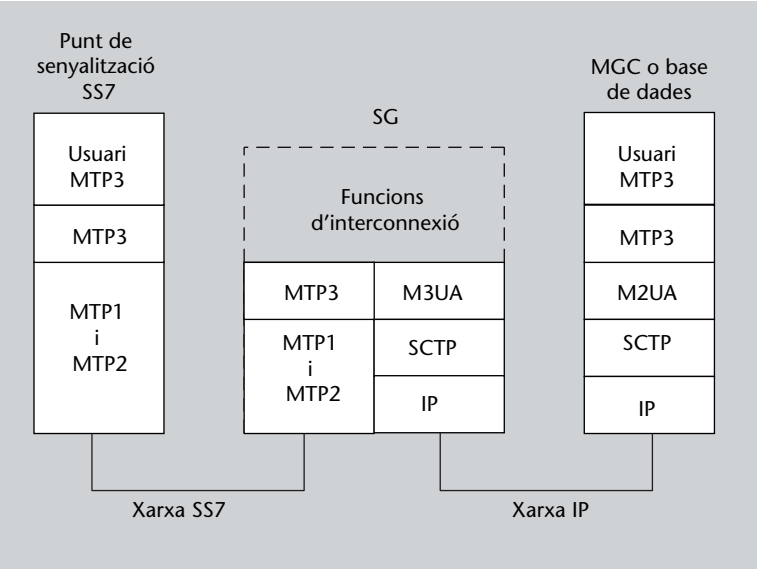
1) Entre un SG i l'MGC per a comunicar els usuaris MTP3 d'un punt de senyalització de la xarxa SS7 i d'un MGC de la xarxa IP.

2) Permetre l'accés d'un punt de senyalització SS7 a una base de dades (a través d'un SG) connectada a una xarxa IP.

3) Entre dues aplicacions IP, els nodes de les quals es troben connectats a la xarxa IP.

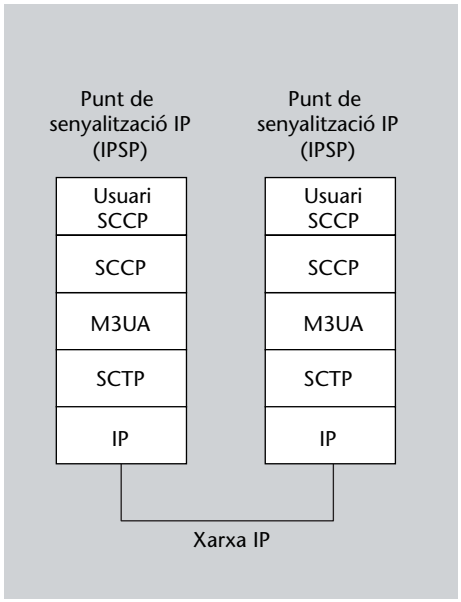
Aquestes tres situacions es mostren a les figures 13, 14 i 15. Totes tres situacions són anàlogues a les situacions mostrades per als protocols M2UA i M2PA; per tant, no les descriurem en detall. La més interessant de les tres arquitectures proposades a l'RFC 4666, però, és la que mostra la figura 15. Les arquitectures de la figura 13 i de la figura 15 són molt semblants i només es diferencien en l'SG. A la primera (figura 13), l'SG no té cap instància de les capes superiors a MTP3, mentre que a la segona (figura 15) hi ha una instància SCCP. Aquesta darrera situació, que és molt concreta, ha estat definida perquè l'SG pot dur a terme la traducció de títol global que defineix l'SS7 (*Global Title Translation*, GTT).

Figura 13. Primera arquitectura de referència per a M3UA



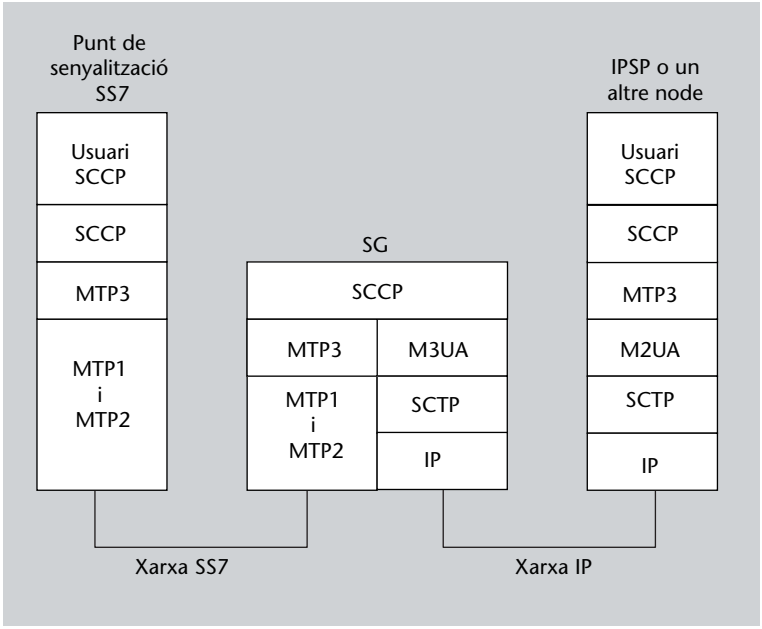
Font: RFC 4666. SS7 MTP3 User Adaptation Layer.

Figura 14. Segona arquitectura de referència per a M3UA



Font: RFC 4666. SS7 MTP3 User Adaptation Layer.

Figura 15. Tercera arquitectura de referència per a M3UA



Font: RFC 4666. SS7 MTP3 User Adaptation Layer.

A la xarxa SS7, la capa MTP3 té la responsabilitat d'encaminar els missatges de senyalització en funció de l'estat dels enllaços i de l'estat dels punts de senyalització distants. En el context de SIGTRAN, la capa M3UA ha de dur a terme les mateixes funcions. Aquest protocol per una banda defineix funcions de gestió natives (independents de la capa MTP3) i per l'altra defineix funcions que permeten adaptar les funcions desenvolupades per l'MTP3 a la xarxa IP.

Fixem-nos en la figura 14. En aquesta situació les funcions de gestió de l'M3UA, com per exemple notificar errors o encaminar els missatges, no estan relacionades amb la capa MTP3. En escenaris com aquest M3UA executa funcions de

gestió definides específicament per a aquest protocol. Si, en canvi, observem la figura 15, les funcions de gestió de l'M3UA adapten les funcions definides per al protocol MTP3 de la ITU-T.

Els tipus de missatges de l'M3UA poden ser de diverses classes, però en essència podem dir que hi ha els missatges de transferència i els missatges de gestió (*SS7 Signalling Network Management*, *ASP state management*, etc). L'estructura dels missatges segueix la que hem vist per a les altres capes d'adaptació d'usuari però amb una diferència: **no hi ha una capçalera específica**. Així, el format dels missatges consta de la capçalera comuna i del camp d'informació (un conjunt de paràmetres amb l'estructura etiqueta-longitud-valor).

Pel que fa als missatges de transferència, els paràmetres que inclou són els següents:

- **Aparença de la xarxa**. Aquest paràmetre inclou el context de la xarxa SS7, la informació sobre l'usuari MTP3 i sobre el protocol MTP3, així com altres informacions d'interès (32 bits).

- **Context d'encaminament**. Descriu el context d'encaminament i les claus d'encaminament dels missatges (32 bits).

- **Dades del protocol**. El camp de dades del protocol té una longitud variable, i conté el missatge original de la capa MTP3. Per tant, a dins d'aquest camp s'hi poden trobar els camps que conté habitualment un missatge MTP3, com ara les adreces dels punts de senyalització d'origen i de destinació (OPC i DPC, el *Service Indicator* (SI), el *Signalling Link Selector* (SLS), el *Network Indicator* (NI), el *Message Priority* (MP) i les dades.

- **Identificador de correlació**. Camp que identifica l'MSU transportada al camp de dades del protocol (32 bits).

La resta de missatges de l'M3UA són similars però amb alguns canvis. L'estructura és la mateixa que la dels missatges de transferència, però sense el camp de dades. En comptes del camp de dades inclouen una llista de punts de senyalització afectats per la situació que notifica el missatge (congestió, accessibilitat o inaccessibilitat, etc.) i, finalment, un camp d'informació addicional.

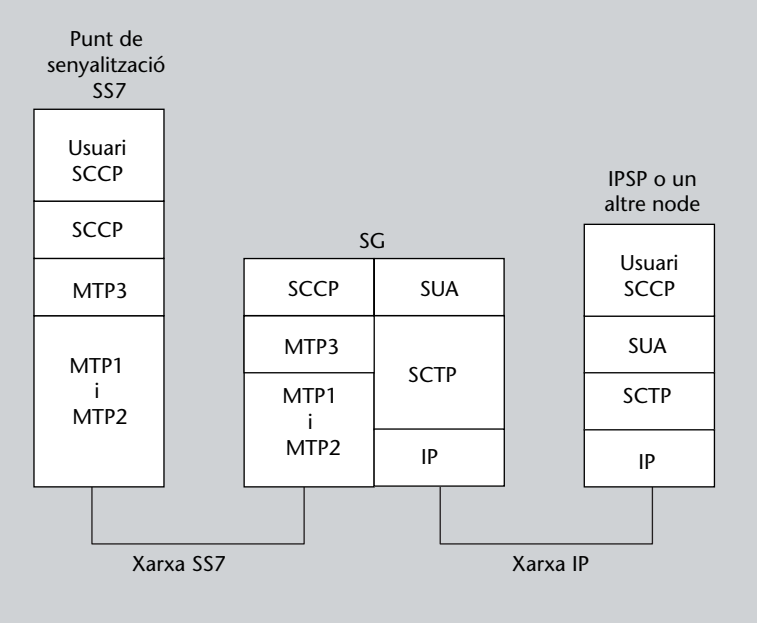
2.2.4. *SCCP User Adaptation* (SUA)

El darrer dels protocol d'adaptació d'usuari és el SUA. Es tracta d'una capa anàloga a l'M2UA i l'M3UA. La figura 16 i la figura 17 mostren les dues arquitectures proposades per la IETF. Totes dues són molt similars a les que hem vist fins ara.

SUA

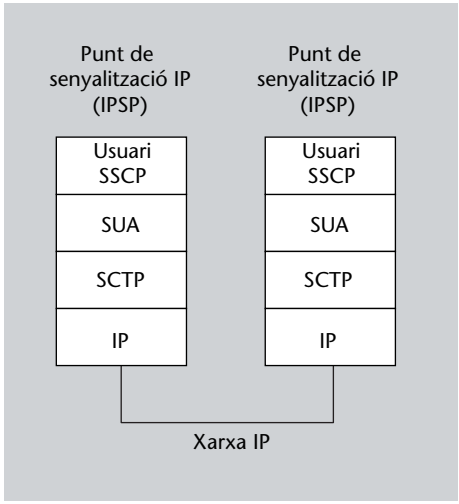
La capa SUA està descrita a l'RFC 3868 de la IETF.

Figura 16. Primera arquitectura de referència per a SUA



Font: RFC 3868. SS7 SCCP User Adaptation Layer.

Figura 17. Segona arquitectura de referència per a SUA



Font: RFC 3868. SS7 SCCP User Adaptation Layer.

Com que la definició és molt similar a la d'aquestes dues capes, no aprofundirem en els camps de cada missatge. Tot i així, cal destacar que, com succeeix a l'M3UA, els missatges inclouen la capçalera comuna però no hi ha capçalera específica per a aquest protocol.

Si ho recordem, la capa SCCP permet transferència de dades no orientada a connexió (classes 0 i 1) i transferència de dades orientada a connexió (classes 2 i 3). És per aquest motiu que el protocol SUA ha de suportar la transferència de dades per a qualsevol de les quatre classes.

3. El protocol *Session Initiation Protocol* (SIP)

Fins ara hem vist un conjunt de protocols que tenen l'objectiu d'aconseguir la interconnexió de la xarxa de senyalització SS7 i la xarxa IP. A partir d'ara ens centrarem en un protocol de senyalització definit per a la xarxa IP. Hi ha dos protocols que per les seves característiques són els més estesos: l'H.323 (ITU-T) i el *Session Initiation Protocol* (SIP).

El protocol H.323 fou el primer estàndard que donava solució a la veu sobre IP d'una manera adequada. Es tracta d'un protocol que desenvolupa la funció de paraigua agrupant altres fonts d'estandardització. La Recomanació de la ITU-T que el defineix fa referència a diversos estàndards, com ara els protocols per a serveis en temps real RTP i RTCP, o les Recomanacions H.225, Q.931 i H.245. Malgrat ser un estàndard complet que permet oferir millors funcionalitats, interoperabilitat i interconnexió que, per exemple, el protocol SIP, sovint la seva complexitat n'ha limitat el desplegament.

L'altra opció, el SIP, és un protocol simple i flexible que, malgrat no oferir les mateixes prestacions que l'H.323, permet establir senyalització entre nodes de la xarxa IP d'una manera senzilla i amb un baix cost. A més, gràcies a 3GPP i la introducció de l'arquitectura IMS a les xarxes troncals, el protocol SIP ha pres més importància. L'arquitectura IMS és una proposta per a les futures xarxes IP, i la seva definició està basada en el protocol de senyalització SIP.

És per aquest motiu i per la seva acceptació que en aquest mòdul ens centrarem en el protocol SIP i deixarem de banda l'H.323.

El *Session Initiation Protocol* (SIP) és un protocol de la capa d'aplicació que permet l'establiment, modificació i finalització d'una sessió en una xarxa IP de paquets.

Estandardització del SIP

A mitjan dècada dels 90, investigadors de la Columbia University van establir per primera vegada les bases del protocol SIP. La IETF es va fer càrrec de la seva estandardització i va crear l'RFC 2543, que posteriorment va ser substituïda per l'RFC 3261.

Es tracta d'un protocol creat i estandarditzat per la IETF i que, actualment, després d'una evolució històrica, ha quedat fixat en l'RFC 3261, si bé és cert que hi ha diverses RFC que amplien alguns aspectes del protocol.

El SIP no és per ell mateix un protocol que transporti informació multimèdia, sinó que es tracta d'un protocol que estableix i gestiona les sessions entre dos usuaris. Un cop establerta la sessió, la informació multimèdia és transportada mitjançant altres protocols de transport, com per exemple el popular

Real-Time Transport Protocol (RTP). És precisament aquesta flexibilitat –establir, mantenir i alliberar sessions genèriques sense imposar com es transporta la informació– la que l'ha fet esdevenir un protocol estès i popular per a serveis com la VoIP, l'*streaming* de vídeo o la missatgeria instantània en xarxes de paquets.

En general es podria dir que el protocol SIP presenta les característiques següents:

- És capaç de determinar la **localització de l'usuari** que participa en la comunicació a partir de paràmetres com, per exemple, l'adreça IP (o un número de telèfon).
- Permet que l'usuari estableixi, de manera prèvia a l'establiment d'una sessió, l'accessibilitat i la **disponibilitat*** d'un determinat usuari.

*** La disponibilitat d'un usuari la pot establir el mateix usuari.**

- **Estableix una sessió** entre dos usuaris. En cada sessió es poden establir els paràmetres que regiran aquella sessió.
- **Gestiona la sessió establerta**, i permet modificar els paràmetres de la sessió durant el seu transcurs o finalitzar-la.

Gràcies a aquestes característiques, que el converteixen en un estàndard molt obert i flexible per a gestionar les sessions de tota mena de serveis, el SIP ha esdevingut un dels més populars –si no el més popular– dels protocols de senyalització per a xarxes de paquets. De fet, la seva flexibilitat preveu, per exemple, que el protocol de transport utilitzat per a transportar els missatges de SIP sigui tant TCP com UDP, els dos protocols de transport més habituals en xarxes IP.

Fixem-nos que fins ara, en aquest mòdul, ens hem centrat en els protocols que conformen SIGTRAN. SIGTRAN és un conjunt de protocols amb l'objectiu d'assolir interoperabilitat entre les noves xarxes IP i les antigues, però molt esteses i utilitzades, xarxes commutades de telefonia (i XDSI). Ara, en canvi, presentem un protocol pensat explícitament per a usuaris connectats a una xarxa IP. Malgrat que dos usuaris poden establir i gestionar una sessió SIP sense la necessitat de nodes addicionals, a mesura que la dimensió i la complexitat de la xarxa creix el protocol SIP inclou nodes addicionals que intervenen de diferent manera en la sessió.

Per tal de definir quins són aquests nodes i, alhora, establir la nomenclatura utilitzada en el cotext del SIP, a continuació en fem una breu descripció:

- **L'usuari (*User Agent*, UA)**. Es tracta de l'usuari final d'una sessió SIP, tant l'usuari que inicia la sessió com l'usuari que la rep. Quan es parla dels usuaris es diferencia entre el que ha iniciat l'establiment de la sessió, que rep la denominació de *client*, i el que rep la petició d'establiment, que és denominat *server*.

Client i servidor

La denominació completa del client i el servidor és *User Agent Client* (UAC) i *User Agent Server* (UAS).

- **El servidor *proxy***. Aquest node dóna suport, en cas de ser requerit mitjançant l'enviament d'una petició, a la determinació de l'encaminament entre l'UAC i l'UAS. De la mateixa manera, pot desenvolupar tasques d'autenticació dels usuaris.

- **Servidor de reencaminament (*Redirect Server*)**. És un node amb la funció de respondre a la petició d'un usuari o d'un altre servidor lliurant un conjunt d'adreces. Com indica el seu nom, desenvolupa les seves funcions en el context del l'encaminament dels missatges SIP, però la seva única participació és aquesta: proveir el node que ha generat la petició amb les adreces requerides.

- **Servidor de registre (*Register Server*)**. Per motius de mobilitat que seran explicats més endavant, és necessari que els usuaris puguin registrar la seva posició en aquest servidor.

- **Servidor de localització (*Location Server*)**. La mobilitat dels usuaris és un dels reptes al qual s'enfronta qualsevol protocol de senyalització de xarxes IP. Aquest servidor és el que fa possible, gràcies a la seva interacció amb el servidor de registre, conèixer la localització dels diferents usuaris.

Tots aquest nodes descrits poden intervenir en l'establiment, gestió i finalització d'una sessió SIP, però no són necessaris si els dos usuaris (client i servidor) són capaços de comunicar-se directament.

3.1. Diàlegs, transaccions i missatges

Blocs bàsics de SIP

Missatges, transaccions i diàlegs són els blocs bàsics sobre els quals es fonamenta SIP.

El protocol SIP es basa en missatges, transaccions i diàlegs. Els missatges poden ser de dos tipus: Peticions (en anglès, *Request*) i Respostes (*Response*). Una transacció és el conjunt de missatges que inclouen una petició i una o diverses respostes. El diàleg, en canvi, es defineix com el conjunt de transaccions que intercanvien client i servidor entre l'establiment i alliberament de la sessió (ambdues transaccions –establiment i alliberament– incloses).

Per tal d'analitzar el funcionament dels diàlegs i com es pot establir, gestionar i alliberar una sessió, comencem analitzant el format dels missatges.

3.1.1. Format dels missatges

El protocol SIP es basa en conceptes molt similars al protocol HTTP, i el format del missatge n'és un bon exemple. Els missatges SIP són un conjunt de línies de text separades entre elles per un salt de línia. Malgrat que, tal com s'ha fet notar, hi ha dos tipus de missatges (peticions i respostes), el format dels missatges és independent del tipus de missatge i presenta un únic format:

1) Línia inicial.

2) Capçaleres.

3) Línia en blanc.

4) Cos del missatges.

La **línia inicial** del missatge presenta una estructura una mica diferent en funció de si es tracta d'una petició o d'una resposta. La forma general és la següent:

Method URI-Request SIP-Version **(Petició)**
SIP-Version Status-Code Reason-Phrase **(Resposta)**

En una petició SIP el mètode (*Method*) és el paràmetre que identifica el motiu de la petició. El nombre de mètodes de SIP és reduït i l'RFC 3261 en defineix sis: INVITE, ACK, OPTIONS, BYE, CANCEL i REGISTER. Posteriorment, el número de mètodes s'ha ampliat en diferents RFC incloent-hi els mètodes INFO (RFC 2976), MESSAGE (RFC 3428), NOTIFY (RFC 3265), PRACK (RFC 3263), REFER (RFC 3515), SUBSCRIBE (RFC 3265) i UPDATE (RFC 3311). A la taula 1 es defineixen els mètodes més importants inclosos a l'RFC 3261.

Taula 1. Mètodes dels missatges SIP

Mètode	Descripció
INVITE	Inicia la sessió
ACK	Notifica que la sessió s'ha establert correctament
OPTIONS	Permet sol·licitar informació de les capacitats de la destinació
BYE	Finalitza la sessió
CANCEL	Cancel·la una sessió oberta
REGISTER	Envia la informació perquè l'usuari sigui registrat al servidor de registre

El paràmetre *URI-Request* fa referència a l'adreça del node al qual s'envia la petició. Les adreces SIP poden tenir diferents formats. El més habitual és que tingui la forma **sip:usuari@domini**, tot i que també pot incloure-hi paràmetres com una contrasenya, el port, etc. A banda d'aquest format, l'adreça URI (*Uniform Resource Identifier*) també pot incloure el número de telèfon en comptes de l'adreça. En aquest cas, l'adreça presentaria una forma **sip:+telèfon@domini;user=phone**.

En qualsevol cas, l'URI pot anar precedit d'un descriptor entre cometes i presentar un aspecte com "**Descriptor**"**<sip:usuari@domini>**.

Exemple

Imaginem un usuari connectat al domini *uoc.edu*, amb nom d'usuari *consultor*. L'adreça URI de l'usuari seria sip:consultor@uoc.edu

Si, per a aquest mateix usuari, el port utilitzat per l'aplicació basada en el protocol SIP utilitzés el port de TCP 5060, aleshores l'adreça es podria escriure de la manera següent: sip:consultor@uoc.edu:5060

En cas que, per a accedir a la xarxa, l'usuari que genera la petició hagués de proporcionar una contrasenya, l'URI podria afegir-la: sip:consultor:contrasenya@uoc.edu:5060

Sí, en canvi, l'usuari tingués un número de telèfon +34933263535, aleshores l'URI podria tenir l'aspecte següent: sip:+34-933263535@uoc.edu;user=phone

Pel que fa al paràmetre *SIP-Version*, té l'unic objectiu de notificar al destinatari del missatge quina és la versió del protocol SIP que s'executa a l'origen.

Finalment, al missatge de petició hi apareixen els paràmetres *Status-Code* i *Reason-Phrase*. Tots dos paràmetres estan molt relacionats entre ells, ja que, malgrat que el primer és un camp numèric i el segon no, tots dos notifiquen el resultat de la petició. Cada valor de l'*Status-Code* es correspon amb un valor de *Reason-Phrase*. El codi d'estat és un enter de 3 dígits. El primer dels tres dígits designa la classe de resposta, i els dos darrers dígits en determinen la resposta concreta. Hi ha sis classes de respostes:

La descripció de totes les respostes possibles es pot trobar a la secció 21 de l'RFC 3261.

- **Provisional**: Tenen un *Code-Status* amb el primer dígit igual a 1 (1xx). Les respostes d'aquesta família indiquen al client que el servidor està duent a terme alguna tasca i que trigarà més de 200 ms. Per tal d'evitar retransmissions innecessàries, les respostes d'aquesta classe alerten al client que la resposta trigarà, però que està essent servida. Algunes de les respostes més importants que pertanyen a aquesta classe són *Code-Status*=100 i *Reason-Phrase=Trying* (la petició ha estat rebuda i s'està processant) o *Code-Status*=180 i *Reason-Phrase=Ringing* (el servidor ha estat alertat de la petició entrant).
- **Èxit**. Consta d'una única resposta per a indicar que la petició ha estat satisfactòria. La resposta és *Code-Status*=200 i *Reason-Phrase=OK*.
- **Redireccionament**. Tenen un *Code-Status* amb el primer dígit igual a 3 (3xx). Les respostes d'aquesta classe informen sobre la nova localització d'un usuari o dels nous serveis disponibles.
- **Petició errònia**. Tenen un *Code-Status* amb el primer dígit igual a 4 (4xx). Indiquen que la petició rebuda al servidor és errònia i, per tant, no pot ser reenviada sense modificacions.
- **Error del servidor**. Tenen un *Code-Status* amb el primer dígit igual a 5 (5xx). Les respostes que pertanyen a aquesta classe són emprades pel servidor quan l'error és del servidor, i no pas de la petició rebuda.
- **Fallada global**. Tenen un *Code-Status* amb el primer dígit igual a 6 (6xx). Aquestes respostes ofereixen informació definitiva sobre un usuari, no sobre la petició en concret, com per exemple la declinació de sessió per part del servidor, la inexistència de l'usuari, etc.

El camp següent del missatge SIP són les **capçaleres**. Hi ha dues classes de capçaleres: les capçaleres generals i les capçaleres específiques. Pel que fa a la generals, hi ha cinc capçaleres que són obligatòries tant per a les peticions com per a les respostes (**Call-ID**, **To**, **From**, **Cseq** i **Via**). A més, les peticions

inclouen una sisena capçalera obligatòria (**Max-Forwards**) que, malgrat no ser obligatòria a les respostes, pot ser-hi inclosa opcionalment.

- **Call-ID**. Aquesta capçalera identifica tots els missatges involucrats en una sessió. Abans d'iniciar l'establiment d'una sessió, l'UAC determina un valor de Call-ID que es manté fins al final de la sessió. En cas que a la sessió hi intervingui més d'un client, tots ells utilitzen el mateix valor per al Call-ID. El format del Call-ID respon a número@domini.

- **To**. Es tracta de l'adreça de la destinació del missatge. Per a identificar la destinació s'utilitza el format de l'URI, tal com s'ha fet a la línia inicial. Aquesta capçalera, però, va acompanyada d'un *tag* o etiqueta. Aquesta etiqueta és útil per a poder identificar, junt amb les capçaleres Call-ID i From, la sessió. Aquesta etiqueta és obligatòria i en cas de no ser-hi s'interpreta que és igual a 0. Per exemple, To: sip_consultor@uoc.edu; tag=381492.

  Per a les peticions de REQUEST, la capçalera To no inclou la destinació (ja incorporada a la línia inicial), sinó que pren el valor de l'adreça que ha de ser registrada al servidor de registre.

- **From**. És una capçalera completament anàloga a la capçalera To, però per a l'adreça d'origen.

- **Cseq**. Aquesta capçalera pren un valor enter inicialment aleatori. Un cop establert, i dins d'una sessió, cada vegada que es finalitza una transacció exitosa, Cseq s'incrementa en una unitat. Dins de cada transacció, tant la petició com les respostes utilitzen el mateix valor. A més del número de seqüència, també s'hi inclou el mètode. Per exemple, en una petició INVITE, la capçalera prendria un valor igual a Cseq: 2837 INVITE.

- **Via**. Les peticions SIP poden passar per diversos servidors *proxy* entre l'usuari client i l'usuari servidor. Cadascun dels servidors que encaminen la petició inclou la seva adreça per tal que, a recepció, la resposta pugui refer el camí de la petició. El format de cada capçalera Via és el següent: *Protocol/Version/Transport host; port; Via-parameter comment*

  El *Protocol* pren el valor de SIP, la *Version* pren el valor que correspongui a la versió del protocol, *Transport* fa referència al protocol de la capa de transport utilitzat, que habitualment és UDP o TCP, i el *host* i el *port* són l'adreça del servidor que el retransmet. Addicionalment es poden afegir més paràmetres, però només n'hi ha un d'obligatori: l'anomenat *branch*. El valor de *branch* es igual a l'identificador de la transacció precedit pel valor z9hG4bk. Per exemple, si una petició és retransmesa per un servidor proxy.uoc.edu, a través del port 5060 i SIP utilitza el protocol UDP, la capçalera introduïda per aquest servidor podria tenir la següent estructura: Via: SIP/2.0/UDP proxy.uoc.edu:5060; branch=z9hG4bk17321.

- **Max-Forwards**. El client, en enviar una petició, pot establir un nombre màxim de salts. En concret, si la petició no ha arribat al servidor en un nombre màxim de salts, es produeix un error. Tal com ja s'ha fet notar,

aquesta capçalera només és obligatòria per a les peticions i no s'inclou a la capçalera de les respostes.

Les capçaleres específiques no són obligatòries i estan definides per a poder transportar informació addicional. Les més importants són aquelles capçaleres que inclouen, per exemple, informació d'autenticació o de registre.

El **cos del missatge** conté la informació que intercanvien els dos usuaris. És precisament en aquesta part del missatge en la qual s'inclou la informació de negociació dels paràmetres del servei. Per a aquesta negociació es fa servir el *Session Description Protocol* (SDP), definit a l'RFC 4566.

3.2. La sessió SIP

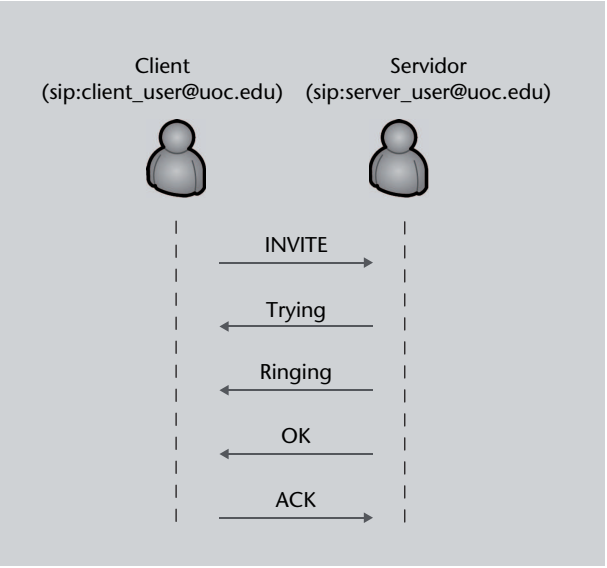
Les tres transaccions bàsiques dutes a terme pel protocol SIP són l'establiment de la sessió, la finalització de la sessió, i la modificació de la sessió existent. A continuació s'explica cadascuna d'aquestes transaccions.

3.2.1. Establiment de la sessió

L'establiment d'una sessió es divideix en tres parts. La primera part és aquella en la qual el client envia una petició INVITE per a iniciar el procés d'establiment de la sessió. En una segona part, el servidor respon afirmativament o negativament. Finalment, el client, en cas de rebre una resposta positiva, en notifica positivament la recepció.

La millor manera de veure-ho és mitjançant un exemple. Imaginem la situació de la figura 18, on un client (amb una URI sip:client_user@uoc.edu) es disposa a inicar una sessió amb un servidor (amb una URI sip:server_user@uoc.edu). La versió del protocol SIP és la 2.0, la capa de transport és UDP i el port utilitzat el 5060.

Figura 18. Establiment d'una sessió SIP



Inicialment el client envia la petició següent:

```
INVITE sip:server_user@uoc.edu:5060 SIP/2.0
Via: SIP/2.0/UDP uoc.edu; branch=z9hG4bk4582
Max-Forwards: 70
From: sip:client_user@uoc.edu:5060; tag=354828
To: sip:server_user@uoc.edu:5060
Call-ID: 257284@uoc.edu
Cseq: 1 INVITE
Contact: < sip:client_user@uoc.edu:5060;transport=UDP >
Content-Type: application/sdp
Content-Length: 151
— Informació de negociació (SDP) —
```

És important notar que el client ha seleccionat, aleatòriament, el *tag* per a la capçalera From. Aquest paràmetre és triat localment. Pel que fa al número de seqüència, el valor que pren també ha estat seleccionat pel client. Suposem que és 1 perquè es tracta de la primera seqüència. La capçalera Contact fa referència a l'adreça URI on es volen rebre les peticions, mentre que Content-Type determina quin tipus de contigut inclou el cos del missatge. En aquest cas, es tracta d'un inici de sessió i, en conseqüència, d'una negociació de paràmetres mitjançant el protocol SPD. El cos del missatge conté informació de la negociació dels paràmetres de la sessió, però no hi aprofundirem perquè queda fora de l'objectiu de l'apartat.

En rebre la petició, el servidor ha de respondre indicant si s'ha pogut alertar l'usuari servidor o no. A l'exemple de la figura 18 s'hi inclou una resposta Trying. Aquesta resposta és enviada pel servidor si, iniciat el processament de la Petició, preveu un retard excessiu que podria fer pensar al client que la petició s'ha perdut. Si el servidor té un temps de resposta baix, no caldria enviar cap resposta Trying i s'enviaria directament la Resposta Ringing (indicadora de l'alerta al servidor).

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP sip:server_user@uoc.edu:5060;branch=z9hG4bk4582
From: sip:server_user@uoc.edu:5060;tag=187272
To: sip:client_user@uoc.edu:5060; tag=354828
Call-ID: 257284@uoc.edu
CSeq: 1 INVITE
Contact: < sip:server_user@uoc.edu:5060;transport=UDP >
Content-Length: 0
```

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP sip:server_user@uoc.edu:5060;branch=z9hG4bk4582
From: sip:server_user@uoc.edu:5060;tag=187272
To: sip:client_user@uoc.edu:5060; tag=354828
Call-ID: 257284@uoc.edu
CSeq: 1 INVITE
Contact: < sip:server_user@uoc.edu:5060;transport=UDP >
Content-Length: 0
```

Fixem-nos que el servidor selecciona un *tag* localment i s'inclou a la capçalera From. A més, en totes dues respostes es conserva un únic identificador de diàleg (Call-ID) i, com que es tracta de dues respostes que pertanyen a la mateixa transacció, la capçalera CSeq es manté. En el moment en el qual el servidor accepta l'establiment de la sessió, la resposta és un OK que inclou la informació dels paràmetres negociats de la sessió.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP sip:server_user@uoc.edu:5060;branch=z9hG4bk4582
From: sip:server_user@uoc.edu:5060;tag=187272
To: sip:client_user@uoc.edu:5060; tag=354828
Call-ID: 257284@uoc.edu
CSeq: 1 INVITE
Contact: < sip:server_user@uoc.edu:5060;transport=UDP >
Content-Type: application/sdp
Content-Length: 147
— Informació de negociació (SDP) —
```

La resposta OK suposa la confirmació de l'establiment per part de l'usuari servidor i, per tant, cal una notificació positiva com la que es mostra:

```
ACK sip:server_user@uoc.edu:5060 SIP/2.0
Via: SIP/2.0/UDP uoc.edu; branch=z9hG4bk4582
Max-Forwards: 70
From: sip:client_user@uoc.edu:5060; tag=354828
To: sip:server_user@uoc.edu:5060
Call-ID: 257284@uoc.edu
Cseq: 1 ACK
Content-Length: 0
```

En aquest moment la sessió ha quedat establerta i la informació multimèdia, com per exemple la VoIP, es comença a transferir entre els dos usuaris mitjançant protocols com l'RTP.

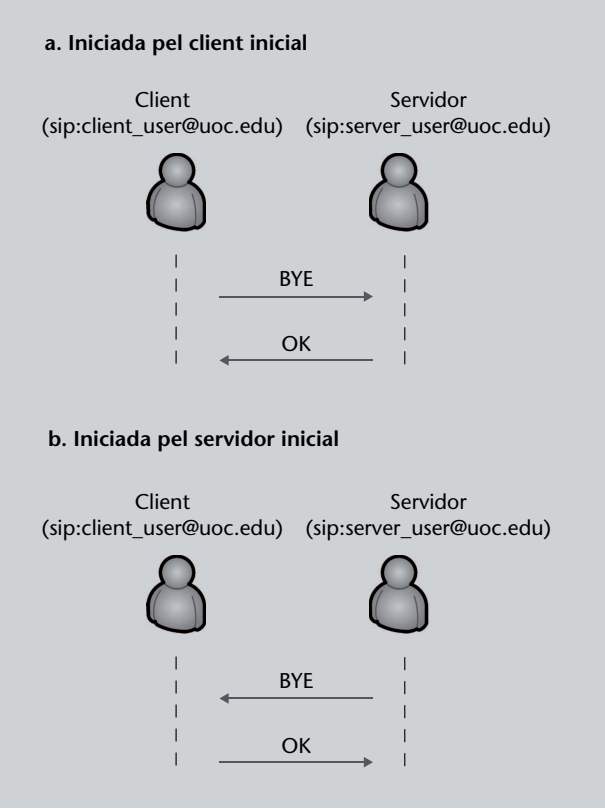
Aquest exemple és el d'un establiment satisfactori, però també hi podria haver problemes. Si l'usuari servidor, després d'enviar la Resposta Ringing, no respon amb una resposta OK abans d'un temps màxim, l'usuari client enviaria una petició CANCEL per a cancel·lar l'establiment de sessió en comptes d'una resposta OK. Una altra possibilitat seria que l'usuari servidor estigui ocupat. En aquest cas, la resposta de l'usuari servidor seria una alerta d'ocupació com la següent:

```
SIP/2.0 486 Busy Here
Via: SIP/2.0/UDP sip:server_user@uoc.edu:5060;branch=z9hG4bk4582
From: sip:server_user@uoc.edu:5060;tag=187272
To: sip:client_user@uoc.edu:5060; tag=354828
Call-ID: 257284@uoc.edu
CSeq: 1 INVITE
Contact: < sip:server_user@uoc.edu:5060;transport=UDP >
Content-Length: 0
```

3.2.2. Finalització de la sessió

La finalització de la sessió és un procés que consta d'una petició i la resposta corresponent. Aprofitant l'exemple anterior, expliquem l'alliberament.

Figura 19. Alliberament d'una sessió SIP



L'usuari que inicia l'alliberament amb una petició BYE pot ser tant el que inicialment era el client com el que inicialment era el servidor. Cal notar que el rol de client o servidor s'adquireix en iniciar una transacció. Per tant, a la figura 19 (a) el client és l'usuari de l'esquerra (client_user@uoc.edu) i a la figura 19 (b) el client és l'usuari de la dreta (server_user@uoc.edu). En tots dos casos la petició és igual, però cal tenir present el següent:

- A la figura 19 (a) la capçalera Cseq ha de prendre el mateix valor que a l'establiment més 1 (es tracta d'una nova transacció).

```
BYE sip:server_user@uoc.edu:5060 SIP/2.0
Via: SIP/2.0/UDP uoc.edu; branch=z9hG4bk4582
Max-Forwards: 70
From: sip:client_user@uoc.edu:5060; tag=354828
To: sip:server_user@uoc.edu:5060;tag=187272
Call-ID: 257284@uoc.edu
CSeq: 2 BYE
Content-Length: 0
```

```
ACK sip:client_user@uoc.edu:5060 SIP/2.0
Via: SIP/2.0/UDP uoc.edu; branch=z9hG4bk4582
Max-Forwards: 70
From: sip:server_user@uoc.edu:5060; tag=187272
To: sip:client_user@uoc.edu:5060; tag=354828
Call-ID: 257284@uoc.edu
Cseq: 2 ACK
Content-Length: 0
```

- Si la finalització s'inicia com a la figura 19 (b), el número de seqüència Cseq pren el valor de la darrera transacció iniciada per l'usuari de la dreta. En aquest cas hem considerat que Cseq val 5, però en realitat dependrà del valor que hagués pres en la darrera petició.

```
BYE sip:client_user@uoc.edu:5060 SIP/2.0
Via: SIP/2.0/UDP uoc.edu; branch=z9hG4bk4582
Max-Forwards: 70
From: sip:server_user@uoc.edu:5060;tag=187272
To: sip:client_user@uoc.edu:5060; tag=354828
Call-ID: 257284@uoc.edu
CSeq: 5 BYE
Content-Length: 0
```

```
ACK sip:server_user@uoc.edu:5060 SIP/2.0
Via: SIP/2.0/UDP uoc.edu; branch=z9hG4bk4582
Max-Forwards: 70
From: sip:client_user@uoc.edu:5060; tag=354828
To: sip:server_user@uoc.edu:5060; tag=187272
Call-ID: 257284@uoc.edu
Cseq: 5 ACK
Content-Length: 0
```

3.2.3. Modificació de la sessió

El protocol SIP permet modificar els paràmetres de la sessió sense necessitat de finalitzar-la. De la mateixa manera que la negociació inicial duta a terme durant l'establiment es fa mitjançant el protocol SDP, i unes instruccions semblants a les instruccions bàsiques d'establiment i finalització.

3.3. Serveis oferts per SIP

Fins ara hem analitzat les sessions SIP però, més enllà dels servidors *proxy* que reenvien les peticions i les respostes, no s'han explicat els serveis oferts per la resta de nodes: el servidor de registre, el servidor de reencaminament i el servidor de localització.

SIP és un protocol de senyalització en xarxes de paquets dissenyat per a fer front a la mobilitat dels usuaris. Atès aquest requisit, cal que qualsevol usuari pugui ser localitzat en qualsevol moment.

La dificultat associada a la localització és que a les xarxes IP l'adreça URI de l'usuari pot canviar al llarg del temps. La xarxa a través de la qual es connecta l'usuari té efectes sobre la seva adreça i, en conseqüència, sobre la possibilitat de localitzar-lo. El protocol SIP defineix el servidor de registre com el node que emmagatzema periòdicament la relació entre l'URI de l'usuari i la identitat de l'usuari. Per a fer-ho, calen dues condicions:

1) Que cada usuari disposi d'un identificador global.

2) Que el servidor de registre emmagatzemi en cada moment quina és la relació entre l'adreça global i l'URI.

L'adreça global per a un usuari s'anomena, segons la terminologia pròpia de la IETF, *Address of Record* (AoR)*. Aquesta adreça no canvia independentment de la xarxa des de la qual es connecta. El procés de registre es fa mitjançant una

*** En la terminologia de 3GPP, l'AoR es denomina *Public identity*.**

petició REGISTER. Per a aquestes peticions, la línia inicial incorpora l'adreça del servidor de registre, mentre que la capçalera To inclou l'AoR de l'usuari.

El problema de la mobilitat, un cop registrada la relació entre la localització d'un usuari i la seva identitat, requereix poder consultar la informació emmagatzemada al servidor de registre. L'estructura definida pel protocol SIP no preveu la possibilitat que l'usuari faci peticions directament al servidor de registre; el servidor de registre rep exclusivament peticions de registre i en confirma o no la recepció correcta, però no proveeix l'usuari amb la informació que emmagatzema.

Podeu consultar l'RTC 3261 per a aprofundir en el format i els paràmetres de la petició de registre (REGISTER).

Per aconseguir implementar mobilitat cal la participació d'un altre node: el servidor de reencaminament. El servidor de reencaminament té la funció de rebre les peticions dels clients i, gràcies a la comunicació amb el servidor de registre, contestar la petició amb una resposta que conté l'adreça de l'UAS. Així, gràcies als servidors de registre i de reencaminament és possible implementar una solució que suporta mobilitat dels usuaris.

En una xarxa amb certa complexitat difícilment els usuaris client i servidor poden comunicar-se directament sense l'ajut d'un servidor *proxy*. La funció del **servidor proxy** és la de rebre missatges (peticions i respostes) i reencaminar-los cap al node següent. Fixem-nos, doncs, que, si ens centrem en un proxy determinat i per a un mateix missatge, exerceix la funció de servidor quan rep el missatge provinent d'un altre node i, alhora, exerceix la funció de client quan el retransmet cap al node següent.

Per tant, la funció bàsica del servidor *proxy* és la de retransmetre els missatges rebuts cap al node apropiat. És important adonar-se que en aquest procés el servidor *proxy* pot prendre dues polítiques: intervenir en la comunicació de manera activa o, per contra, exercir només la funció de retransmissió. Els servidors *proxy*, en funció de la seva estratègia, s'anomenen *stateless proxy* o *stateful proxy*.

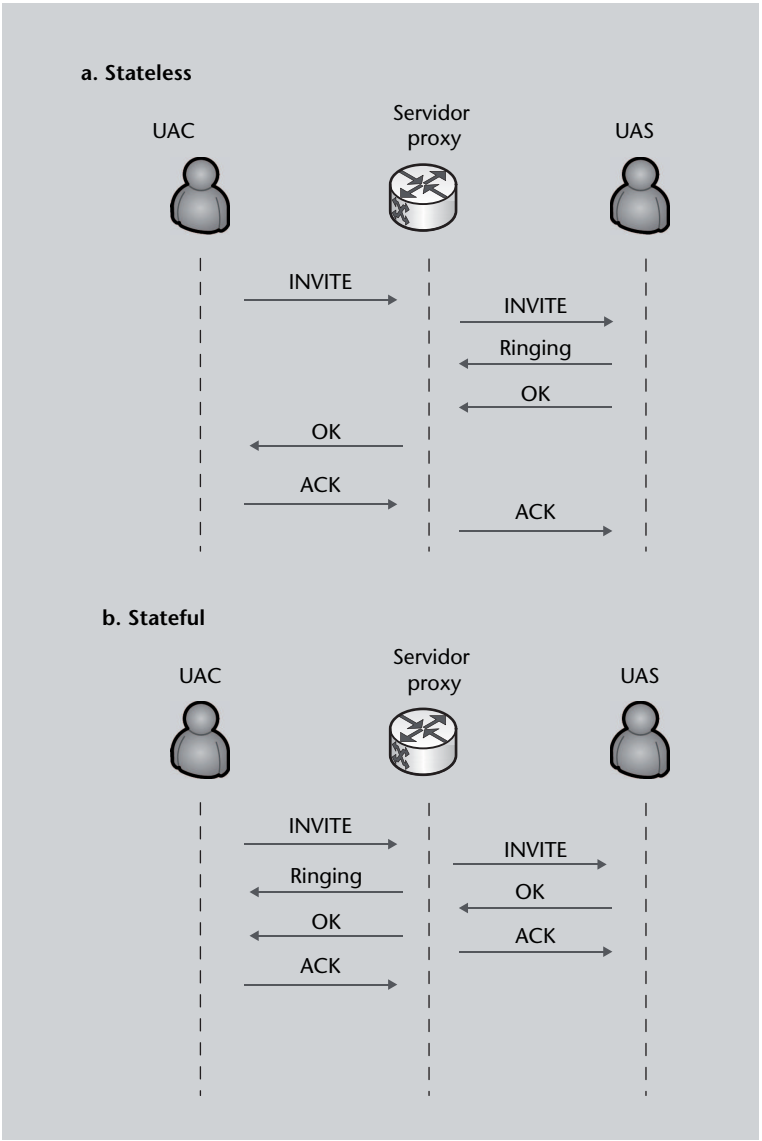
- Els anomenats ***stateless proxys*** són aquells servidors que no duen a terme cap processament dels missatges. L'objectiu és que aquest tipus de servidor esdevingui transparent als usuaris finals. El fet que les capçaleres dels missatges incorporin l'adreça dels diferents servidors per on ha transcorregut el missatge permet que el servidor *proxy* no hagi de guardar en memòria cap informació sobre els missatges. Per exemple, aquest tipus de servidor mai no retransmetria un missatge en detectar una pèrdua, ja que no utilitza cap temporitzador per a controlar-ho.

- Els ***stateful proxys***, en canvi, incorporen moltes més funcionalitats. Aquests servidors gestionen les transaccions i són capaços de respondre a determi-

nades peticions abans de reenviar els missatges. Són, doncs, servidors que intervenen en la comunicació de manera activa i que, per tant, no són transparents als usuaris. Per exemple, si després de reenviar un missatge no es rep el missatge esperat abans d'un període determinat, aquests servidors entenen que hi ha hagut una pèrdua i tornen a retransmetre el missatge.

La figura 20 mostra l'esquema de l'establiment d'una sessió amb la intervenció d'un servidor *proxy*. A la figura 20 (a) el servidor és *stateless* i a la figura 20 (b) el servidor és *stateful*. Com es pot observar, el servidor *stateless* només reenvia els missatges rebuts, mentre que el servidor *stateful* reenvia missatges però també genera respostes.

Figura 20. Establiment de sessió amb *proxy*



4. El futur de la senyalització a les xarxes IP

Es fa difícil predir el futur de les xarxes de telecomunicació amb precisió, però sembla una evidència que les xarxes del futur, les xarxes anomenades de nova generació (*Next Generation Networks*, NGN), convergeixen cap a les xarxes IP. La convergència tant de la xarxa telefònica com de les xarxes de telefonia mòbil cap a xarxes troncals de paquets basades en el protocol IP és un fet avui en dia.

Arquitectures com la *IP Multimedia Subsystem* (IMS), inicialment pensada per a la xarxa troncal de comunicacions mòbils però posteriorment entesa com una possibilitat per a esdevenir l'arquitectura de les xarxes de nova generació, deixen intuir que en el camp de la senyalització protocols com el SIP tenen un present i un futur prometedor*.

*** L'IMS fou definit segons les especificacions del protocol SIP.**

Malgrat això, no es poden obviar les incerteses. Els esforços ingents dels diferents actors del món de les telecomunicacions per a aconseguir definir estàndards globals s'ha demostrat, gairebé sempre, impossible. Exemples com la dicotomia entre els protocols H.323 i SIP en són una prova.

El que sí sembla evident és que els milers de quilòmetres d'enllaços i de nodes de xarxa desplegats arreu del món no poden ser substituïts d'un dia per l'altre. La interoperabilitat entre xarxes, i concretament entre els seus protocols de senyalització, és una necessitat avui i ho serà en el futur. És en aquest context que podem assegurar que les xarxes del futur seran el resultat d'un conjunt heterogeni de xarxes amb característiques diferents, amb protocols de senyalització diversos, i amb necessitats particulars. Cal, doncs, tenir clar que en un entorn com el que es planteja, la senyalització continuarà essent, en essència, el camp fonamental de les telecomunicacions que permetrà arribar a oferir serveis globals.

Resum

Aquest mòdul ens ha permès veure quines són les problemàtiques en la interconnexió de xarxes telefòniques de commutació de circuits i xarxes IP, així com la solució aportada pel conjunt de protocols d'adaptació de SIGTRAN. S'ha descrit en detall quins són els protocols que ho permeten i com, amb els clàssics protocols de la capa de transport (TCP i UDP), no és possible assolir els requisits de la senyalització SS7.

SIGTRAN examina les mancances dels protocols UDP i TCP i soluciona els desavantatges existents basant-se, principalment, en el protocol TCP. Característiques com ara el *multi-homing* o *el multi-streaming* són les grans aportacions del protocol de la capa de transport definit: l'SCTP.

Pel que fa a la senyalització entre usuaris de VoIP, aquest mòdul també ens ha permès endinsar-nos en els conceptes bàsics del protocol SIP i en les característiques dels seus missatges. Hem pogut comprovar que la gran flexibilitat i senzillesa (si més no en les primeres versions de SIP) han fet que s'imposi per sobre d'altres alternatives, com per exemple l'H.323, amb vista a les futures xarxes *All-IP*.

Exercicis d'autoavaluació

1. Expliqueu els motius pels quals la senyalització SS7 no es pot transportar amb UDP o TCP. Quines són les característiques principals que permeten que l'SCTP sigui apropiat per a fer-ho?

2. En què consisteix el *cookie mechanism* d'SCTP?

3. En una PDU d'SCTP, es poden incloure més d'un *chunk* de dades? I un *chunk* de dades amb un *chunk* INIT ACK? Raoneu la resposta.

4. Assenyaleu la resposta falsa i raoneu-ho. Un *Signalling Gateway* que connecta una xarxa SS7 i una xarxa IP:

a) Sempre té una adreça IP per a la xarxa IP i un codi de punt per a la xarxa SS7.

b) No sempre té un codi de punt; només si té una instància de la capa MTP3.

c) Si fa servir la capa d'adaptació M2UA només té adreça IP, però si fa servir M2PA té adreça IP i codi de punt.

d) Quan té una instància d'M3UA o de SUA té tant adreça IP com Codi de Punt.

5. Expliqueu per què el protocol M3UA implementa funcions d'encaminament independents de la capa MTP3.

6. Assenyaleu l'afirmació incorrecta.

a) SIP només defineix l'establiment, finalització i gestió d'una sessió, però no és responsable del transport de dades multimèdia.

b) El protocol H.323 és més complet que el SIP però és menys flexible.

c) En cada transacció, el *Call-ID* present tant en peticions com en respostes s'ha d'incrementar en una unitat.

d) Els *tags* de les capçaleres *From* i *To* són seleccionades localment.

7. Suposeu la següent petició i resposta entre dos nodes SIP. Substituïu els valors marcats amb una X pels valors que corresponguin.

INVITE sip:david@in3.edu SIP/2.0
Via: SIP/2.0/X in3.edu; branch=X
Max-Forwards: 70
From: sip:rosa@uoc.edu; tag=X
To: sip:david@in3.edu
Call-ID: 82283@uoc.edu
Cseq: X INVITE
Contact: < sip:david@in3.edu;transport=TCP >
Content-Type: application/sdp
Content-Length: 149
— *Informació de negociació (SDP)* —

SIP/2.0 X Ringing
Via: SIP/2.0/X sip:david@in3.edu;branch=z9hG4bk431ssl
From: david@in3.edu;tag=14533
To: sip:rosa@uoc.edu; tag=22164
Call-ID: X
CSeq: 163 X
Contact: < david@in3.edu;transport=TCP >
Content-Length: 0

Glossari

3GPP 3rd Generation Partnership Project. Organisme d'estandardització de les comunicacions mòbils.

AIMD Additive-Increase Multiplicative-Decrease. Mecanisme de control de congestió i de flux implementat tant a TCP com a SCTP.

All-IP Tot IP. Situació en què totes les xarxes convergeixen cap a xarxes IP (tot el trànsit és IP).

AoR Address of Record. Identificador global d'un usuari SIP emmagatzemat al servidor de registre.

BSN Backward Sequence Number. Camp utilitzat en el mecanisme de correcció d'errors a la capa MTP2.

DoS Denial of Service. Tipus d'atac contra TCP.

DP Destination Port. Camp del port de destinació en una PDU d'SCTP.

DPC Destination Point Code. Camp del *routing label* del missatge MTP3.

FISU Fill-In Signal Unit. Un dels tres tipus d'unitats de senyalització.

FSN Forward Sequence Number. Camp utilitzat en el mecanisme de correcció d'errors a la capa MTP2.

GK Gatekeeper. Node de la xarxa IP.

GTT Global Title Translation. Mecanisme que permet convertir una adreça en format GT a un format PC+SSN.

HTTP Hypertext Transfer Protocol. Protocol d'aplicació utilitzat al WWW.

IETF Internet Engineering Task Force. Organització estandarditzadora a Internet.

IMS IP Multimedia Subsystem. Arquitectura de xarxa per a serveis basats en IP.

IP Internet Protocol.

IPSP IP Signalling Point. Punt de senyalització IP connectat a la xarxa IP que implementa les capes altes de l'SS7.

ISUP Integrated Services User Part. Protocol del nivell 4 de l'SS7.

ITU-T ITU - Telecommunications Standardization Sector. Es tracta d'una de les tres divisions de la ITU.

IUA ISDN Q.921-User Adaptation Layer.

LSSU Link Status Signal Unit. Un dels tres tipus d'unitats de senyalització.

M2PA MTP2-user Peer-to-peer Adaptation. Protocol de SIGTRAN.

M2UA MTP2-User Adaptation. Protocol de SIGTRAN.

M3UA MTP3-User Adaptation. Protocol de SIGTRAN.

MEGACO Media Gateway Controller. Protocol de senyalització usat entre un Media Gateway i un Media Gateway Controller. També conegut com a H.248.

MG Media Gateway. Node de la xarxa IP.

MGC Media Gateway Controller. Node de la xarxa IP.

MP Message Priority. Paràmetre del missatge M3UA.

MSU Message Signal Unit. Un dels tres tipus d'unitats de senyalització.

MTP Message Transfer Part. Protocols MTP1, MTP2 i MTP3 dels nivells 1, 2 i 3 d'SS7, respectivament.

NGN Next Generation Network. Arquitectura de xarxa per a les xarxes All-IP.

NI Network Indicator. Paràmetre del missatge M3UA.

OPC Originating Point Code. Camp del *Routing label* del missatge MTP3.

OSI Open System Interconnection. Model de xarxa dividit en set capes.

PDU Protocol Data Unit. Unitat de transferència de dades d'SCTP.

QoS Quality of Service.

RFC Request for Comments.

RTCP Real-Time Control Protocol. Vegeu RTP.

RTP Real-Time Transport Protocol. Protocol d'aplicació utilitzat per a la transmissió d'informació en temps real.

SCCP Signalling Connection Control Part. Protocol del nivell 4 de l'SS7.

SCTP Stream Control Transmission Protocol. Protocol de la capa de transport.

SDP Session Description Protocol. Protocol de descripció de paràmetres de dades multimèdia.

SG Service Gateway. Node de la xarxa IP.

SI Service Indicator. És un dels dos subcamps del SIO del missatge MTP3.

SIGTRAN Signaling Transport. Conjunt de protocols definits per la IETF.

SIP Session Initiation Protocol. Protocol de senyalització IP.

SLS Signalling Link Selector. Camp del *routing label* del missatge MTP3 de les funcions SMH.

SP Source Port. Camp del port d'origen en una PDU d'SCTP.

SS7 Signalling System No 7. Estàndard de senyalització desenvolupat per la ITU-T.

SSN Stream Sequence Number. Camp de la PDU d'SCTP.

STP Signal Transfer Point. Punt de senyalització de la xarxa SS7.

SUA SCCP User Adaptation. Protocol de SIGTRAN.

TCAP Transaction Capabilities Application Part. Protocol del nivell 4 de l'SS7.

TCP Transmission Control Protocol. Protocol de la capa de transport.

TUP Telephone User Part. Protocol del nivell 4 de l'SS7.

UA User Adaptation layer. Conjunt de protocols que juntament amb l'SCTP conformen SIGTRAN.

UAC User Agent Client. Usuari que transmet una petició SIP.

UAS User Agent Server. Usuari que transmet una resposta SIP.

UDP User Datagram Protocol. Protocol de la capa de transport.

URI Uniform Resource Identifier.

V5UA V5.2-User Adaptation Layer. Protocol de SIGTRAN.

VoIP Voice over IP. Conjunt de normes, dispositius i protocols per a comunicacions de veu sobre el protocol de xarxa IP.

XDSI Xarxa Digital de Serveis Integrats. És la denominació catalana per a l'acrònim anglès ISDN.

XTC Xarxa Telefònica Commutada. És la denominació catalana per a l'acrònim anglès PSTN.

Bibliografia

Agbinya, J. I. (2004). *IP Communications and Services for NGN*. Boca Raton (EUA): CRC Press.

van Bosse, J. G.; F. U. Devetak (2007). *Signaling in Telecommunication Networks* (2a ed.). Nova Jersey (EUA): John Wiley & Sons, Inc.

Davidson, J.; J. Peters (2000). *Voice over IP fundamentals*. Indianapolis (EUA): Cisco Press.

Dryburgh, L.; J. Hewett (2004). *Signaling Systems No. 7 (SS7/C7). Protocol, Architecture and Services*. Indianapolis (EUA): Cisco Press.

Hersent, O. (2011). *IP Telephony. Deploying VoIP Protocols and IMS Infrastructure, Second Edition*. West Sussex (Regne Unit): John Wiley & Sons, Inc.

IETF *RFC 4960. Stream Control Transmission Protocol*.

IETF *RFC 3331. Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Adaptation Layer*.

IETF *RFC 4165. Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Peer-to-Peer Adaptation Layer (M2PA)*.

IETF *RFC 4666. Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)*.

IETF *RFC 3868. Signalling Connection Control Part User Adaptation Layer (SUA)*.

IETF *RFC 3261. SIP: Session Initiation Protocol*.

ITU-T *Recomanació H.323: Packet-based multimedia communications systems*.

Johnston, A. B. (2009). *Sip: Understanding the Session Initiation Protocol*. Norwood (EUA): Artech House.

Kozierok, C. H. (2004). *The TCP/IP guide: A comprehensive, illustrated Internet Protocol Reference*. San Francisco (EUA): William Pollock.

Poikselka, M.; G. Mayer; H. Khartabil; A. Niemi (2004). *The IMS. IP Multimedia Concepts and Services in the Mobile Domain*. West Sussex (Regne Unit): John Wiley & Sons, Inc.

Russell, T. (2006). *Signaling Systems 7. Fifth Edition.*. Nova York (EUA): McGraw-Hill Professional.

Stewart, R. R.; Q. Xie (2001). *Stream Control Transmission Protocol (SCTP): A Reference Guide*. Addison-Wesley.